CONSIGLIO NAZIONALE
DEGLI INGEGNERI

FONDAZIONE
CONSIGLIO NAZIONALE INGEGNERI

ORDINE DEGLI INGEGNERI
DELLA PROVINCIA DI TREVISO

MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI

OBBLIGO PER GLI ORDINI DI ADEGUAMENTO
NORMATIVO ENTRO IL 31 DICEMBRE 2017
AI SENSI DELLA CIRCOLARE AGID N.2/2017

INCONTRO FORMATIVO

TREVISO

Martedì 21 novembre 2017

Sala conferenze Ordine Ingegneri
Prato della Fiera 23

MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI

Treviso 21 Novembre 2017

FONDAZIONE
CONSIGLIO NAZIONALE INGEGNERI

AGENDA

14:00 Saluti
14:15 1° modulo “Il quadro normativo di riferimento”
14:45 2° modulo “La circolare AgID e la sicurezza informatica”
15:30 Pausa
15:40 3° modulo “Aspetti tecnici-operativi per l’attuazione delle misure minime di sicurezza ICT”
16:30 4° modulo “Domande e dibattito”
17:00 Chiusura Lavori

1° modulo “Il **quadro normativo** di riferimento”

elisabetta canali

FONDAZIONE
CONSIGLIO NAZIONALE INGEGNERI

QUADRO NORMATIVO

- Regolamento UE 2016/679 (GDPR)
- Circolare AgID n°2/2017
- Codice della Privacy (D.Lgs. 196/2003)
- Codice dell'Amministrazione Digitale (CAD)
- Piano Triennale 2017-2019

Normativa europea di riferimento sulla sicurezza informatica

- **Regolamento UE 2016/679** (*General Data Protection Regulation* - GDPR) pubblicato in Gazzetta Ufficiale Europea il 4 maggio 2016, immediatamente applicabile dal 25 maggio 2018, abroga la Direttiva 95/46/CE.
- Il Regolamento sostituirà (non integralmente) il Codice della Privacy, in vigore dal 1° gennaio 2004, e sarà necessario un coordinamento normativo.

Novità introdotte dal Regolamento UE 2016/679

- **Elimina la frammentazione applicativa della normativa** in materia di protezione dei dati personali nel territorio dell'UE, dovuta alle diverse leggi di recepimento della Direttiva 95/46/CE.
- **Previsti nuovi adempimenti** e richiesta un'**intensa attività di adeguamento**, preliminare alla sua definitiva applicazione a partire dal 25 maggio 2018.

Novità introdotte dal Regolamento UE 2016/679

- **Ambito di applicabilità:**
  - Trattamento dati personali di persone fisiche (art.2)
  - Rovesciato il principio di stabilimento: trattamento dati da parte di titolari anche non stabiliti nell'UE, sempre che gli interessati si trovino nell'UE (art.3).

Novità introdotte dal Regolamento UE 2016/679

- **Principio di «Responsabilizzazione» di Titolari e Responsabili (c.d. *Accountability*):**

Devono adottare comportamenti proattivi e tali da dimostrare la concreta adozione di misure (art. 5, comma 2).

Autorità di controllo interviene "ex post", ossia dopo le determinazioni assunte autonomamente dal Titolare/Responsabile.

Novità introdotte dal Regolamento UE 2016/679

- **Nuovi obblighi per il Titolare ed il Responsabile del trattamento (artt. 24-34)**

Ruolo più proattivo e obblighi più pregnanti: rispetto delle regole e adozione di tutti gli accorgimenti tecnici e organizzativi necessari a garantire la qualità del risultato del processo di adeguamento in atto.

Inadempimento degli obblighi è fonte di responsabilità (principio di responsabilizzazione o "*accountability*").

Novità introdotte dal Regolamento UE 2016/679

Titolare del trattamento: persona fisica/giuridica che determina le finalità ed i mezzi del trattamento dei dati personali.

Responsabile del trattamento: persona fisica/giuridica che tratta i dati personali per conto del Titolare.

Novità introdotte dal Regolamento UE 2016/679

- **Introdotta la figura del Responsabile della protezione dei dati (RPD) (artt. 37–39) c.d. *Data Protection Officer* (DPO)**

RDP designato - dal Titolare o dal Responsabile del trattamento - in base alla sua professionalità e conoscenza della legislazione di protezione dei dati ed è tenuto, *inter alia* a:

- informare e consigliare il Titolare o il Responsabile in merito agli obblighi derivanti dal Regolamento e da altre disposizioni dell'UE;

- sorvegliare che il Regolamento sia osservato;

- fornire, se richiesto, un parere in merito alla Valutazione d'Impatto;

- cooperare con l'Autorità di controllo (ruolo di "facilitatore").

Novità introdotte dal Regolamento UE 2016/679

- Nomina del Responsabile della protezione dei dati (RPD) è **obbligatoria**:
  - per autorità e soggetti pubblici;
  - per altri soggetti che effettuano un monitoraggio regolare e sistematico delle persone fisiche, o trattano su larga scala dati sensibili.
- Negli altri casi è comunque consigliata la nomina.

Novità introdotte dal Regolamento UE 2016/679

- **Istituzione del Registro delle attività di trattamento (art. 30)** obbligatoria per organizzazioni con più di 250 dipendenti o in tutti i casi in cui il trattamento presenta un rischio per i diritti e le libertà dell'interessato.
- Registro tenuto in forma scritta, anche in formato elettronico, contiene gli elementi di cui all'art. 30.

Novità introdotte dal Regolamento UE 2016/679

- **Notifica delle violazioni dei dati personali - cd. *data breach* - all'autorità di controllo (art. 33)**

Titolare del trattamento deve notificare la violazione, senza ingiustificato ritardo, all'autorità di controllo (i.e., al Garante) e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

Notifica dopo le 72 ore → solo se adeguatamente motivata.

Responsabile del trattamento deve informare il Titolare, senza ingiustificato ritardo, della violazione.

Novità introdotte dal Regolamento UE 2016/679

- **Notifica delle violazioni dei dati personali - cd. *data breach* - all'interessato (art. 34)**

Titolare del trattamento deve comunicare la violazione all'interessato, senza giustificato ritardo, in caso di violazione suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Novità introdotte dal Regolamento UE 2016/679

Valutazione d'Impatto sulla protezione dei dati (art. 35)

Obbligatoria nelle ipotesi di **rischio elevato** per i diritti e le libertà delle persone interessate (es.: monitoraggio sistematico di comportamenti, o moltitudine soggetti interessati).

Titolare del trattamento svolge la Valutazione, previa consultazione del Responsabile della protezione dei dati.

→ Valutazione dimostra l'osservanza del Regolamento (principio di «*accountability*»).

Novità introdotte dal Regolamento UE 2016/679

Valutazione di Impatto sulla protezione dati: modalità operative basilari (esempio)

- Raccolta di informazioni (es. questionario)
- Identificazione e valutazione del rischio
- Identificazione opzioni per mitigare o evitare il rischio
- Selezione di una metodologia per la Valutazione di Impatto
- Stesura e monitoraggio della Valutazione

Principali benefici:

- Pronta identificazione e gestione del rischio
- Risoluzione gap potenziali in termini di sicurezza

Novità introdotte dal Regolamento UE 2016/679

- **Trattamento sanzionatorio uniformato e inasprito (artt. 83-84)**

- **Sanzioni amministrative pecuniarie (art. 83)**: approccio graduale riguardo i criteri per l'imposizione e per la determinazione dell'ammontare massimo imponibile. Indici di valutazione:

(i) la natura, la gravità e la durata della violazione;

(ii) il carattere doloso o colposo della stessa;

(ii) le misure adottate dal Titolare.

Novità introdotte dal Regolamento UE 2016/679

- Sanzioni amministrative pecuniarie **fino a €10.000.000**, o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: violazione obblighi previsti dal Regolamento.
- Sanzioni amministrative pecuniarie **fino a €20.000.000**, o per le imprese fino al 5% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: violazione di obblighi più stringenti previsti dal Regolamento o nel caso di inosservanza degli ordini del Garante.
- Sanzioni amministrative pecuniarie inflitte in aggiunta alle misure di cui all'art. 58, par. 2 lett. da a) a h) e j), ovvero i **poteri correttivi** dell'Autorità di controllo.

Novità introdotte dal Regolamento UE 2016/679

- **Altre sanzioni (art. 84)**

Gli Stati membri possono stabilire le norme relative alle altre sanzioni, sempre che si assicuri la proporzionalità e l'efficacia dissuasiva.

Materia penale è di competenza dei singoli Stati.

Ogni Stato membro deve notificare alla Commissione la normativa applicata entro il 25 maggio 2018.

Normativa italiana di riferimento sulla sicurezza informatica

Circolare AgID 18 aprile 2017 n°2

- Sostituisce integralmente la Circolare AgID n°1/2017 (17 marzo 2017), recante misure minime di sicurezza ICT per le P.A., emessa in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015.
- Corregge alcune imprecisioni formali relative a riferimenti normativi ormai superati dal Codice dell'Amministrazione Digitale (CAD).

Normativa italiana di riferimento sulla sicurezza informatica

Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015

Assegna all'AgID il compito di sviluppare e rendere disponibili "indicatori degli standard di riferimento" che mettano le amministrazioni in grado di dotarsi degli standard minimi di prevenzione e reazione ad eventi cibernetici.

Circolare AgID n°2/2017
Misure minime di sicurezza ICT

- **FINALITA'** (art. 1): fornire alle P.A. un riferimento pratico (Misure Minime) per valutare e innalzare il proprio livello di sicurezza informatica.

Misure minime di sicurezza

↓

Insieme ordinato e ragionato di "controlli", ossia azioni puntuali di natura tecnica od organizzativa.

Circolare AgID n°2/2017
Misure minime di sicurezza ICT

L’insieme dei controlli - che costituiscono le Misure Minime AgID - è:

- modulato in modo da non costringere le Amministrazioni ad introdurre misure esagerate per la propria organizzazione.
- suddiviso in tre gruppi verticali, riferiti a livelli complessivi di sicurezza crescente:

– **“Minimo”**: obbligatorio per tutte le P.A. indipendentemente dalla struttura;

– **“Standard”**: base di riferimento per la maggior parte delle P.A., rappresenta un compromesso tra efficacia delle misure ed onerosità della loro implementazione;

– **“Alto”**: livello adeguato per le organizzazioni maggiormente esposte a rischi.

Circolare AgID n°2/2017
Misure minime di sicurezza ICT

DESTINATARI (art. 2): soggetti di cui all'art. 2, comma 2 del Codice dell'Amministrazione Digitale (C.A.D.)

- Pubbliche Amministrazioni (art.1, comma 2, D.Lgs. 30 marzo 2001, n.165).
- Enti pubblici non economici nazionali, regionali e locali (D.Lgs. 165/2001 art. 1 comma 2).

Circolare AgID n°2/2017
Misure minime di sicurezza ICT

- **ATTUAZIONE** (art.3): Il Responsabile dei sistemi informativi (definito all'art. 10 del D.Lgs. 39/1993) o, in sua assenza, il dirigente allo scopo designato deve attestare l'adozione delle misure di sicurezza informatica.

Circolare AgID n°2/2017
Misure minime di sicurezza ICT

- **IMPLEMENTAZIONE** (art.4): L'attestazione (tramite compilazione modulo di implementazione) deve essere sottoscritta digitalmente, con marcatura temporale, dal Responsabile informatico (o dal dirigente designato) e dal rappresentante legale dell'ente.

N.B. → marcatura temporale deve essere apposta sul documento.

Il numero di protocollo non è idoneo.

Circolare AgID n°2/2017
Misure minime di sicurezza ICT

- **INCIDENTE INFORMATICO** (c.d. *data breach*) → attestazione con segnalazione incidente deve essere inviata al CERT-P.A.
- **CONTROLLI**: Dopo l'entrata in vigore del Regolamento (25 maggio 2018) il Garante svolgerà delle ispezioni presso l'ente che ha subìto l'attacco – al fine di verificare le misure di sicurezza adottate – ed eventualmente comminare le sanzioni.

Circolare AgID n°2/2017
Misure minime di sicurezza ICT

- **SCADENZA** (art.5): Misure minime di sicurezza ICT devono essere adottate entro il **31 dicembre 2017**.

Il Responsabile dovrà adottare almeno le misure di livello minimo e tendere a rendere il sistema sicuro a seconda della propria situazione contingente.

Circolare AgID n°2/2017
Misure minime di sicurezza ICT

MANCATA APPLICAZIONE DELLE MISURE MINIME

- Fino all'entrata in vigore del Regolamento UE (25 maggio 2018): si applicano le sanzioni previste dal Codice della Privacy.
- Dopo l'entrata in vigore del Regolamento UE: l'attuale quadro sanzionatorio delineato dal Codice della Privacy dovrà essere adeguato al nuovo quadro di obblighi e requisiti che introdurrà il Regolamento UE.

Sanzioni Codice della Privacy

“Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell’articolo 2050 del codice civile” (art. 15, co. 1)

C.d. doppio binario:

- Sanzioni amministrative disciplinate agli artt.161-166.
- Sanzioni penali disciplinate agli artt. 167-170.

Violazione amministrativa

Violazione amministrativa	Sanzione
Omessa informativa	3k - 18k €
Omessa informativa in caso di dati sensibili o giudiziari o di trattamenti che presentino rischi specifici	5k - 30k €
Cessione dei dati	5k - 30k €
Omessa o incompleta informativa al Garante	10k - 60k €
Mancata esibizione di informazioni o documenti richiesti dal Garante	4k - 24k €

Illecito penale

Illecito penale	Sanzione
Trattamento illecito di dati	Reclusione da 6 mesi a 3 anni
False dichiarazioni e notificazioni al Garante	Reclusione da 6 mesi a 3 anni
Mancata adozione delle misure di sicurezza	Arresto fino a 2 anni o ammenda da 10.000 a 50.000 euro
Inosservanza dei provvedimenti del Garante	Reclusione da 3 mesi a 2 anni

Codice dell'Amministrazione Digitale (CAD)

- Codice dell'amministrazione digitale (CAD) adottato con D.Lgs. 7 marzo 2005, n.82 (e aggiornato al D.Lgs. 26 agosto 2016, n. 179): fondamentale per la digitalizzazione e la dematerializzazione dell'attività amministrativa.
- Art. 17 CAD: "Responsabile della transizione digitale" deve garantire "l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le regole tecniche" e deve essere presente in tutte le Amministrazioni.

Piano Triennale 2017- 2019

- **Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017–2019** definisce il modello di riferimento per lo sviluppo dell'informatica pubblica italiana e la strategia operativa di trasformazione digitale del Paese.
- Razionalizzazione delle risorse ICT come metodo prioritario per aumentare il livello di sicurezza attraverso la riduzione della "superficie" esposta agli attacchi informatici (capitolo 3 "Infrastrutture fisiche").

CONCLUSIONE

- Attuazione delle misure minime di sicurezza previste nella Circolare AgID n° 2/2017 è essenziale per l'adeguamento agli obblighi previsti dal Regolamento UE 2016/679 (necessario il coordinamento della normativa).
- Garante europeo della protezione dei dati (GEPD) - tramite il Gruppo di Lavoro WP 29 - sta collaborando con il Garante della Privacy per promuovere e facilitare l'applicazione del Regolamento (pubblicazione di linee guida, raccomandazioni e migliori prassi).

2° modulo “La circolare **AgID** e la **sicurezza informatica**”

marcello coiana

FONDAZIONE
CONSIGLIO NAZIONALE INGEGNERI

PREMESSA

- realtà digitale vs realtà analogica
  - il dato sensibile e il dato personale nel digitale e nell'analogico
  - cybersecurity
- consapevolezza cibernetica del cittadino e del personale
- privacy e security by design
- digitalizzazione dei processi nelle pubbliche amministrazioni
- BYOD vs COPE

PA TARGET

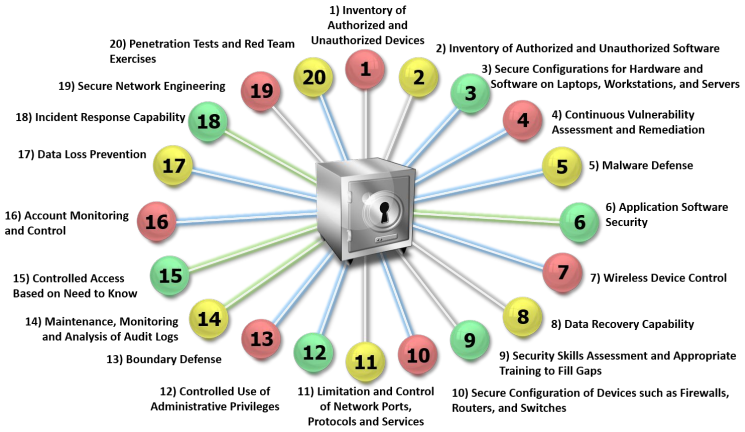
La valorizzazione del patrimonio informativo pubblico è un obiettivo strategico per la Pubblica Amministrazione. Per sfruttare le potenzialità dell'immenso patrimonio dei dati raccolti e gestiti dalle PA è necessario attuare un cambio di paradigma nella loro gestione che consenta di superare la "logica a silos" in favore di una visione sistemica

Si introduce una **cultura della gestione del rischio** all'interno dell'organizzazione per combattere la minaccia cyber.

Questo significa che ogni organizzazione deve necessariamente impiegare risorse umane interne a difesa dei propri asset. Questo personale deve definire e perseguire politiche di sicurezza adattabili nel tempo e in grado di trovare un equilibrio tra investimenti e rischio residuo, congeniale rispetto alla esposizione dell'organizzazione alla minaccia cyber.

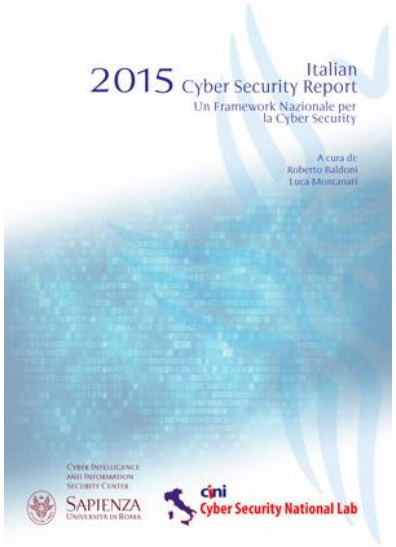
CIRCOLARE AgID - RIFERIMENTI

Critical Controls for Effective Cyber Defense v6 2015



CIS CENTER INTERNET SECURITY

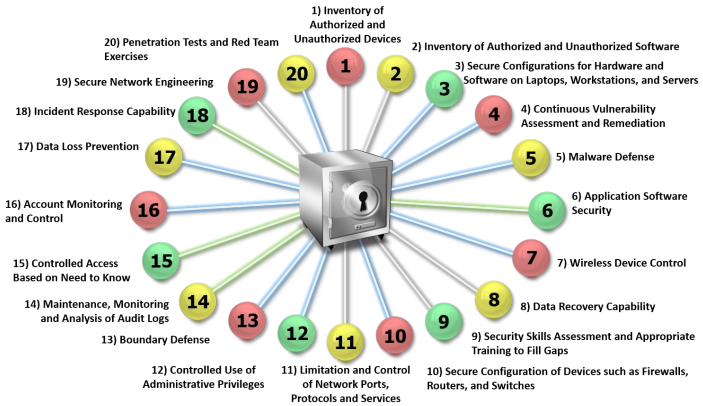
Framework Nazionale per la Cyber Security (FNCS)



FONDAZIONE
CONSIGLIO NAZIONALE INGEGNERI

SANS20

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software on Mobile Devices, Laptop, Workstations, and Servers
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises



FNSC 15 Controlli Essenziali di cybersecurity

1. Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.
2. I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc. . .) offerti da terze parti a cui si è registrati sono quelli strettamente necessari.
3. Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.
4. È stato nominato un referente che sia Responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.
5. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.
6. Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.
7. Le password sono diverse per ogni account, dalla complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).

FNSC 15 Controlli Essenziali di cybersecurity

8. Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati.
9. Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.
10. Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, . . .). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.
11. La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, Responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.
12. Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono conservati in modo sicuro e verificati periodicamente.
13. Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione).
14. In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.
15. Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.

FNSC tematiche di sicurezza

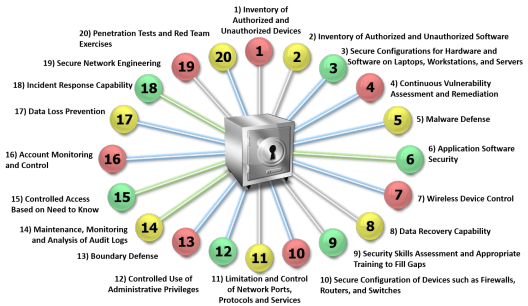
La guida è organizzata in 8 tematiche di sicurezza:

1. Inventario dispositivi e software (Sezione 3.1); “Inventario dispositivi e software” e la Category “Asset Management ID.AM”
2. Governance (Sezione 3.2); “Governance” e la Category “Governance ID.GV”
3. Protezione da malware (Sezione 3.3); ID.CM -“Protezione da Malware” e la Category “Security Continuous Monitoring DE.CM”
4. Gestione password e account (Sezione 3.4); “Gestione password e account” e la Category “Access Control PR.AC”
5. Formazione e consapevolezza (Sezione 3.5); “Formazione e Consapevolezza” e la Category “Awareness and Training PR.AT”
6. Protezione dei dati (Sezione 3.6); “Protezione dei dati” e la Category “Information Protection Processes and Procedures PR.IP”
7. Protezione delle reti (Sezione 3.7); “Protezione delle reti” e la Category “Protective Technology PR.PT”
8. Prevenzione e mitigazione (Sezione 3.8). “Prevenzione e mitigazione” e la Category “Mitigation RS.MI”

CIRCOLARE AgID P.A.

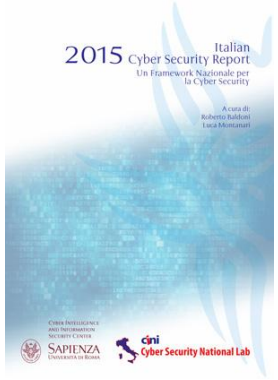
CCSC

CIS Critical Security Control for effective cyber defense



FNSC

(Framework Nazione di Sicurezza Cibernetica)



AgID

ABSC

(AgID Basic Security Control)

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

FONDAZIONE
CONSIGLIO NAZIONALE INGEGNERI

CIRCOLARE AgID P.A.

AgID ha predisposto un documento che contiene l’elenco ufficiale delle “Misure minime per la sicurezza ICT delle pubbliche amministrazioni" al fine di fornire alle pubbliche amministrazioni un riferimento pratico per valutare e migliorare il proprio livello di sicurezza informatica.

Le misure minime di sicurezza informatica prevedono tre diversi livelli di attuazione e costituiscono parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione.

L’obiettivo del documento è quello di fornire tempestivamente alle PA un riferimento normativo e consentire loro di intraprendere un percorso di progressiva verifica e adeguamento in termini di sicurezza informatica.

CIRCOLARE AgID P.A.

AG.I.D.
AGENZIA PER L'ITALIA DIGITALE

FONDAZIONE
CONSIGLIO NAZIONALE INGEGNERI

AgID

ABSC 1(CSC 1):	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	rilevazione delle anomalie operative
ABSC 2 (CSC 2)	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	rilevazione delle anomalie operative
ABSC 3 (CSC 3)	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	protezione della configurazione corrente
ABSC 4 (CSC 4)	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	protezione scalabilità accessi
ABSC 5 (CSC 5)	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	protezione accessi
ABSC 8 (CSC 8	DIFESE CONTRO I MALWARE	gestione codici malevoli (inserimento, esecuzione)
ABSC 10 (CSC 10	COPIE DI SICUREZZA	ripristino dopo un incidente.
ABSC 13 (CSC 13)	PROTEZIONE DEI DATI	ripristino dopo un incidente.

Classi di controlli 1 - 3

Nella circolare ci sono 8 classi di controlli che le PA devono effettuare:

- **ABSC1**(CSC1): **inventario dei dispositivi autorizzati e non autorizzati.** Il livello minimo prevede l'implementazione, l'aggiornamento e la gestione dell'inventario di tutti i sistemi di rete (compresi i dispositivi di rete stessi) registrando almeno l'indirizzo IP.
- **ABSC2**(CSC2): **inventario dei software autorizzati e non autorizzati.** Il livello minimo prevede la realizzazione dell'elenco dei software autorizzati (e relative versioni), con regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzati. L'installazione di software non presenti nell'elenco è vietata.
- **ABSC3**(CSC3): **proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server.** Il livello minimo di questa classe di controlli prevede le definizione di configurazioni standard per tutti i sistemi (server, workstation, ecc.), con il tassativo rispetto di tali standard nelle fasi di installazione o ripristino dei sistemi. Le immagini di installazione dei sistemi devono essere memorizzate offline e tutte le operazioni di amministrazione remota devono essere eseguite tramite connessioni protette.

Classi di controlli 4 - 6

- **ABSC4**(CSC4): **valutazione e correzione continua della vulnerabilità.** Il livello minimo prevede la ricerca delle vulnerabilità tramite strumenti automatici ad ogni modifica della configurazione; detti strumenti devono fornire agli amministratori di sistema report con indicazione delle vulnerabilità più critiche. Non solo i sistemi devono essere aggiornati, ma anche gli stessi strumenti di scansione.
- **ABSC5**(CSC5): **uso appropriato dei privilegi di amministratore**. Il livello minimo della classe di controlli relativa agli amministratori di sistema definisce una specifica policy di gestione degli utenti con diritti amministrativi, che disciplini i limiti nei privilegi attribuiti e l'inventario dei profili abilitati. Tale policy prevede tutte le accortezze che si rendono necessarie per l'adeguata gestione degli amministratori di sistema, dai controlli sulle scadenze delle password alla creazione di profili nominativi e individuali (non generici). Per questa classe di controlli, le azioni relative al tracciamento dei log degli amministratori sono definite come livello "standard", mentre rappresentano un obbligo di legge sancito da un provvedimento del Garante Privacy sugli amministratori di sistema del 2008.
- **ABSC8**(CSC8): **difese contro i malware**. Il livello minimo impone l'installazione e l'aggiornamento automatico di sistemi antimalware, firewall e Intrusion Prevention Systems (IPS). Si deve disabilitare inoltre l'esecuzione automatica di tutti quei sistemi che potrebbero inavvertitamente attivare una minaccia (es. apertura degli allegati delle email, esecuzione di macro, eseguibili lanciati da chiavette USB, ecc).

Classi di controlli 7 - 8

- **ABSC10**(CSC10): **copie di sicurezza**. Il livello minimo di sicurezza contempla una copia almeno settimanale delle informazioni strettamente necessarie per il completo ripristino del sistema (in linea con le misure minime di sicurezza previste dal Codice della Privacy, anche se perdere una settimana di lavoro potrebbe essere troppo penalizzante per una PA). Si pone una certa attenzione anche alla riservatezza delle informazioni contenute nelle copie di sicurezza, tramite adeguata protezione fisica o mediante cifratura delle informazioni sottoposte a salvataggio. Infine, è necessario garantire che almeno una delle copie non sia permanentemente accessibile dal sistema stesso, onde evitare che eventuali attacchi al sistema possano coinvolgere anche le sue copie di sicurezza.
- **ABSC13**(CSC13): **protezione dei dati**. Il livello minimo da garantire stabilisce di effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza, ai quali applicare una protezione crittografica. Inoltre, si deve prevedere il blocco del traffico da e verso url presenti in una blacklist.

Livelli di sicurezza

Vengono introdotti dei controlli denominati ABSC (AgID *Basic Security Controls*) che dovrebbero essere implementati per ottenere un determinato livello di sicurezza.

Si identificano 3 livelli di sicurezza:

– “Minimo”, al di sotto il quale nessuna amministrazione può scendere;

– “Standard”, che costituisce la base di riferimento nella maggior parte dei casi;

– “Alto”, che potrebbe essere un obiettivo a cui tendere.

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

ABSC		ID #	Descrizione	FNSC	Min.	Std.	Alto
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		X	X
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ID.AM-1			X
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	ID.AM-1			X
	2	1	Implementare il "logging" delle operazione del server DHCP.	ID.AM-1		X	X
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	ID.AM-1		X	X
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X
	4	1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	ID.AM-1	X	X	X
		2	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	ID.AM-1		X	X
		3	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	ID.AM-1			X

classe di controllo

livello di sicurezza

Allegato B

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 da solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4		M
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico		S
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.		A
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.		A
	2	1	Implementare il "logging" delle operazione del server DHCP.		S
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.		S
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.		M
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in		S

Minimo

Standard

Alto

Alto

...

FONDAZIONE
CONSIGLIO NAZIONALE INGEGNERI

STAY
PARANOID
AND
STAY
HUNGRY

3° modulo
“Aspetti tecnici-operativi per **l’attuazione** delle misure minime di sicurezza ICT”

alessio chiga

FONDAZIONE
CONSIGLIO NAZIONALE INGEGNERI

cybersecurity e PA

La circolare AgID 2/2017 che stiamo analizzando, si propone di implementare una serie di controlli che possano aiutare la Pubblica Amministrazione a limitare al minimo i disservizi creati da problemi di sicurezza informatica.

La cybersecurity è diventato, quindi, argomento fondamentale da tenere in conto quando si lavora su un sistema composto di apparati informatici.

Cercheremo di capire come poter attuare il protocollo specificato nella circolare AgID con l'ausilio di un esempio.

Modulo di implementazione delle misure minime di sicurezza per le Pubbliche Amministrazioni

- **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

Ordine di esempio

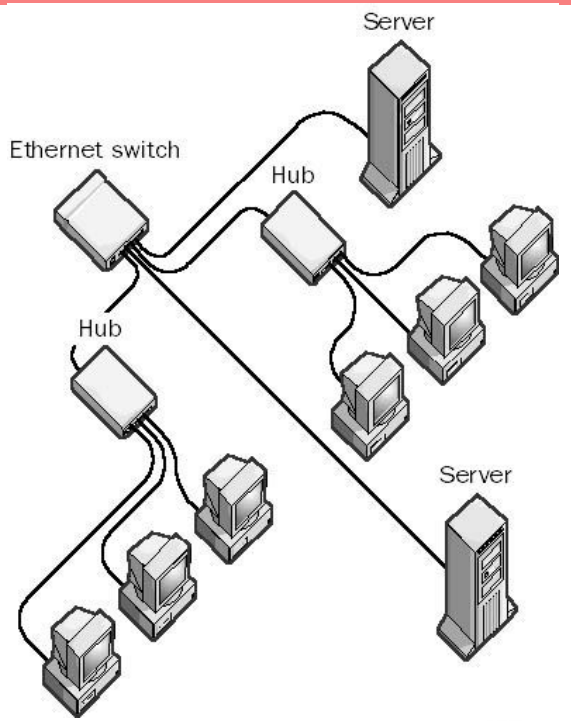
personale dell'Ordine:

- 1 presidente
- 1 segretario
- 6 dipendenti
- 2 consulenti esterni

Ordine di esempio

dispositivi utilizzati dall'Ordine:

- 1 Firewall
- 1 Access point
- 1 Server
- 1 NAS
- 10 computer
- 3 Tablet
- 6 Smartphone per utilizzo dell'ente
- 10 pendrive USB



Ordine di esempio

servizi utilizzati dall'Ordine:

servizi interni

- gestione documentale
- software amministrativi
- software office automation
- sistema di backup
- gestione albo

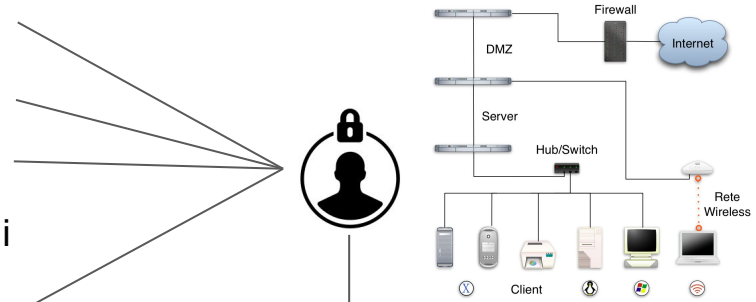
servizi esterni

- sito web
- mail
- fatture elettroniche
- gestione albo

Ordine di esempio

info esterne alla rete locale

- 1 presidente
- 1 segretario
- 6 dipendenti
  - segretaria
  - ragioniere
- 2 consulenti esterni



SERVIZIO ESTERNO
gestito da società esterna o risorsa interna Ordine

iscritto

Allegato B

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 da solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4		M
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico		S
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.		A
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.		A
	2	1	Implementare il "logging" delle operazione del server DHCP.		S
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.		S
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.		M
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.		S

FONDAZIONE
CONSIGLIO NAZIONALE INGEGNERI

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Tutti i dispositivi collegati in rete sono gestiti con un sistema di inventario automatico che si aggiorna automaticamente tramite client installato su ogni dispositivo.

Ogni dispositivo invia almeno giornalmente al sistema centrale l'elenco di tutte le periferiche collegate e l'indirizzo IP; invia inoltre l'indicazione di nuovi dispositivi collegati alla rete.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

Tutti i dispositivi collegati in rete sono gestiti con un sistema di inventario automatico dei software che si aggiorna automaticamente tramite client installato su ogni dispositivo.

Ogni dispositivo invia almeno giornalmente al sistema centrale l'elenco di tutti i software installati corredati del numero di versione.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

Tutte le macchine in rete (compresi server e workstation) utilizzano configurazioni base standard che permettono il veloce ripristino del sistema in caso di compromissione.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

Tutte le macchine in rete devono essere costantemente aggiornate per limitarne le vulnerabilità.

Tutti gli strumenti di scansione delle vulnerabilità devono essere aggiornati automaticamente, come anche i sistemi operativi.

Prevedere un software di scansione delle vulnerabilità centralizzato può semplificare la gestione da parte di un amministratore che deve aggiornare i sistemi quando non è possibile farlo automaticamente.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Tutti i sistemi in rete sono utilizzati con un account non amministrativo, ad esclusione di necessità di interventi mirati (aggiornamento del sistema, installazione di nuovi software, ecc.).

Le credenziali amministrative devono avere password robuste e devono essere aggiornate regolarmente evitando il riutilizzo nel corso del tempo.

Le credenziali amministrative devono essere disponibili al Responsabile ICT per coprire eventuali assenze dei responsabili.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

Tutte le macchine in rete sono controllate da software antivirus e antimalware per la ricerca di vulnerabilità.

Tutti gli antivirus e antimalware sono aggiornati automaticamente, come anche i sistemi operativi.

Prevedere un antivirus/antimalware centralizzato può semplificare la gestione da parte di un amministratore.

Tutti i sistemi di avvio automatico dei file e di lettura automatica dei contenuti devono essere disattivati e deve essere inoltre filtrato il traffico web.

ABSC 10 (CSC 10): COPIE DI SICUREZZA

L’archivio dei documenti è centralizzato (su un sistema di storage) e di questo deve essere effettuata una copia di backup almeno settimanalmente.

I backup devono essere cifrati per poter essere archiviati anche su cloud così da consentire un ripristino anche in caso di incidente grave presso la sede della PA.

Le copie di backup non devono essere costantemente accessibili in rete per evitare che attacchi a sistema possano compromettere tutte le copie di backup.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

La protezione dei dati deve essere strutturata per far sì che i dati rilevanti non siano accessibili in modalità semplice; a tal proposito è necessario cifrare i dati con una protezione crittografica.

I sistemi portatili (laptop, telefoni, tablet) devono avere una protezione crittografica.

È necessario bloccare l'accesso verso determinate URL tramite una blacklist (a livello centrale).

QUANTO COSTA?

Non è possibile definire un costo standard per l'implementazione delle specifiche contenute all'interno della circolare AgID perché ogni situazione deve essere analizzata nelle sue specificità. Possiamo dire che una stima dei costi dei Controlli Essenziali (Minimi) può essere di 2 tipi:

- costi una tantum
- costi ricorrenti

I costi **una tantum** sono quelli relativi all'acquisto di software e hardware e per il recovery post incidente.

I costi **ricorrenti** sono quelli per il mantenimento di licenze, le consulenze, la formazione del personale.

QUANTO COSTA?

Basandoci sull'esempio che stiamo sviluppando, le attività rese necessarie all'implementazione delle misure minime dell'AgID sono state:

- server da usare come sistema di virtualizzazione
- NAS per i backup interni
- licenze antivirus centralizzate
- predisposizione di un sistema centralizzato di utenze e ACL (dominio o LDAP)
- configurazione delle postazioni
- formazione del personale.

Stima dei costi dei Controlli Essenziali - CSR

Secondo il Cyber Security Report La Sapienza un costo stimato per una piccola organizzazione (Ordine Professionale nel nostro caso) si aggira intorno ai 10.500,00 € per il primo anno contro un "danno medio stimato" di 35.000,00 € per anno.

- Stima costi una tantum: 2.700,00 €
- Stima costi ricorrenti: 7.800,00 €

Per un Ordine delle dimensioni prese ad esempio si può così schematizzare:

- spese iniziali + spese ricorrenti annuali × 5 anni = 41.450,00 €;
- danno medio stimato su 5 anni = 175.000,00 €;
- investimento inferiore del 76% rispetto al danno stimato.

FONTE: Cyber Security Report La Sapienza - 2015 Italian Cyber Security Report del CIS

4° modulo “Domande e dibattito”

elisabetta canali

alessio chiga

marcello coiana

FONDAZIONE
CONSIGLIO NAZIONALE INGEGNERI

GRAZIE PER L’ATTENZIONE