POWERCON2020

Come adeguare l'infrastruttura IT a normative regolamenti per la sicurezza ICT

Ermanno Goletto

Microsoft MVP Reconnect

@ermannog

www.devadmin.it

Roberto Massa

Microsoft MVP Reconnect

@robi_massa

massarobi.wordpress.com

Agenda

- Overview
- Indicazioni tecniche nel GDPR (Regolamento 2016/679)
- Misure minime di sicurezza ICT per le pubbliche amministrazioni

Torino Technologies Group

Overview

Come adeguare l'infrastruttura IT a normative regolamenti per la sicurezza ICT

Cybersecurity e riferimenti normativi

D. Lgs. **196/2003** *Codice in materia di protezione dei dati personali*

D. Lgs. **259/2003** *Codice delle Comunicazioni elettroniche*

D. Lgs. **82/2005** *Codice dell'amministrazione digitale* successivamente integrato e modificato dai D. Lgs. 179/2016 e 217/2017

DPCM 24 gennaio **2013** *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* e *Piano nazionale per la protezione cibernetica e la sicurezza informatica*

Direttiva 1 agosto **2015** del Presidente del Consiglio dei Ministri *Attuazione degli indirizzi strategici ed operativi del DPCM 24 gennaio 2013*

GU Serie Generale n.103 del 05-05-**2017** *Misure minime di sicurezza ICT per le pubbliche amministrazioni* redatte da AgID

D. Lgs. **51/2018** *Attuazione della direttiva (UE) 2016/680 Regolamento generale sulla protezione dei dati*

D. Lgs. **65/2018** *Attuazione della direttiva (UE) 2016/1148 Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione* (Direttiva NIS)

D. Lgs. **101/2018** *Disposizioni per l'adeguamento della normativa nazionale (196/2003) alle disposizioni del regolamento (UE) 2016/679*

D. Lgs. **105/2019** *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*

2002 — Direttiva 2002/58/CE Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche

2004 — Regolamento 2004/460 European Network and Information Security Agency (ENISA)

2013 — Piano di sicurezza informatica dell'UE per garantire un elevato livello di *network and information security* (NIS)

2015 — Accordo sulla prima normativa UE relativa alla cybersecurity (NIS)

2016 — Regolamento 2016/679 (GDPR) Direttiva 2016/1148 (NIS)

2017 — Adozione di un cybersecurity package per garantire resilienza, deterrenza e difesa Proposta di creazione di un cybersecurity certification framework

2019 — Regolamento 2019/881 (Cybersecurity Act) Regolamento per la certificazione della sicurezza informatica di prodotti ICT e servizi digitali

CERT Nazionale, CERT-PA e CSIRT

- *Individuato presso il **Ministero dello sviluppo economico** ai sensi dell'art. 16 bis del d.lgs. 259/2003 (Codice delle Comunicazioni elettroniche)*
- ***Attivo dal 5 giugno 2014** presso l'Istituto Superiore delle comunicazioni e delle tecnologie, opera **a supporto di Cittadini ed Imprese***
- *Fornisce **informazioni su potenziali minacce informatiche**, **raccomandazioni**, **consigli** e **contromisure** per la prevenzione e la risoluzione di incidenti informatici*
- *Opera sulla base di un **modello cooperativo pubblico-privato** e collabora con CERT-PA, CSIRT, CERT Difesa, CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche), CERT EU, CERT extra UE e importanti imprese che gestiscono infrastrutture informatizzate*

- *Opera all'interno di **AgID** in linea con il modello organizzativo previsto dal DPCM 24 gennaio 2013 (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale)*
- ***Attivo dal 3 marzo 2014**, opera **a supporto delle Pubbliche Amministrazioni***
- ***Attivo dal 3 marzo 2014**, fornisce alle PA richiedenti supporto per la **definizione dei processi di gestione della sicurezza**, **bollettini** e **segnalazioni di sicurezza**, **gestione di allarmi di sicurezza** e **formazione***

- *Costituito presso la **Presidenza del Consiglio dei Ministri** ai sensi del d.lgs 65/2018 (Attuazione Direttiva UE NIS 2016/1148) mediante unificazione del CERT Nazionale e del CERT-PA*
- *Entro il **9 novembre** sarà adottato un provvedimento definirà la sua organizzazione*
- ***CERT Nazionale** e **CERT-PA** nella frattempo assolvono congiuntamente il ruolo e le funzioni del CSIRT Italiano, ovvero **continuano a svolgere compiti di prevenzione e risposta ad incidenti informatici** e congiuntamente **gestiscono le notifiche di incidenti informatici**, che nella fase transitoria hanno carattere obbligatorio solo per i fornitori di servizi digitali*

Normative e linee guida ICT italiane

Piano Triennale per l'informatica nella Pubblica Amministrazione

- Il modello di Cloud della PA
- Censimento ICT
- Linee Guida Modello Interoperabilità
- Piano triennale ICT
- Codice dell'amministrazione digitale (CAD)

CAD (D. Lgs. 82/2005)

Testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese

Framework Nazionale per la Cybersecurity e la Data Protection

Strumento di supporto alle organizzazioni che necessitano di strategie e processi volti alla protezione dei dati personali e alla sicurezza cyber

Misure minime di sicurezza ICT per le pubbliche amministrazioni

Misure emanate dall'AgID che costituiscono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti

Torino Technologies Group

Indicazioni tecniche nel GDPR

Come adeguare l'infrastruttura IT a normative regolamenti per la sicurezza ICT

Articolo 17 Paragrafo 1 e 2

Diritto alla cancellazione («diritto all'oblio») (C65, C66)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

   a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
   b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
   c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
   d) i dati personali sono stati trattati illecitamente;
   e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
   f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Eliminazione dati

Backup e diritto all'oblio

- L'autorità danese Data Inspectorate afferma che la cancellazione dei dati dei record dai backup è obbligatoria "se ciò è tecnicamente possibile"

- Secondo l'autorità francese CNIL (Commission Nationale Informatique et Libertés) le organizzazioni non devono necessariamente eliminare i backup a fronte di una richiesta di cancellazione. Tuttavia, le organizzazioni dovranno spiegare chiaramente all'interessato (usando un linguaggio semplice e chiaro) che i suoi dati personali sono stati rimossi dai sistemi di produzione, ma una copia di backup potrebbe rimanere, e scadrà dopo un certo periodo di tempo (il tempo di conservazione va indicato nella comunicazione con l'interessato)

- Altre autorità di controllo potrebbero avere una posizione in merito differente e più rigida

- Per essere in grado di dimostrare che non è pratico eliminare i dati di backup bisogne condurre una valutazione del rischio e una valutazione d'impatto sul business

- Occorre documentare le politiche e le procedure per mantenere sicuri i dati di backup, con apposite istruzioni sulla crittografia dei backup e sul luogo di mantenimento dei dispositivi di backup

https://www.garanteprivacy.it/temi/diritto-all-oblio

https://blog.quantum.com/backup-administrators-the-1-advice-to-deal-with-gdpr-and-the-right-of-erasure

https://www.cybersecurity360.it/legal/privacy-dati-personali/backup-e-diritto-alloblio-alla-luce-del-gdpr/

Articolo 19

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (C31)

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Notifica

Articolo 20

Diritto alla portabilità dei dati (C68)

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
   a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
   b) il trattamento sia effettuato con mezzi automatizzati.
2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Formato dati di uso comune

Trasmissione diretta dei dati

Articolo 21

Diritto di opposizione (C69, C70)

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.
4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Blocco del trattamento dei dati

Articolo 22

Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione (C71, C72)

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il paragrafo 1 non si applica nel caso in cui la decisione:

    a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
    b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
    c) si basi sul consenso esplicito dell'interessato.

3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Bypass decisioni automatizzate

Articolo 25

Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita (C75-C78)

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Pseudonimizzazione	Trattamento dei soli dati necessari	Accessibilità limitata

Articolo 32 Paragrafo 1

Sicurezza del trattamento (C83)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della **natura**, dell'**oggetto**, del **contesto** e delle **finalità del trattamento**, come anche del **rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche**, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:

a) la **pseudonimizzazione e la cifratura** dei dati personali;

b) la **capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento**;

c) la **capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico**;

d) una **procedura per testare**, **verificare** e **valutare regolarmente l'efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.

Pseudonimizzazione e Cifratura | Riservatezza, Integrità, Disponibilità e Resilienza | Ripristino

Articolo 32 Paragrafi 2,3,4

Sicurezza del trattamento (C83)

2. Nel valutare l'adeguato livello di sicurezza, **si tiene conto** in special modo dei **rischi presentati dal trattamento** che derivano in particolare dalla **distruzione**, dalla **perdita**, dalla **modifica**, dalla **divulgazione non autorizzata** o dall'**accesso**, in modo **accidentale o illegale**, a dati personali trasmessi, conservati o comunque trattati.
3. L'**adesione a un codice di condotta** approvato di cui all'articolo 40 o a un **meccanismo di certificazione approvato** di cui all'articolo 42 può essere utilizzata come **elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1** del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Valutazione livello sicurezza

Istruzione

Articolo 33 Paragrafi 1, 2

Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Monitoraggio

Rilevamento, Correlazione e Analisi

Articolo 33 Paragrafi 3, 4, 5

Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)

3. La notifica di cui al paragrafo 1 deve almeno:
   a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
   b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
   c) descrivere le probabili conseguenze della violazione dei dati personali;
   d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Incident Report | Post-Incident Activity

Articolo 34

Comunicazione di una violazione dei dati personali all'interessato (C86-C88)

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
   a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
   b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
   c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Cifratura

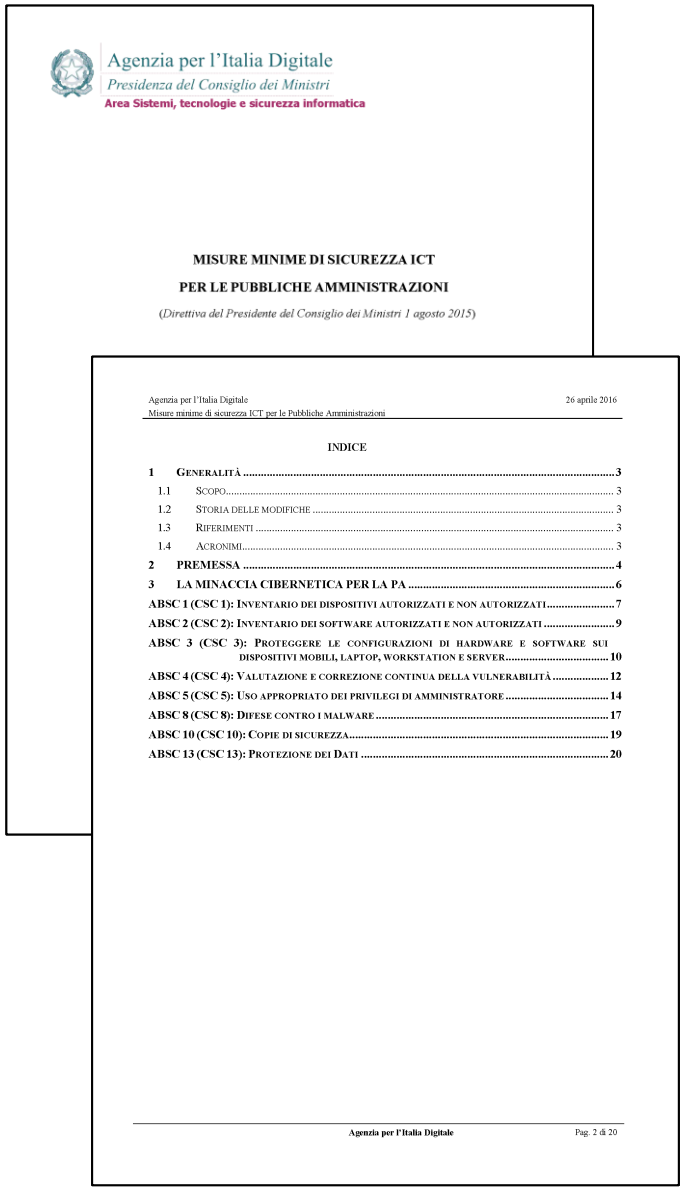
Contenimento, Sradicamento e Ripristino

Torino Technologies Group

Misure minime di sicurezza ICT per le pubbliche amministrazioni

Come adeguare l'infrastruttura IT a normative regolamenti per la sicurezza ICT

Overview



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)

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

INDICE

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 per tutte le PP. AA.

Adeguamenti entro il 31/12/2017

- Basate sull'insieme di controlli SANS 20, pubblicato dal Center for Internet Security come CCSC «CIS Critical Security Controls for Effective Cyber Defense» versione 6.0 ottobre 2015
- Il SANS20 è un elenco composto da venti controlli, denominati Critical Security Control (CSC), ordinato sulla base dell'impatto sulla sicurezza dei sistemi
- Ciascun controllo precede tutti quelli la cui implementazione innalza il livello di sicurezza in misura inferiore alla sua
- Nell'identificazione degli ABSC ci si è riferiti alla versione 6 dei CCSC. Tuttavia l'insieme dei controlli definiti è più vicino a quello della versione 5.1 poiché AgID ha ritenuto che molti dei controlli eliminati nel passaggio alla nuova versione anche se non più attuali nella realtà statunitense, sono ancora importanti nel contesto della pubblica amministrazione italiana

Strutturazione delle Misure minime di sicurezza ICT

- Il CCSC è stato concepito essenzialmente nell'ottica di prevenire e contrastare gli attacchi cibernetici, non viene data particolare rilevanza agli eventi di sicurezza dovuti a casualità quali guasti ed eventi naturali
- Ai controlli delle prime cinque classi AgID ha deciso di aggiungere quelli relativi alle difese contro i malware (CSC8), quelli delle alle copie di sicurezza (CSC10) e quelli riferiti alla protezione dei dati rilevanti contro i rischi di esfiltrazione (CSC13)
- Ciascun CSC è costituito da una famiglia di misure di dettaglio più fine che possono essere adottate in modo indipendente, AgID ha ritenuto che anche al secondo livello ci fosse una granularità ancora eccessiva, che avrebbe costretto le piccole amministrazioni ad introdurre misure esagerate per la propria organizzazione
- E' stato introdotto un ulteriore terzo livello nel quale la misura di secondo livello viene decomposta in misure elementari implementabili in modo indipendente
- Un ABSC è identificato da un identificatore gerarchico a tre livelli x, y, z
  - x e y sono i numeri che identificano il CSC corrispondente
  - z individua ciascuno dei controlli di livello 3
- Le Misure minime di sicurezza ICT sono composte da 8 ABSC che sono derivati dai CSC 1,2,3,4,5,8,10 e 13
- Viene indicato quali controlli implementare per ottenere un determinato livello di sicurezza:
  - «Minimo» specifica il livello sotto il quale nessuna amministrazione può scendere, i controlli in essa indicati debbono riguardarsi come obbligatori
  - «Standard» può essere assunta come base di riferimento nella maggior parte dei casi
  - «Alto» può essere considerata come un obiettivo a cui tendere
- Le amministrazioni NSC (Nucleo di Sicurezza Cibernetica), per l'infrastruttura che gestisce dati NSC, dovrebbero collocarsi almeno a livello "standard" in assenza di requisiti più elevati

Formato delle Misure minime di sicurezza ICT

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.

3 livelli

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
10	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	PR.IP-4	X	X	X
		2	Per assicurare la capacità di … devono riguardare il sistem…	PR.IP-4			X
		3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	PR.IP-4			X
	2	1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	PR.IP-4		X	X
	3	1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud. .	PR.DS-6	X	X	X
	4	1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	PR.AC-2 PR.IP-4 PR.IP-5 PR.IP-9	X	X	X

Subcategory del Framework Core del Framework nazionale per la Cyber Security

Livello di sicurezza

ABSC 1 (CSC 1)

Inventario dei dispositivi autorizzati e non autorizzati

1.1.1 Inventario delle risorse attive | 1.1.2 Inventario automatizzato | 1.1.3 Discovery dispositivi in rete con allarmi su anomalie

1.1.4 Qualificazione sistemi in rete tramite analisi del traffico

1.2.1 Logging DHCP | 1.2.2 Utilizzo Logging DHCP per migliorare inventario

1.3.1 Aggiornare l'inventario quando sono connessi nuovi dispositivi approvati

1.3.2 Inventario automatizzato automaticamente quando sono connessi nuovi dispositivi approvati

1.4.1 Registrare indirizzo IP di tutti i sistemi e dispositivi in rete

1.4.2 Registrare hostname, funzione, responsabile, ufficio, tipologia (portatile/personale) dei dispositivi con indirizzo IP

1.4.3 Identificare telefoni cellulari, tablet, laptop e altri dispositivi portatili che memorizzano o elaborano dati

1.5.1 Autenticazione a livello di rete 802.1x correlata all'inventario per distinguere i sistemi autorizzati

1.6.1 Certificati lato client per validare e autenticare i sistemi prima della connessione alla rete locale

ABSC 2 (CSC 2):

Inventario dei software autorizzati e non autorizzati

2.1.1 Elenco software autorizzati con versione per tipo di sistema, non consentire installazione software non in elenco

2.2.1 "Whitelist" (anche ampia) applicazioni autorizzate, bloccare esecuzione software non lista

2.2.2 "Whitelist" mirata per sistemi con funzioni specifiche

2.2.3 Verifica integrità file applicazioni in "whitelist" per verificare che non siano state modificate

2.3.1 Scansioni regolari per rilevare presenza software non autorizzato

2.3.2 Inventario software completo

2.3.3 Inventario software automatizzato che registri versione OS, applicazioni installate e livello patch

2.4.1 VM e/o sistemi air-gapped (isolati) per eseguire applicazioni dedicate a operazioni strategiche o critiche

ABSC 3 (CSC 3)

Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server

3.1.1 Utilizzo di configurazioni sicure standard

3.1.2 Configurazioni sicure standard "hardened" OS/applicazioni (eliminazione account utente/servizio non necessari, disattivazione/eliminazione servizi non necessari, configurazione stack/heaps non eseguibili, applicazione patch, chiusura porte di rete non utilizzate

3.1.3 Validazione/aggiornamento regolare immagini d'installazione

3.2.1 Definizione configurazione standard per tutti i tipi di sistema

3.2.2 Ripristino sistemi compromessi con configurazione standard

3.2.3 Procedure gestione cambiamenti per modifiche a configurazione standard

3.3.1 Immagini installazione memorizzate offline

3.3.2 Conservazione protetta immagini installazione (integrità/accesso protetto)

3.4.1 Eseguire amministrazione remota su connessioni protette (protocolli sicuri/canali protetti)

3.5.1 Verifica integrità file critici di sistema, eseguibili sistema/applicazioni, librerie, configurazioni

3.5.2 Verifica integrità file automatica e alert su alterazione

3.5.3 Cronologia modifica configurazione e identificazione autore

3.5.4 identificare alterazioni sospette sistema, permessi file/cartelle

3.6.1 Sistema centralizzato controllo automatico configurazioni

3.7.1 Strumenti per ripristino impostazioni configurazioni standard

Livello sicurezza Minimo | Livello sicurezza Standard | Livello sicurezza Alto

ABSC 4 (CSC 4) 1/2

Valutazione e correzione continua della vulnerabilità

4.1.1 Ricerca automatica vulnerabilità ad ogni modifica significativa della configurazione di tutti i sistemi in rete

4.1.2 Ricerca periodica vulnerabilità (frequenza commisurata complessità dell'infrastruttura)

4.1.3 Utilizzo SCAP (Security Content Automation Protocol) per validazione vulnerabilità basate sul codice e configurazione

4.2.1 Correlazione log di sistema - scansioni delle vulnerabilità

4.2.2 Verificare che i log registrino attività di scanning delle vulnerabilità

4.2.3 Verificare che i log registrino gli attacchi

4.3.1 Eseguire scansioni vulnerabilità locali/remote con account dedicato

4.3.2 Eseguire scansioni vulnerabilità da host/IP specifici

4.4.1 Aggiornare gli strumenti di scansione delle vulnerabilità

4.4.2 Registrazione a servizio che fornisce informazioni tempestive su nuove minacce/vulnerabilità e utilizzarle nelle scansioni

4.5.1 Installazione automatica patch/aggiornamenti per software/OS

4.5.2 Aggiornare sistemi separati dalla rete/air-gapped in base al loro livello di criticità

Livello sicurezza Minimo | Livello sicurezza Standard | Livello sicurezza Alto

ABSC 4 (CSC 4) 2/2

Valutazione e correzione continua della vulnerabilità

4.6.1 Verifica che le scansioni siano eseguite con policy predefinite

4.7.1 Verifica risoluzione vulnerabilità emerse (patch, contromisure documentazione accettazione rischio)

4.7.2 Revisione periodica delle accettazioni dei rischi di vulnerabilità

4.8.1 Definizione piano gestione rischi

4.8.2 Attribuire alle azioni per risoluzione vulnerabilità un livello di priorità in base al rischio

4.9.1 Misure alternative se non è possibile risolvere la vulnerabilità

4.10.1 Ambiente test per patch software non standard (xes. ad hoc)

ABSC 5 (CSC 5) 1/2

Uso appropriato dei privilegi di amministratore

5.1.1 Limitare privilegi di amministrazione ai soli utenti necessari

5.1.2 Utilizzo utenze amministrative solo quando necessario

5.1.3 Assegnare agli utenti amministratori solo i privilegi necessari

5.1.4 Log attività utenze amministrative e rilevare anomalie

5.2.1 Inventario utenze amministrative

5.2.2 Automazione inventario utenze amministrative e alert variazioni

5.3.1 Cambio credenziali amministrative predefinite dei dispositivi connessi in rete

5.4.1 Log aggiunta/soppressione utenza amministrativa

5.4.2 Alert aggiunta utenza amministrativa

5.4.3 Alert aumento privilegi utenza amministrativa

5.5.1 Log accessi falliti da utenze amministrative

5.6.1 Utilizzo sistemi di autenticazione a più fattori per tutti gli accessi amministrativi

5.7.1 Se l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali robuste (almeno 14 caratteri)

5.7.2 Impedire utilizzo credenziali amministrative deboli

5.7.3 Assicurarsi che credenziali delle utenze amministrative vengano sostitute con sufficiente frequenza (password aging)

5.7.4 Impedire riutilizzo credenziali utenze amministrative a breve distanza di tempo (password history)

5.7.5 Consentire modifica credenziali amministrative dopo un lasso di tempo sufficiente

5.7.6 Impedire riutilizzo credenziali amministrative prima di 6 mesi

Livello sicurezza Minimo | Livello sicurezza Standard | Livello sicurezza Alto

ABSC 5 (CSC 5) 2/2

Uso appropriato dei privilegi di amministratore

5.8.1 Impedire accesso diretto ai sistemi con utenze amministrative, obbligare gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi

5.9.1 Utilizzare per operazioni amministrative macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet

5.10.1 Credenziali distinte utenze privilegiate e non privilegiate degli amministratori

5.10.2 Tutte le utenze devono essere nominative e riconducibili ad una sola persona, in particolare quelle amministrative

5.10.3 Le utenze amministrative anonime («root», «administrator») devono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso

5.10.4 Evitare uso utenze amministrative locali quando sono disponibili utenze amministrative di livello più elevato (xes. dominio)

5.11.1 Conservare le credenziali amministrative garantendo disponibilità e riservatezza

5.11.2 Se si utilizzano certificati digitali per l'autenticazione, garantire adeguata protezione per le chiavi private

ABSC 8 (CSC 8) 1/2

Difese contro i malware

8.1.1 Installare su tutti i sistemi della rete locale antivirus e mantenerli aggiornati automaticamente

8.1.2 Installare su tutti i dispositivi firewall ed IPS personali

8.1.3 Inviare e archiviare gli eventi in un repository centrale (syslog)

8.2.1 Gli antivirus, firewall e IPS devono essere monitorati e gestiti centralmente, gli utenti non devono poter alterarne la configurazione

8.2.2 La console centrale deve poter forzare manualmente l'aggiornamento dei sistemi antimalware e verificare la automaticamete la corretta esecuzione dell'aggiornamento

8.2.3 Analisi potenziali malware eseguita su infrastruttura dedicata, eventualmente in cloud

8.3.1 Limitare i dispositivi esterni a quelli necessari

8.3.2 Monitorare uso e tentativi d'uso dei dispositivi esterni

8.4.1 Abilitare funzioni atte a contrastare lo sfruttamento delle vulnerabilità (DEP, ASLR, virtualizzazione, etc.)

8.4.2 Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità (xes. quelli forniti dai produttori di OS)

8.5.1 Usare strumenti di filtraggio del traffico di rete per impedire che il malware raggiunga gli host

8.5.2 Installare sistemi di analisi avanzata del software sospetto

8.6.1 Monitorare, analizzare e bloccare gli accessi a indirizzi che abbiano una cattiva reputazione

ABSC 8 (CSC 8) 2/2

Difese contro i malware

8.7.1 Disattivare esecuzione automatica su dispositivi removibili

8.7.2 Disattivare esecuzione automatica contenuti dinamici file (macro)

8.7.3 Disattivare apertura automatica mail

8.7.4 Disattivare anteprima automatica contenuto file

8.8.1 Eseguire scansione anti-malware automatica alla connessione di supporti rimuovibili

8.9.1 Filtrare il contenuto delle mail prima raggiungano la casella del destinatario, prevedere anche l'impiego di antispam

8.9.2 Filtrare il contenuto del traffico web

8.9.3 Bloccare nelle email e traffico web i tipi di file non necessari e potenzialmente pericolosi

8.10.1 Utilizzare anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento

8.10.1 Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate

8.4.2 Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità (xes. quelli forniti dai produttori di OS)

ABSC 10 (CSC 10)

Copie di sicurezza

10.1.1 Effettuare almeno copia settimanale delle informazioni strettamente necessarie per il completo ripristino del sistema

10.1.2 Eseguire backup di OS, applicazioni e dati

10.1.2 Eseguire backup multipli con strumenti diversi

10.2.1 Eseguire una verifica periodica delle copie tramite rispristino di prova

10.3.1 Assicurare la riservatezza delle copie di sicurezza mediante protezione fisica dei supporti o mediante cifratura, la codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud

10.4.1 Assicurare che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema per evitare che attacchi possano coinvolgere anche tutte le sue copie di sicurezza

ABSC 13 (CSC 13)

Protezione dei dati

13.1.1 Effettuare un'analisi dei dati per individuare quelli riservati (dati rilevanti) a cui applicare la protezione crittografica

13.2.1 Utilizzare la cifratura per dispositivi portatili e sistemi che contengono informazioni rilevanti

13.3.1 Monitorare e bloccare con strumenti automatici l'uso della crittografia non autorizzata sul traffico di rete uscente

13.4.1 Effettuare scansioni periodiche con sistemi automatici per rilevare sui server "data pattern" significativi per l'Amministrazione che evidenzino l'esistenza di dati rilevanti in chiaro

13.5.1 Implementare sistemi/configurazioni per impedire la scrittura di dati dispositivi esterni se questi non sono strettamente necessari

13.5.2 Gestire centralmente il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a proprietà univoche) cifrando i dati e mantendo una lista aggiornata dei dispositivi

13.6.1 Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare il flusso dei dati in rete e individuare anomalie

13.6.2 Registrare le anomalie del traffico di rete per consentire analisi off line

13.7.1 Monitorare il traffico uscente rilevando la crittografia non prevista

13.8.1 Bloccare il traffico da e verso url presenti in una blacklist

13.9.1 Assicurare che la copia autorizzata di un file mantenga le limitazioni di accesso della sorgente

Question & Answer