FRAMEWORK NAZIONALE PER LA CYBERSECURITY E LA DATA PROTECTION

TUTORIAL – PARTE 5/6
PROTOTIPI DI CONTESTUALIZZAZIONE GDPR e MMS

Pisa, 12-02-2019

info@cybersecurityframework.it

SAPIENZA
UNIVERSITÀ DI ROMA

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

cini
Cyber Security National Lab

PROTOTIPO DI CONTESTUALIZZAZIONE

Cosa contiene…

- Selezione delle subcategory (classe)
  - “Obbligatorie”
  - “Consigliate”
  - “Libere”
- Livelli di Priorità
- Guida all’implementazione
  - Vincoli su selezione e/o definizione livelli di priorità
  - Controlli

PROTOTIPO DI CONTESTUALIZZAZIONE GDPR

PROTOTIPO GDPR

https://www.cybersecurityframework.it

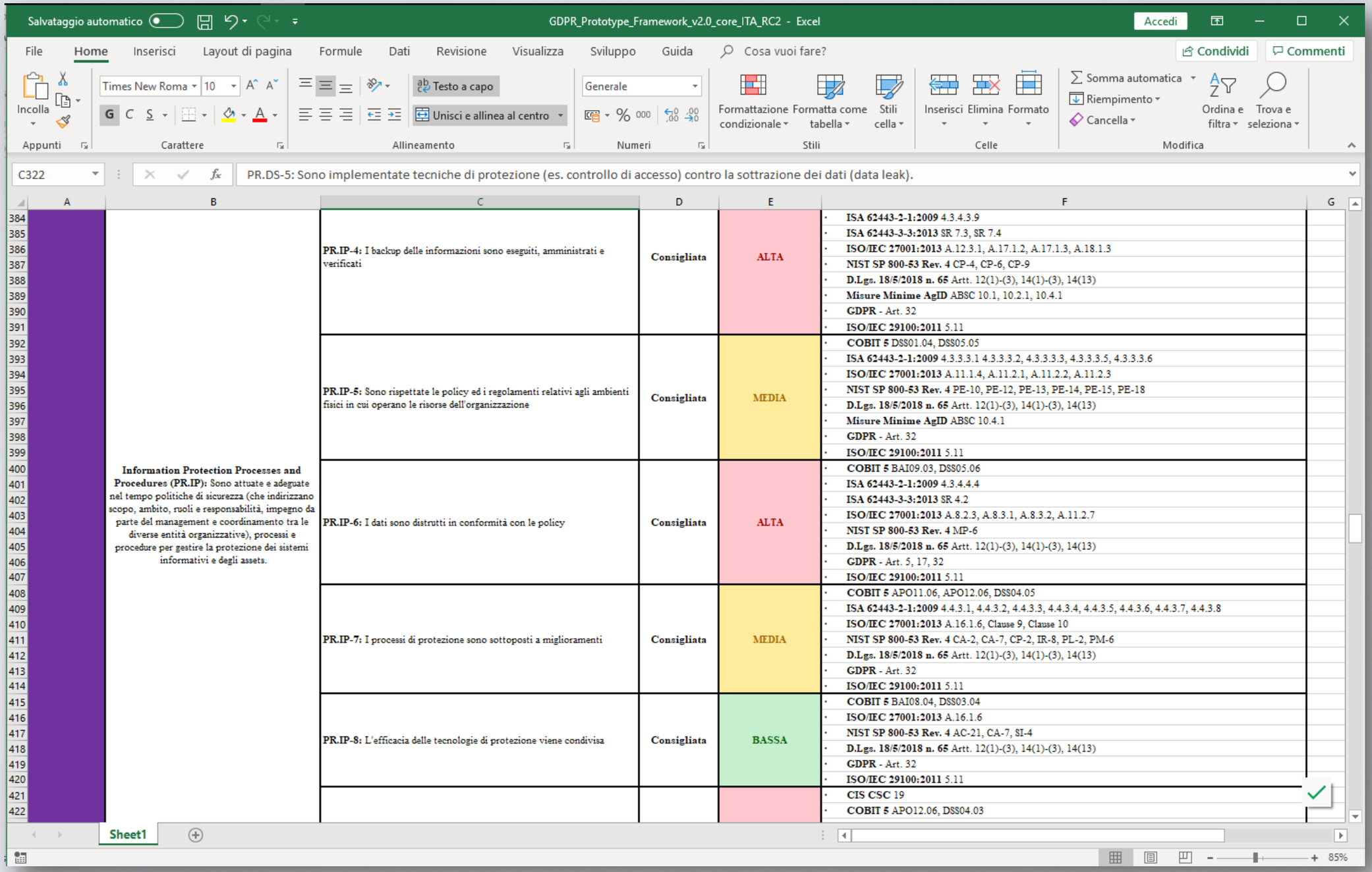
Scarica i contenuti:

- Framework Nazionale per la Cybersecurity e la Data Protection
- Framework core (formato Excel)
- Prototipo di contestualizzaione per GDPR - definizione (formato Excel)
- Prototipo di contestualizzaione per GDPR - controlli (formato Excel)

Per ulteriori informazioni: info@cybersecurityframework.it

PROTOTIPO GDPR

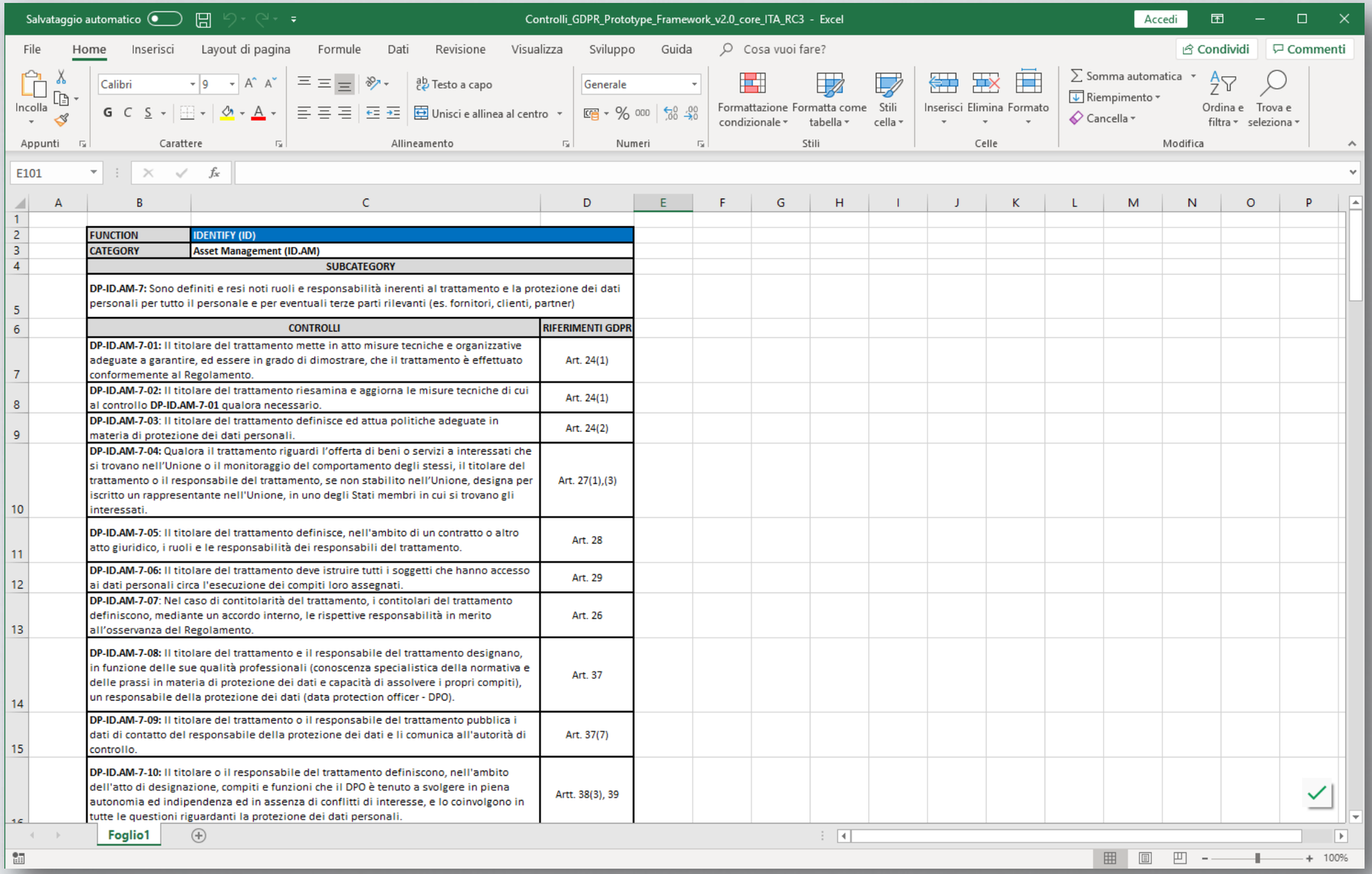
Foglio di lavoro del prototipo



		PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati	**Consigliata**	**ALTA**	· **ISA 62443-2-1:2009** 4.3.4.3.9 · **ISA 62443-3-3:2013** SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 · **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 10.1, 10.2.1, 10.4.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-5: Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione	**Consigliata**	**MEDIA**	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 10.4.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
	Information Protection Processes and Procedures (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.	**PR.IP-6:** I dati sono distrutti in conformità con le policy	**Consigliata**	**ALTA**	· **COBIT 5** BAI09.03, DSS05.06 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · **NIST SP 800-53 Rev. 4** MP-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 5, 17, 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-7: I processi di protezione sono sottoposti a miglioramenti	**Consigliata**	**MEDIA**	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-8: L'efficacia delle tecnologie di protezione viene condivisa	**Consigliata**	**BASSA**	· **COBIT 5** BAI08.04, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
					· **CIS CSC** 19 · **COBIT 5** APO12.06, DSS04.03

PROTOTIPO GDPR

Foglio di lavoro con i controlli



FUNCTION	IDENTIFY (ID)	
CATEGORY	Asset Management (ID.AM)	
SUBCATEGORY		
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)		
CONTROLLI		RIFERIMENTI GDPR
DP-ID.AM-7-01: Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento.		Art. 24(1)
DP-ID.AM-7-02: Il titolare del trattamento riesamina e aggiorna le misure tecniche di cui al controllo **DP-ID.AM-7-01** qualora necessario.		Art. 24(1)
DP-ID.AM-7-03: Il titolare del trattamento definisce ed attua politiche adeguate in materia di protezione dei dati personali.		Art. 24(2)
DP-ID.AM-7-04: Qualora il trattamento riguardi l'offerta di beni o servizi a interessati che si trovano nell'Unione o il monitoraggio del comportamento degli stessi, il titolare del trattamento o il responsabile del trattamento, se non stabilito nell'Unione, designa per iscritto un rappresentante nell'Unione, in uno degli Stati membri in cui si trovano gli interessati.		Art. 27(1),(3)
DP-ID.AM-7-05: Il titolare del trattamento definisce, nell'ambito di un contratto o altro atto giuridico, i ruoli e le responsabilità dei responsabili del trattamento.		Art. 28
DP-ID.AM-7-06: Il titolare del trattamento deve istruire tutti i soggetti che hanno accesso ai dati personali circa l'esecuzione dei compiti loro assegnati.		Art. 29
DP-ID.AM-7-07: Nel caso di contitolarità del trattamento, i contitolari del trattamento definiscono, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza del Regolamento.		Art. 26
DP-ID.AM-7-08: Il titolare del trattamento e il responsabile del trattamento designano, in funzione delle sue qualità professionali (conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e capacità di assolvere i propri compiti), un responsabile della protezione dei dati (data protection officer - DPO).		Art. 37
DP-ID.AM-7-09: Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.		Art. 37(7)
DP-ID.AM-7-10: Il titolare o il responsabile del trattamento definiscono, nell'ambito dell'atto di designazione, compiti e funzioni che il DPO è tenuto a svolgere in piena autonomia ed indipendenza ed in assenza di conflitti di interesse, e lo coinvolgono in tutte le questioni riguardanti la protezione dei dati personali.		Artt. 38(3), 39

PROTOTIPO GDPR

Selezione delle Subcategory

- **Obbligatorie**:
  - Subcategory che catturano elementi fondamentali del GDPR.
  - Non selezionarle comporta trascurare un aspetto fondamentale del GDPR
  - Devono essere selezionate in tutte le contestualizzazioni coerenti con il prototipo GDPR

PROTOTIPO GDPR

Selezione delle Subcategory

- **Consigliate**:
  - Subcategory che non catturano singolarmente un aspetto del GDPR
  - Opportunamente combinate permettono di coprire quegli aspetti su cui il Regolamento lascia maggiore libertà in merito all'implementazione
  - Vanno considerate selezionate per impostazione predefinita
  - Possono essere deselezionate in fase di contestualizzazione se non ritenute adatte allo specifico contesto
  - NOTA: «Consigliata» è riferito alla selezione della subcategory, non agli aspetti del GDPR eventualmente connessi

PROTOTIPO GDPR

Selezione d

- Consigliat
  - Subcateg DPR
  - Opportuna i su cui il Regolamento lascia maggiore libertà in merito all'implementazione
- Vanno co
- Possono e non ritenute adatte allo
- NOTA: «C on agli aspetti del GDPR

Articolo 25

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

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.

Articolo 32

Sicurezza del trattamento

1. 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.

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.

PROTOTIPO GDPR

Selezione delle Subcategory

- **Libere**:
  - Tutte le altre Subcategory
  - Non si hanno elementi che facciano propendere nettamente per la loro selezione
  - Sono considerate non selezionate per impostazione predefinita
  - È possibile selezionarle in fase di contestualizzazione (es. per integrare aspetti secondari rispetto al Regolamento)

PROTOTIPO GDPR

Livelli di Priorità

- Sono definiti per tutte le Subcategory “Obbligatorie” e “Consigliate”

- Tutte le Subcategory “Obbligatorie” hanno priorità “Alta”
  - Coprono aspetti fondamentali del GDPR che devono essere implementati indipendentemente dalla complessità

- Vincolo sui livelli di priorità: *Tutte le Subcategory “**Obbligatorie**” devono avere priorità “**Alta**”*

PROTOTIPO GDPR

Subcategory	Classe	Priorità	Informative References
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	GDPR - Artt. 24, 26-29, 37-39
DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati	Obbligatoria	ALTA	GDPR - Art. 30
DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato	Obbligatoria	ALTA	GDPR - Art 15-22
DP-RS.CO-6: Gli incidenti che si configurano come violazioni di dati personali sono documentati ed eventualmente vengono informati le autorità di riferimento e gli interessati	Obbligatoria	ALTA	GDPR - Artt. 33, 34

PROTOTIPO GDPR

Subcategory	Classe	Priorità	Informative References
PR.AC-4: Gli accessi alle risorse e le autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	Consigliata	ALTA	GDPR – Artt. 25, 32
PR.DS-4: I sistemi hanno adeguate risorse a disposizione per poter garantire la disponibilità	Consigliata	MEDIA	GDPR – Art. 32
PR.IP-6: I dati sono distrutti in conformità con le policy	Consigliata	ALTA	GDPR - Artt. 5, 17, 32
PR.IP-8: L'efficacia delle tecnologie di protezione viene condivisa	Consigliata	BASSA	GDPR – Art. 32

PROTOTIPO GDPR

Subcategory	Classe	Priorità
PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	Libera	
DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità	Libera	
DE.CM-5: Il codice non autorizzato su dispositivi mobili viene rilevato	Libera	

PROTOTIPO GDPR

Guida all'implementazione

1. Ruoli e responsabilità
2. Registri delle attività di trattamento
3. Principi
4. Valutazione d'impatto sulla protezione dei dati personali
5. Informazioni all'interessato
6. Consenso dell'interessato
7. Diritti dell'interessato
8. Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali
9. Gestione incidenti che si configurano come violazioni di dati personali

PROTOTIPO GDPR

1. Ruoli e Responsabilità

FUNCTION	IDENTIFY (ID)	
CATEGORY	Asset Management (ID.AM)	
SUBCATEGORY		
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)		
CONTROLLI		**RIFERIMENTI GDPR**
DP-ID.AM-7-01: Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento.		Art. 24(1)
DP-ID.AM-7-02: Il titolare del trattamento riesamina e aggiorna le misure tecniche di cui al controllo **DP-ID.AM-7-01** qualora necessario.		Art. 24(1)
DP-ID.AM-7-03: Il titolare del trattamento definisce ed attua politiche adeguate in materia di protezione dei dati personali.		Art. 24(2)
DP-ID.AM-7-04: Qualora il trattamento riguardi l'offerta di beni o servizi a interessati che si trovano nell'Unione o il monitoraggio del comportamento degli stessi, il titolare del trattamento o il responsabile del trattamento, se non stabilito nell'Unione, designa per iscritto un rappresentante nell'Unione, in uno degli Stati membri in cui si trovano gli interessati.		Art. 27(1),(3)
DP-ID.AM-7-05: Il titolare del trattamento definisce, nell'ambito di un contratto o altro atto giuridico, i ruoli e le responsabilità dei responsabili del trattamento.		Art. 28
DP-ID.AM-7-06: Il titolare del trattamento deve istruire tutti i soggetti che hanno accesso ai dati personali circa l'esecuzione dei compiti loro assegnati.		Art. 29
DP-ID.AM-7-07: Nel caso di contitolarità del trattamento, i contitolari del trattamento definiscono, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza del Regolamento.		Art. 26
DP-ID.AM-7-08: Il titolare del trattamento e il responsabile del trattamento designano, in funzione delle sue qualità professionali (conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e capacità di assolvere i propri compiti), un responsabile della protezione dei dati (data protection officer - DPO).		Art. 37
DP-ID.AM-7-09: Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.		Art. 37(7)
DP-ID.AM-7-10: Il titolare o il responsabile del trattamento definiscono, nell'ambito dell'atto di designazione, compiti e funzioni che il DPO è tenuto a svolgere in piena autonomia ed indipendenza ed in assenza di conflitti di interesse, e lo coinvolgono in tutte le questioni riguardanti la protezione dei dati personali.		Artt. 38(3), 39
DP-ID.AM-7-11: Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati (ad esempio pseudonimizzazione, minimizzazione) fin dalla progettazione (data protection by-design).		Art. 25(1)
DP-ID.AM-7-12: Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita (data protection by-default), solo i dati personali necessari per ogni specifica finalità del trattamento.		Art. 25(2)

PROTOTIPO GDPR

2. Registri delle attività di trattamento

FUNCTION	IDENTIFY (ID)
CATEGORY	Asset Management (ID.AM)
SUBCATEGORY	
DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati.	
CONTROLLI	**RIFERIMENTI GDPR**
DP-ID.AM-8-01: Il titolare del trattamento e il responsabile del trattamento tengono, in forma scritta (anche in formato elettronico), un registro delle attività di trattamento svolte.	Art. 30(1-3)

PROTOTIPO GDPR

3. Principi

FUNCTION	IDENTIFY (ID)
CATEGORY	Governance (ID.GV)
SUBCATEGORY	
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.	
CONTROLLI	**RIFERIMENTI GDPR**
ID.GV-3-01: Sono definiti e gestiti processi atti a garantire che i trattamenti di dati personali rispettino i principi di liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza (art. 5).	Art. 5(1)
ID.GV-3-02: Il titolare del trattamento è in grado di dimostrare il rispetto dei principi di cui al controllo **ID.GV-3-01** e la conformità delle attività di trattamento con il Regolamento (accountability).	Art. 5(2)

PROTOTIPO GDPR

4. Valutazione d'impatto sulla protezione dei dati personali

FUNCTION	**IDENTIFY (ID)**
CATEGORY	**Risk Assessment (ID.RA)**
SUBCATEGORY	
DP-ID.RA-7: Viene effettuata una valutazione di impatto sulla protezione dei dati personali.	
CONTROLLI	**RIFERIMENTI GDPR**
DP-ID.RA-7-01: Qualora un tipo di trattamento di dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, consultato il responsabile della protezione dei dati, effettua una valutazione dell'impatto sulla protezione dei dati personali.	Art. 35(1-5)
DP-ID.RA-7-02: Il titolare del trattamento si assicura che la valutazione d'impatto contenga quanto previsto dal Regolamento.	Art. 35(7)
DP-ID.RA-7-03: Il titolare del trattamento, nell'effettuare la valutazione d'impatto sulla protezione dei dati personali, tiene conto del rispetto dei codici di condotta e, se del caso, delle opinioni degli interessati o dei loro rappresentanti sul trattamento.	Art. 35(8),(9)
DP-ID.RA-7-04: Il titolare del trattamento procede ad un riesame della valutazione di impatto con cadenza periodica e qualora insorgano variazioni del rischio rappresentato dalle attività relative al trattamento.	Art. 35(11)
DP-ID.RA-7-05: Qualora la valutazione di impatto sulla protezione dei dati personali indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio, il titolare del trattamento consulta l'autorità di controllo.	Art. 36(1),(3)

PROTOTIPO GDPR

5. Informazioni all'interessato

FUNCTION	IDENTIFY (ID)
CATEGORY	Data Management (DP-ID.DM)
SUBCATEGORY	
DP-ID.DM-2: Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati.	
CONTROLLI	**RIFERIMENTI GDPR**
DP-ID.DM-2-01: Il titolare del trattamento adotta processi per fornire all'interessato tutte le informazioni inerenti il trattamento dei dati personali comunque raccolti (sia presso lo stesso interessato che presso terzi) nonché l'esistenza e le modalità di esercizio dei diritti previsti dal Regolamento.	Artt. 12, 13 14

PROTOTIPO GDPR

6. Consenso dell'interessato

FUNCTION	IDENTIFY (ID)
CATEGORY	Data Management (DP-ID.DM)
SUBCATEGORY	
DP-ID.DM-3: Sono definiti, implementati e documentati i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati.	
CONTROLLI	**RIFERIMENTI GDPR**
DP-ID.DM-3-01: Il titolare del trattamento mette in atto processi che gli permettano di dimostrare che, per i trattamenti basati sul consenso, l'interessato, o nel caso di minori il titolare della responsabilità genitoriale, ha liberamente prestato uno specifico consenso per ciascun trattamento dei propri dati personali.	Art. 7(1),(2),(4) e art. 8
DP-ID.DM-3-02: Il titolare del trattamento mette in atto processi che gli permettano di gestire e documentare la revoca del consenso al trattamento dei dati personali da parte dell'interessato, o nel caso di minori del titolare della responsabilità genitoriale.	Art. 7(3) e art. 8

PROTOTIPO GDPR

7. Diritti dell'interessato

FUNCTION	IDENTIFY (ID)	
CATEGORY	Data Management (DP-ID.DM)	
SUBCATEGORY		
DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato.		
CONTROLLI		**RIFERIMENTI GDPR**
DP-ID.DM-4-01: È definito un processo che garantisce al titolare del trattamento la capacità di fornire all'interessato la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano.		Art. 15
DP-ID.DM-4-02: Il titolare del trattamento mette in atto processi che garantiscono l'esercizio da parte dell'interessato del diritto di accesso ai dati personali ed alle informazioni relative al trattamento, qualora la richiesta avvenga tramite mezzi elettronici, utilizzando un formato elettronico di uso comune.		Art. 15
DP-ID.DM-4-03: Il titolare del trattamento mette in atto processi che garantiscono all'interessato l'esercizio del diritto di rettifica dei dati personali che lo riguardano qualora ne faccia richiesta, senza ingiustificato ritardo.		Art. 16
DP-ID.DM-4-04: Il titolare del trattamento mette in atto processi che garantiscono all'interessato l'esercizio del diritto di cancellazione dei dati personali che lo riguardano qualora ne faccia richiesta, senza ingiustificato ritardo, senza ingiustificato ritardo i dati personali qualora sussista uno dei motivi di cui all'art. 17 par. 1.		Art. 17(1)
DP-ID.DM-4-05: In riferimento al controllo **DP-ID.DM-4-04**, il titolare del trattamento, qualora abbia reso pubblici i dati personali, adotta le misure ragionevoli, anche tecniche, per informare della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali, tutti gli ulteriori titolari del trattamento che stanno trattando i dati personali.		Art. 17(2)
DP-ID.DM-4-06: Il titolare del trattamento mette in atto processi che garantiscono all'interessato l'esercizio del diritto di limitazione del trattamento dei dati personali che lo riguardano e che successivamente alla limitazione i dati vengano trattati esclusivamente nelle circostanze previste dal Regolamento (es. consenso dell'interessato, accertamento diritti in sede giudiziaria, ecc.).		Art. 18(1-3)
DP-ID.DM-4-07: Il titolare del trattamento mette in atto processi per la comunicazione a ciascuno dei destinatari cui sono stati trasmessi i dati personali delle eventuali rettifiche, cancellazioni o limitazioni del trattamento richieste dall'interessato.		Art. 19
DP-ID.DM-4-08: Il titolare del trattamento mette in atto processi che garantiscono all'interessato l'esercizio del diritto di portabilità dei dati.		Art. 20
DP-ID.DM-4-09: Il titolare del trattamento mette in atto processi che garantiscono all'interessato l'esercizio del diritto di opposizione al trattamento dei dati personali, ove ne ricorrano i presupposti.		Art. 21
DP-ID.DM-4-10: Il titolare del trattamento mette in atto processi che garantiscono all'interessato 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.		Art. 22(1)
DP-ID.DM-4-11: In riferimento al controllo **DP-ID.DM-4-10**, nel caso in cui la decisione si basi sul consenso esplicito dell'interessato oppure sia necessaria per la conclusione o l'esecuzione di un contratto, 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).		Art. 22(2-3)

PROTOTIPO GDPR

8. Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali

FUNCTION	IDENTIFY (ID)
CATEGORY	Data Management (DP-ID.DM)
SUBCATEGORY	
DP-ID.DM-5: Sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale.	
CONTROLLI	**RIFERIMENTI GDPR**
DP-ID.DM-5-01: È definito un processo per regolare il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali in conformità a quanto sancito nell'art 44.	Art. 44
DP-ID.DM-5-02: È definito un processo atto a verificare che sussistano le condizioni affinché un trasferimento di dati personali verso paesi terzi o organizzazioni internazionali sia ammesso, ai sensi dell'art. 45.	Art. 45
DP-ID.DM-5-03: In mancanza di una decisione ai sensi dell'art. 45, par. 3, il titolare del trattamento o il responsabile del trattamento effettuano il trasferimento verso un paese terzo o organizzazione internazionale solo se sono in grado di fornire garanzie adeguate in conformità all'art. 46 parr. 2 e 3 oppure, in ultima analisi, qualora sussistano le specifiche condizioni, di cui all'art. 49.	Art. 46, 47 e art. 49

PROTOTIPO GDPR

9. Gestione incidenti che si configurano come violazioni di dati personali

FUNCTION	RESPOND (RS)
CATEGORY	Communications (RS.CO)
SUBCATEGORY	
DP-RS.CO-6: Gli incidenti che si configurano come violazioni di dati personali sono documentati ed eventualmente vengono informati le autorità di riferimento e gli interessati.	
CONTROLLI	**RIFERIMENTI GDPR**
DP-RS.CO-6-01: In caso di violazione dei dati personali che presenti un rischio per gli interessati, il titolare del trattamento notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo, e comunque entro 72 ore dal momento in cui ne è venuto a conoscenza.	Art. 33
DP-RS.CO-6-02: In caso di violazione dei dati personali che presenti un rischio elevato per gli interessati, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.	Art. 34
DP-RS.CO-6-03: Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza di una violazione dei dati personali.	Art. 33(2)
DP-RS.CO-6-04: Il titolare del trattamento documenta tutte le violazioni dei dati personali, comprese le circostanze a esse relative, le loro conseguenze e i provvedimenti adottati per porvi rimedio.	Art. 33(5)

PROTOTIPO DI CONTESTUALIZZAZIONE “Misure Minime AgID”

“MISURE MINIME” AGID

- “Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni”
- Emesso in attuazione della Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015
- Le indicazioni contenute nel documento devono essere adottate dalle PA

“MISURE MINIME” AGID

- Specificano dei controlli di sicurezza “AgID Basic Security Control” (ABSC)
- Sono una selezione dei controlli CCS CSC* (SANS20)

Codice	Descrizione
CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Sofware
CSC 3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 8	Malware Defenses
CSC 10	Data Recovery Capability
CSC 13	Data Protection

* CIS Critical Security Controls for Effective Cyber Defense, https://www.cisecurity.org/controls/

“MISURE MINIME” AGID

Ad ogni misura di sicurezza (ABSC) è associato un livello:

- Minimo: il livello sotto il quale nessuna PA può scendere.
  Le misure “minime” sono obbligatorie.

- Standard: livello da considerarsi come base di riferimento (una sorta di caso medio).

- Alto: identifica il livello a cui tendere.

“MISURE MINIME” AGID

Mapping con le subcategory del Framework Nazionale

Livello

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.

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
8	1	1	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l’esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	DE.CM-4 DE.CM-5	X	X	X
		2	Installare su tutti i dispositivi firewall ed IPS personali.	DE.CM-1	X	X	X
		3	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	DE.AE-3 DE.CM-1 RS.CO-1 RS.MI-1		X	X
	2	1	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	PR.IP-3 DE.DP-1		X	X
		2	È possibile forzare manualmente dalla console centrale l’aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell’aggiornamento è automaticamente verificata e riportata alla console centrale.	PR.IP-3 PR.MA-1 PR.MA-2 DE.CM-4		X	X
		3	L’analisi dei potenziali malware è effettuata su di un’infrastruttura dedicata, eventualmente basata sul cloud.	PR.DS-7 DE.CM-4			X
	3	1	Limitare l’uso di dispositivi esterni a quelli necessari per le attività aziendali.	PR.PT-3 DE.CM-7	X	X	X
		2	Monitorare l’uso e i tentativi di utilizzo di dispositivi esterni.	PR.AC-3 DE.AE-1 DE.CM-7			X
	4	1	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	PR.IP-1 RS.MI-1 RS.MI-2		X	X
		2	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	PR.IP-1 RS.MI-1 RS.MI-2			X

PROTOTIPO MM AGID

Selezione delle subcategory

- La classificazione è guidata dai livelli
  - **Obbligatorie**: tutte le Subcategory associate ad almeno un controllo ABSC di livello “Minimo”
  - **Consigliate**: tutte le Subcategory non associate a controlli ABSC di livello “Minimo” ma associate almeno ad un controllo di livello “Standard” o “Alto”
  - **Libere**: tutte le altre Subcategory (non associate direttamente a controlli ABSC)

PROTOTIPO MM AGID

Selezione delle subcategory

- La classificazione è guidata dai livelli
  - **Obbligatorie**: rollo ABSC di livello "Minim
  - **Consigliate**: C di livello "Minimo" ma rd" o "Alto"
  - **Libere**: tutte controlli ABSC)

NOTA:
Dopo la creazione di una contestualizzazione è possibile definire diversi profili:
Esempio:
- Profilo «Minimo»
- Profilo «Standard»
- Profilo «Alto»

PROTOTIPO MM AGID

Livelli di Priorità

- Sono definiti per le Subcategory "Obbligatorie" e "Consigliate"
- Le subcategory "**Obbligatorie**" hanno priorità **Alta**
  - Tutti i controlli di livello minimo devono essere implementati dalle PA indipendentemente dalla complessità
  - La guida all'implementazione vincola la priorità di queste subcategory al livello massimo
- Per le Subcategory "Consigliate" la priorità tiene conto:
  - Del livello AgID (Standard o Alto)
  - Di quanto la Subcategory permette di ridurre il rischio cyber
  - Della complessità implementativa

PROTOTIPO MM AGID

Guida all'implementazione

- Riporta i controlli ABSC organizzati nelle Subcategory del Framework

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.

PROTOTIPO MM AGID

Guida all'implementazione

- Riporta i controlli ABSC organizzati nelle Subcategory del Framework

PROTECT– INFORMATION PROTECTION PROCESSES AND PROCEDURES	
Subcategory FNCS	**ABSC**
PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati periodicamente	**ABSC 10.1.1**: Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
	ABSC 10.4.1: 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.

PROTOTIPO MM AGID

Guida all'implementazione

- Riporta i controlli ABSC organizzati nelle Subcategory del Framework

DETECT– CONTINUOUS MONITORING

Subcategory FNCS	ABSC
DE.CM-1: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	**ABSC 8.6.1**: Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.
	ABSC 13.8.1: Bloccare il traffico da e verso url presenti in una blacklist.