FRAMEWORK NAZIONALE PER LA CYBERSECURITY E LA DATA PROTECTION

TUTORIAL – PARTE 6/6
ESEMPIO DI APPLICAZIONE

Pisa, 12-02-2019

info@cybersecurityframework.it

SAPIENZA
UNIVERSITÀ DI ROMA

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

cini
Cyber Security National Lab

ESEMPIO DI APPLICAZIONE

Guida alla contestualizzazione per GDPR

- Applicazione del prototipo di contestualizzazione che coglie gli elementi fondamentali di GDPR
  - Ruoli e responsabilità
  - Registri delle attività di trattamento
  - Principi e accountability
  - Valutazione d'impatto sulla protezione dei dati personali
  - Informazione dell'interessato
  - Consenso dell'interessato
  - Diritti dell'interessato
  - Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali
  - Gestione incidenti che si configurano come violazioni di dati personali
- Utilizzo dei controlli che possono essere usati in fase di contestualizzazione

SCENARIO DI APPLICAZIONE

Caso basato su «generica» pubblica amministrazione

- Analisi guidata, tra gli altri, da 2 requisiti principali:
  - Conformazione alle Misure Minime ICT per la PA (AgiD)
  - Gestire dei dati personali (GDPR)
- Adattabile a caso di compagnia privata (sostituire ABSC con CSC come standard tecnico)

MISURE MINIME AGID

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

34 Subcategory

ID.AM-1
ID.AM-2
ID.AM-3
ID.AM-5
ID.AM-6
ID.RA-1
ID.RA-4
ID.RA-5

8

PR.AC-1
PR.AC-2
PR.AC-3
PR.AC-4
PR.AT-1
PR.AT-2
PR.DS-5
PR.DS-6
PR.IP-1
PR.IP-2
PR.IP-4
PR.IP-5
PR.IP-9
PR.IP-12
PR.MA-1
PR.MA-2
PR.PT-2
PR.PT-3

18

DE.CM-1
DE.CM-3
DE.CM-4
DE.CM-5
DE.CM-7
DE.CM-8

6

RS.MI-3

1

RC.RP-1

1

PROTOTIPO GDPR

DP-ID.AM-7
DP-ID.AM-8
ID.GV-3
DP-ID.RA-7
DP-ID.DM-2
DP-ID.DM-3
DP-ID.DM-4
DP-ID.DM-5

8

PR.AC-1
PR.AC-2
PR.AC-3
PR.AC-4
PR.AC-5
PR.AC-6
PR.AC-7
PR.DS-1
PR.DS-2
PR.DS-3
PR.DS-4
PR.DS-5
PR.DS-6
PR.DS-8
PR.IP-2
PR.IP-3
PR.IP-4
PR.IP-5
PR.IP-6
PR.IP-7
PR.IP-8
PR.IP-9
PR.IP-10
PR.IP-11
PR.IP-12
PR.PT-1
PR.PT-2
PR.PT-3
PR.PT-4
PR.PT-5

30

0

RS.RP-1
DP-RS.CO-6

2

0

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

40 Subcategory

PROT. GDPR ∩ PROT AGID

DP-ID.AM-7
DP-ID.AM-8
ID.GV-3
DP-ID.RA-7
DP-ID.DM-2
DP-ID.DM-3
DP-ID.DM-4
DP-ID.DM-5

1

PR.AC-1
PR.AC-2
PR.AC-3
PR.AC-4
PR.AC-5
PR.AC-6
PR.AC-7
PR.DS-1
PR.DS-2
PR.DS-3
PR.DS-4
PR.DS-5
PR.DS-6
PR.DS-8
PR.IP-2
PR.IP-3
PR.IP-4
PR.IP-5
PR.IP-6
PR.IP-7
PR.IP-8
PR.IP-9
PR.IP-10
PR.IP-11
PR.IP-12
PR.PT-1
PR.PT-2
PR.PT-3
PR.PT-4
PR.PT-5

13

0

RS.RP-1
DP-RS.CO-6

0

0

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

14 Subcategory

ESEMPIO INTEGRAZIONE

Nessun conflitto

- Stessa Subcategory, stessa classe, stessa priorità

	ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti	**Obbligatoria**	**ALTA**

Prototipo GDPR & Prototipo AgiD

ESEMPIO INTEGRAZIONE

Nessun conflitto

- Subcategory diverse

ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	**Libera**	
DP-ID.AM-7: Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	**Obbligatoria**	**ALTA**

ESEMPIO INTEGRAZIONE

Subcategory diverse: nessun conflitto

ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	**Libera**	
DP-ID.AM-7: Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	**Obbligatoria**	**ALTA**

Prototipo GDPR

+

ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	**Obbligatoria**	**ALTA**
DP-ID.AM-7: Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	**Libera**	

Prototipo AgiD

ESEMPIO INTEGRAZIONE

Subcategory diverse: nessun conflitto

ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	**Obbligatoria**	**ALTA**

DP-ID.AM-7: Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	**Obbligatoria**	**ALTA**

ESEMPIO INTEGRAZIONE

- Stessa Subcategory, **diversa** classe, stessa priorità

PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	**Consigliata**	**ALTA**	Prototipo GDPR
PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	**Obbligatoria**	**ALTA**	Prototipo AgiD

ESEMPIO INTEGRAZIONE

- stessa subcategory, **diversa** priorità

PR.IP-5: Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione	**Consigliata**	**MEDIA**

Prototipo GDPR

PR.IP-5: Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione	**Obbligatoria**	**ALTA**

Prototipo AgiD

ESEMPIO: LIVELLI DI MATURITA’

Posizionare i controlli di sicurezza, presenti nella guida all’implementazione di ogni prototipo, rispetto:

- Alle regole definite nella guida all’implementazione
- Ai fattori di contesto specifico

ESEMPIO:AGID

ID.AM-2

IDENTIFY – ASSET MANAGEMENT	
Subcategory FNCS	**ABSC**
ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	**ABSC 2.1.1**: Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compreso nell'elenco.
	ABSC 2.3.1: Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

M0	M1	M2
ABSC 2.1.1	ABSC 2.2.1	ABSC 2.2.3
ABSC 2.3.1	ABSC 2.2.2	ABSC 2.3.3
	ABSC 2.3.2	ABSC 2.4.1

ESEMPIO:AGID

ID.AM-2

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
2	1	1	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compreso nell'elenco.	ID.AM-2	X	X	X
	2	1	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	ID.AM-2		X	X
		2	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	ID.AM-2		X	X
		3	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	ID.AM-2			X
	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	ID.AM-2	X	X	X
		2	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	ID.AM-2		X	X
		3	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	ID.AM-2			X
	4	1	Utilizzare macchine virtuali e/o sistemi air-gapped1 per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	ID.AM-2			X

M0

ABSC 2.1.1

ABSC 2.3.1

M1

ABSC 2.2.1

ABSC 2.2.2

ABSC 2.3.2

M2

ABSC 2.2.3

ABSC 2.3.3

ABSC 2.4.1

ADATTAMENTO AL CONTESTO

- Esempio esclusione:

PR.IP-8: L'efficacia delle tecnologie di protezione viene condivisa	**Consigliata**	**BASSA**

- Esempio inclusione:

RC.RP-1: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente	**Libera**	

- Documento e materiale di supporto di base

- Pubblicare un certo numero di prototipi di contestualizzazione

www.cybersecurityframework.it