REGIONE BASILICATA

LA GIUNTA

DELIBERAZIONE N° 202300043

SEDUTA DEL **01/02/2023**

Ufficio per l'amministrazione digitale 16BJ
STRUTTURA PROPONENTE

OGGETTO

Definizione della gestione e dei controlli inerenti la Cybersecurity e la protezione dei dati personali. Adesione al modello di qualificazione decreti della ACN Agenzia per la Cybersicurezza Nazionale n. 307 del 18 gennaio 2022 e n. 29 del 2 gennaio 2023.

Relatore **PRESIDENTE**

La Giunta, riunitasi il giorno **01/02/2023** alle ore **13:30** nella sede dell'Ente,

			Presente	Assente
1.	**Bardi Vito**	**Presidente**	X	○
2.	**Fanelli Francesco**	**Vice Presidente**	X	○
3.	**Galella Alessandro**	**Assessore**	X	○
4.	**Merra Donatella**	**Assessore**	X	○
5.	**Latronico Cosimo**	**Assessore**	X	○
6.			○	○

Segretario: **Michele Busciolano**

ha deciso in merito all'argomento in oggetto, secondo quanto riportato nelle pagine successive.

Visto del Direttore Generale — IL DIRETTORE GENERALE **Michele Busciolano**

Ufficio Ragioneria Generale e Fiscalità Regionale

PRENOTAZIONE IMPEGNI

Num. Preimpegno	Bilancio	Missione.Programma.Titolo.Macroaggr.	Capitolo	Importo Euro

IMPEGNI

Num. Impegno	Bilancio	Missione.Programma Titolo.Macroaggr.	Capitolo	Importo Euro	Atto	Num. Prenotazione	Anno

IL DIRIGENTE

Allegati N° 6

Atto soggetto a pubblicazione ⊗ integrale O integrale senza allegati O per oggetto O per oggetto e dispositivo sul Bollettino Ufficiale della Regione Basilicata

VISTO lo Statuto della Regione Basilicata, approvato con la Legge Statutaria regionale 17 novembre 2016, n. 1, modificato ed integrato con la Legge Statutaria regionale 18 luglio 2018, n. 1;

VISTO il decreto legislativo 30 marzo 2001, n. 165 e s.m.i. recante *"Norme generali sull'ordinamento del lavoro alle dipendenze delle Pubbliche Amministrazioni"*;

VISTA la legge regionale 02 marzo 1996, n. 12 e s.m.i. recante *"Riforma dell'organizzazione amministrativa regionale"*;

VISTA la legge regionale 25 ottobre 2010, n. 31 recante: *"Disposizioni di adeguamento della normativa regionale al decreto Legislativo 27 ottobre 2009, n. 150 – Modifica art. 73 della Legge Regionale 30 dicembre 2009, n. 42 – Modifiche della Legge Regionale 9 febbraio 2001, n. 7 – Modifica art. 10 Legge Regionale 2 febbraio 1998, n. 8 e s.m.i."*;

VISTA la legge regionale 30 dicembre 2019, n. 29 recante *"Riordino degli uffici della Presidenza e della Giunta regionale e disciplina dei controlli interni";*

VISTO il decreto del Presidente della Giunta regionale n. 164 del 24 ottobre 2020 *"Decreto di organizzazione degli Uffici di diretta collaborazione del Presidente della Giunta regionale"* e s.m.i.;

VISTO il regolamento regionale 10 febbraio 2021, n. 1 recante *"Ordinamento amministrativo della Giunta regionale della Basilicata"* e s.m.i.;

VISTA la DGR n. 750 del 06 ottobre 2021, recante "*Modifiche parziali alla DGR n. 219/2021. Riapprovazione del documento recante l'organizzazione delle Strutture amministrative della Giunta regionale"*;

VISTA la DGR n. 775 del 06 ottobre 2021, recante "*Art. 3 Regolamento 10 febbraio 2021, n. 1. Conferimento incarichi Direzione Generale"*;

VISTA la DGR n. 906 del 12 novembre 2021, recante "*Dirigenti regionali a tempo indeterminato. Conferimento incarichi"*;

VISTA la DGR n. 179 del 8 aprile 2022 recante "*Regolamento interno della Giunta regionale della Basilicata – Approvazione*", pubblicata sul BUR n. 18 del 16 aprile 2022;

VISTO il regolamento regionale 5 maggio 2022, n. 1 *"Controlli interni di regolarità amministrativa"*, pubblicato sul bollettino ufficiale regionale n. 20 del 6 maggio 2022;

VISTA la DGR n. 676 del 14 ottobre 2022, recante "Piano Integrato di Attività e Organizzazione 2022 – 2024. Approvazione ai sensi dell'art. 6 del decreto legge 9 giugno 2021, n. 80, convertito con modificazioni in legge 6 agosto 2021, n. 113";

VISTA la DGR n. 762 del 14 novembre 2022, recante "Art. 3 Regolamento regionale 10 febbraio 2021, n. 1. Conferimento incarichi di Direzione Generale";

la Deliberazione della Giunta Regionale n. 14/2023, "L. 190/2012, art. 1, comma 8. Definizione degli obiettivi strategici in materia di prevenzione della corruzione e trasparenza per la programmazione triennale 2023/2025";

VISTA la Direttiva NIS (EU 2016/1148 – Network and Information Security Directive) rivolta, a livello europeo, alla protezione delle infrastrutture critiche rispetto alle minacce di tipo cyber;

VISTO il decreto legislativo 18 maggio 2018, n. 65 "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune

elevato di sicurezza delle reti e dei sistemi informativi nell'Unione", di recepimento della predetta Direttiva NIS;

VISTO Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013, cd. regolamento sulla cybersicurezza**;**

VISTO il decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133, recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica"**;**

VISTO il decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni dalla legge 4 agosto 2021, n. 109, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale";

DATO ATTO che, ai sensi dell'articolo 4 par. 1 n. 7 del RGPD e dell'articolo 48 dello Statuto regionale, Titolare del trattamento è la Giunta regionale;

CONSIDERATO che il Titolare del trattamento, ai sensi del predetto art. 4, par. 1 n. 7 e dell'art. 24 del RGPD, è il soggetto che definisce, in particolare, le finalità, i mezzi, le modalità e le misure di sicurezza del trattamento;

VISTO il decreto legislativo 30 giugno 2003, n. 196 ss.mm.ii., recante il "Codice in materia di protezione dei dati personali";

VISTO il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati – RGPD);

RICHIAMATO in particolare l'articolo 5 del RGPD che, al par. 1, enuncia i principi applicabili al trattamento dei dati personali e, al par. 2, pone in capo al titolare il principio di responsabilizzazione (cd *Accountability*), in base al quale lo stesso deve assicurare, ed essere in grado di comprovare, il rispetto di tali principi;

CONSIDERATO che il RGPD nasce per proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare per assicurare un'applicazione coerente e omogenea delle norme a protezione dei dati personali, con regole equivalenti a livello europeo (considerando 10), ed offre un quadro di riferimento aggiornato e fondato sul principio di responsabilizzazione (*Accountability*);

VISTA la deliberazione di Giunta regionale n. 431 del 17 maggio 2018 avente ad oggetto *"Regolamento (UE) 2016/679. Designazione responsabile della protezione dei dati"*, con la quale si è proceduto alla nomina del cd. DPO*;*

RICHIAMATA la deliberazione della Giunta regionale n. 540 del 19/07/2021, relativa alla "Attuazione degli adempimenti previsti dalla normativa per il trattamento dei dati personali Regolamento (UE) 2016/679 - Ridefinizione modello organizzativo"; n. 1. Conferimento incarichi di Direzione Generale";

VISTA la DGR n 1346 del 20 dicembre 2018 con cui è stata ammessa a finanziamento, a valere sull'Asse 2, Azione 2C.2.2.1 del PO FESR Basilicata 2014-2020, l'Operazione "Data Center Unico Regionale" per un importo complessivo pari ad € 11.071.200,00;

la DGR 925 del 13/12/2019 avente ad oggetto "*Accordo tra la Regione Basilicata, l'Agenzia per l'Italia Digitale e l'Agenzia per la Coesione Territoriale, per la reciproca collaborazione in azioni volte allo sviluppo dell'agenda digitale in Basilicata e per la crescita e la cittadinanza digitale verso gli obiettivi EU2020*" con la quale è stata approvata la scheda d'intervento "Data Center Unico Regionale";

DATO ATTO che con la suddetta DGR 1346/2018 sono state demandate all'Ufficio Amministrazione Digitale le iniziative opportune finalizzate al pieno coinvolgimento di tutti i soggetti pubblici interessati dall'intervento nonché il coordinamento delle attività necessarie a conseguire la convergenza del patrimonio informativo sulla infrastruttura unitaria;

che l'Ufficio Speciale per l'Amministrazione Digitale, prendendo le mosse dalla citata DGR, ha avviato una serie di interventi finalizzati alla realizzazione del Data Center Unico Regionale in conformità allo standard ANSI/TIA 942-B-2017 (Data Center TIER III);

che sono in corso i lavori di adeguamento degli impianti elettrici e tecnologici del Data Center che si concluderanno, presumibilmente, entro il mese di agosto 2023;

che per garantire la continuità operativa dei servizi, è prevista inoltre la realizzazione di un sito gemello a Matera che funge da sito secondario per il Disaster Recovery e sono previste opere per la realizzazione di locali nei quali vengono attestate le linee di telecomunicazione ridondate provenienti dall'esterno, opere di adeguamento della cabina elettrica, un nuovo locale per quadri elettrici, un nuovo gruppo elettrogeno;

che il progetto è stato approvato dall'Agid (Agenzia per l'Italia Digitale) ed è stato certificato allo standard ANSI/TIA 942-B-2017 (Data Center TIER III) da un ente terzo leader mondiale nello svolgimento di tali servizi di certificazione, Bureau Veritas, che ne ha rilasciato il relativo certificato di conformità;

che, in parallelo con i lavori di adeguamento degli impianti elettrici e tecnologici del Data Center regionale, l'Ufficio Speciale per l'Amministrazione Digitale ha già effettuato una serie di interventi sul tema della sicurezza informatica:

- PROTEZIONE DEI DATI - Acquisto di un nuovo Sistema DBMS Oracle con opzioni di sicurezza (DB Vault) e crittografia; Acquisto di un sistema "DATA LOSS PREVENTION (DLP)" per garantire la sicurezza dei dati ed il controllo del traffico dati sulla rete;
- SICUREZZA DELLE APPLICAZIONI - Acquisto di un sistema di "Software intelligence analisys" per effettuare una misurazione degli applicativi attraverso la tecnica AFP (Automated Function Point);
- ACQUISTO HARDWARE - Acquisto di nuovi sistemi server e storage per potenziare la capacità elaborativa dei data Center di Potenza e di Matera;
- SERVIZI DI CONSERVAZIONE – Adesione allo specifico contratto Quadro SPC Cloud - Lotto 1 – per l'acquisizione di Servizi di Conservazione Digitale dei dati amministrativi dell'Amministrazione Regionale e dei clinici del Servizio Sanitario Regionale;
- PROGETTO ESECUTIVO DATA CENTER - Servizi professionali di Security Strategy per la progettazione esecutiva del Data Center Unico Regionale di livello Tier 3 in grado di garantire la Governance e la continuità di servizio;
- LAVORI DI MANUTENZIONE IMPIANTI - Lavori di manutenzione impianti elettrici e tecnologici del Sito primario di Potenza e del Sito secondario di Disaster Recovery di Matera;

- CERTIFICAZIONE DATA CENTER - Servizi professionali per la Certificazione del data center regionale secondo lo standard TIA 942:2017 (Tier III);
- CYBERSECURITY - Partecipazione all'Avviso Pubblico n. 03/2022 per la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul PNRR, M1C1 – Investimento 1.5 Cybersecurity. Attivazione del Centro per la Cybersicurezza Regionale;
- POTENZIAMENTO RETE: 1) HUAWEI – Fornitura di nuovi apparati di rete GIGARUPAR (MUX ottici rete primaria); 2) FORTINET - Acquisto di nuovi sistemi hardware, software e relativi servizi di sottoscrizione della famiglia Fortinet per la gestione della sicurezza dei nodi di rete;
- CENTRO TECNICO REGIONALE - Contratto per la fornitura dei servizi di connettività della GIGARUPAR e dei relativi servizi tecnici di gestione del Centro Tecnico Regionale

VISTA la Determina dell'Agenzia per la Cybersicurezza nazionale n. 307 del 18 gennaio 2022 riguardante "*l'aggiornamento degli ulteriori livelli minimi di sicurezza, capacità elaborativa e affidabilità delle infrastrutture digitali per la pubblica amministrazione e delle ulteriori caratteristiche di qualità, sicurezza, performance e scalabilità dei servizi cloud per la pubblica amministrazione, nonché i requisiti di qualificazione dei servizi cloud per la pubblica amministrazione*".

VISTO il Decreto direttoriale n. 29 del 2 gennaio 2023 dell'Agenzia per la Cybersicurezza nazionale (ACN), con il quale si dà avvio al nuovo percorso di qualificazione cloud per la Pubblica Amministrazione;

TENUTO CONTO

che il suddetto Decreto n. 29 del 2 gennaio 2023 adottato dall'Agenzia per la Cybersicurezza Nazionale d'intesa con il Dipartimento per la trasformazione digitale, traccia le tappe che definiscono le nuove modalità che imprese e amministrazioni dovranno seguire a partire dal 19 gennaio 2023;

VALUTATO che le caratteristiche del Data Center regionale rispettano i requisiti di qualificazione prescritti dall'allegato 1 della Determina 307/2022 dell'ACN;

RICHIAMATA altresì la deliberazione della Giunta regionale n. 569 dell'8 settembre 2022, con la quale è stato approvato il "Piano Digitale Regionale", che, tra l'altro, include specifiche previsioni in tema prevenzione, identificazione e risposta agli attacchi cyber in tutti i contesti della sicurezza;

RITENUTO di dover fornire, disposizioni attuative a tutti coloro che effettuano trattamenti di dati personali per conto del Titolare, a comprova della conformità dei trattamenti al RGPD e in ossequio al principio di Responsabilizzazione ("*Accountability*") richiamato dallo stesso Regolamento;

RITENUTO di strutturare i processi decisionali e i controlli (*Governance*) inerenti alla Cybersecurity e alla protezione dei dati personali (*Data Protection*) attraverso la definizione di procedure e regole (*Policy*) dirette al rafforzamento del modello organizzativo e di processo (*Compliance*) per rendere evidente e concreta la conformità al principio della Responsabilizzazione;

SENTITO al riguardo, il Responsabile per la Protezione Dati – DPO;

VISTI **a)** i documenti riportanti le Policy inerenti alla Data Protection, predisposti dal Data Protection Officer (punti 1.2.3.4. dell'elenco sottostante);

b) la check list dei controlli da effettuare per garantire la piena aderenza ai requisiti di sicurezza del datacenter (punto 5. dell'elenco sottostante), approntata dal DPO e dal Responsabile Unico del Procedimento per la realizzazione dei lavori di adeguamento del datacenter unico regionale, progetto di competenza dell'Ufficio Speciale per l'Amministrazione Digitale;

CONSIDERATO che è in corso di realizzazione il datacenter unico regionale (DGR 1346/2018) per i quale si è già in possesso di certificazione del progetto esecutivo rilasciato da Bureau Veritas Certification il 13/09/2021,

VISTO il documento "Posizionamento della strategia regionale rispetto alle iniziative dell'Agenzia per la Cybersicurezza Nazionale per la qualificazione dei Servizi Cloud e delle Infrastrutture dei Servizi Cloud" (punto 6. dell'elenco sottostante), redatto dall'Ufficio per l'Amministrazione Digitale;

che vengono richiamati nel seguente elenco:

1. Allegato 1 "Linee guida sulle Misure di Sicurezza per la Data Protection";
2. Allegato 2 "Linee guida Processo gestione degli incidenti di sicurezza";
3. Allegato 3 "Linee guida sui controlli per la Cybersecurity e la Data Protection";
4. Allegato 4 "Modelli tipo Data Protection Agreement";
5. Allegato 5"Lista controlli per la piena aderenza ai requisiti di sicurezza del datacenter e per la qualificazione dei servizi cloud e delle infrastrutture";
6. Allegato 6 "Posizionamento della strategia regionale rispetto alle iniziative dell'Agenzia per la Cybersicurezza Nazionale per la qualificazione dei Servizi Cloud e delle Infrastrutture dei Servizi Cloud.";

RITENUTO di dover approvare la sopra elencata documentazione quale parte integrante e sostanziale del presente atto:

1. Allegato 1 "Linee guida sulle Misure di Sicurezza per la Data Protection";
2. Allegato 2 "Linee guida Processo gestione degli incidenti di sicurezza";
3. Allegato 3 "Linee guida sui controlli per la Cybersecurity e la Data Protection";
4. Allegato 4 "Modelli tipo Data Protection Agreement";
5. Allegato 5 "Lista controlli per la piena aderenza ai requisiti di sicurezza del datacenter e per la qualificazione dei servizi cloud e delle infrastrutture";
6. Allegato 6 "Posizionamento della strategia regionale rispetto alle iniziative dell'Agenzia per la Cybersicurezza Nazionale per la qualificazione dei Servizi Cloud e delle Infrastrutture dei Servizi Cloud.";

DATO ATTO che il DPO provvede autonomamente ad aggiornare i modelli di Data Protection Agreement in base alle necessità rendendoli disponibili nella INTRANET – Sezione Trattamento Dati Personali e Privacy.

Su proposta del Presidente

e ad unanimità dei voti espressi nelle forme di legge,

D E L I B E R A

per le motivazioni indicate in premessa che qui si intendono integralmente richiamate e trascritte:

1. di approvare le Policy inerenti alla Cybersecurity e alla protezione dei dati personali (Data Protection) attraverso disposizioni attuative a tutti coloro che effettuano trattamenti di dati personali per conto del Titolare a comprova della conformità dei trattamenti al RGPD e in ossequio al principio della Responsabilizzazione ("*Accountability*") richiamato dallo stesso Regolamento;
2. di recepire le direttive n. 307 del 18 gennaio 2022 e n. 29 del 2 gennaio 2023 emanate dell'Agenzia per la Cybersicurezza nazionale;
3. di approvare l'allegata documentazione richiamata nel seguente elenco:
    - Allegato 1 "Linee guida sulle Misure di Sicurezza per la Data Protection";
    - Allegato 2 "Linee guida Processo gestione degli incidenti di sicurezza";
    - Allegato 3 "Linee guida sui controlli per la Cybersecurity e la Data Protection";
    - Allegato 4 "Modelli tipo Data Protection Agreement";
    - Allegato 5 "Lista controlli per la piena aderenza ai requisiti di sicurezza del datacenter e per la qualificazione dei servizi cloud e delle infrastrutture";
    - Allegato 6 "Posizionamento della strategia regionale rispetto alle iniziative dell'Agenzia per la Cybersicurezza Nazionale per la qualificazione dei Servizi Cloud e delle Infrastrutture dei Servizi Cloud.";
4. di notificare il presente provvedimento alle Direzioni Generali regionali ed agli Uffici di Diretta Collaborazione per quanto di competenza ed al fine di assicurare la massima diffusione;
5. di disporre la pubblicazione integrale del presente atto sul Bollettino Ufficiale della Regione e sul sito istituzionale dell'Ente nella sezione "Amministrazione Trasparente".

L'ISTRUTTORE **Rocco Gallucci**

IL RESPONSABILE P.O. **Nicola Petrizzi**

IL DIRIGENTE **Nicola Antonio Coluzzi**

LA PRESENTE DELIBERAZIONE È FIRMATA CON FIRMA DIGITALE QUALIFICATA. TUTTI GLI ATTI AI QUALI È FATTO RIFERIMENTO NELLA PREMESSA E NEL DISPOSITIVO DELLA DELIBERAZIONE SONO DEPOSITATI PRESSO LA STRUTTURA PROPONENTE, CHE NE CURERÀ LA CONSERVAZIONE NEI TERMINI DI LEGGE.

Del che è redatto il presente verbale che, letto e confermato, viene sottoscritto come segue:

IL SEGRETARIO **Michele Busciolano** IL PRESIDENTE **Vito Bardi**

☐ Si attesta che copia in formato digitale viene trasmessa al Consiglio Regionale tramite pec dall'Ufficio Legislativo e della Segreteria della Giunta

REGIONE BASILICATA

ALLEGATO 1

Linee guida sulle Misure di Sicurezza per la Data Protection

Indice dei contenuti

Linee guida sulle Misure di Sicurezza per la Data Protection

Lo scopo del presente documento è di fornire delle linee guida in merito alle principali categorie di misure per la sicurezza, per il Responsabile della sicurezza, gli specialisti di sicurezza e per il Security Manager al fine delle procedure di valutazione dell'efficacia delle contromisure esistenti (Assessment) ma anche per valutare l'introduzione di ulteriori contromisure a protezione di trattamenti particolarmente critici durante la valutazione di impatto o la rilevazione di incidenti.

Premessa

Un processo di analisi dei rischi, sia in ambito SGSI (Sistema di Gestione della Sicurezza delle Informazioni) sia di DPIA (Data Protection Impact Assessment), una volta conclusa la fase di valorizzazione delle vulnerabilità e minacce, porta conseguentemente alla valorizzazione delle contromisure esistenti. L'associazione di minacce e contromisure esistenti consente a questo punto di determinare il rischio effettivo che sarà confrontato con un valore di rischio accettabile, precedentemente definito in associazione fra il Titolare e il DPO. Qualora il valore di rischio sia entro la soglia di accettabilità il trattamento potrà essere definito sufficientemente sicuro e si potrà procedere alla formalizzazione dei risultati in ambito SGSI e/o DPIA. Nel caso in cui invece il valore di rischio residuo risulti sopra la soglia di accettabilità si dovrà procedere a rivedere le contromisure applicate, alzando il livello di implementazione delle contromisure esistenti oppure introducendo nuove contromisure più efficaci a protezione del trattamento analizzato.

Sinergia del sistema di protezione

Per rendere efficace ed efficiente il Processo di Gestione della Sicurezza delle Informazioni, l'approccio all'Information Security deve essere un lavoro comune, che implica la partecipazione ed il supporto di tutti gli attori interni, integrata anche con la partecipazione consapevole di fornitori e soggetti esterni. Questo approccio integrato permetterà di ottenere un sistema di protezione globale ed uniforme nei vari ambiti tecnologici, logistici ed organizzativi dell'Amministrazione. La mancanza, o la non applicazione, di criteri di riferimento, che indirizzino tutte le funzioni su quanto di loro competenza nel processo di costruzione della sicurezza determina una disomogeneità del Sistema di Gestione della Sicurezza delle Informazioni. Di conseguenza, la presenza di discontinuità nel livello di protezione costruito su un sistema/servizio, vanifica taluni controlli di sicurezza introdotti, che di per sé innalzerebbero il livello di sicurezza. Per una gestione efficace della sicurezza delle informazioni, si ritengono importanti i seguenti fattori:

a) la politica di sicurezza delle informazioni e le attività che riflettono gli obiettivi gestionali in essa contenuti;
b) l'approccio al modello di gestione della sicurezza delle informazioni coerente con la cultura dell'Amministrazione;
c) il supporto visibile della Direzione Generale dell'Ente;
d) la buona comprensione dei requisiti di sicurezza, valutazione e gestione dei rischi;
e) la divulgazione efficace dei principi della sicurezza delle informazioni alle risorse coinvolte in tutti i processi;
f) una distribuzione e condivisione ai soggetti interessati delle informazioni importanti così che ogni attore del sistema possa contribuire a garantire la sicurezza delle informazioni;
g) la garanzia di addestramento e formazione inerenti la sicurezza delle informazioni;
h) un sistema di gestione basato sul modello PDCA (Plan – Do – Check – Action) a garanzia di un presidio continuo ed efficace degli aspetti di Sicurezza in ottica di miglioramento continuo;

i) un sistema di misura per valutare le prestazioni del sistema di gestione implementato nonché strumenti di raccolta dei suggerimenti.

Fonti per l'individuazione dei controlli di Sicurezza

I requisiti di sicurezza del sistema informativo sono identificati ed aggiornati mediante il ricorso a tre fonti principali:

a) la valutazione dei rischi per il sistema informativo. Questa fonte consente di individuare le minacce, valutare la vulnerabilità e la probabilità di accadimento delle minacce oltre a stimarne l'eventuale impatto;
b) i requisiti legali, prescritti da leggi e normative cogenti fra cui in particolare il Regolamento Ue 679/2016, i modelli organizzativi e regolamenti interni derivanti dall'applicazione di leggi e normative cogenti, normative e linee guida facoltative (es. ISO/IEC 27001, ISO/IEC 27701, ISDP©10003), vincoli contrattuali;
c) una specifica serie di principi, esperienze, best practice, elaborazioni dello stato dell'arte ed obiettivi per il trattamento dei dati all'interno dell'Amministrazione.

Misure di sicurezza generali (SGSI)

Fermo restando che l'applicazione di specifici controlli di sicurezza è soggetta alle buone prassi riportate all'interno del precedente paragrafo (fra cui in primis l'analisi dei rischi) esistono comunque delle classi di contromisure da cui un'organizzazione complessa e articolata quale la Regione Basilicata non può prescindere per una realizzazione di un sistema di gestione della sicurezza delle informazioni efficace. In altre parole, è difficilmente immaginabile un SGSI in grado di garantire una buona protezione in ambito Data Protection by Default senza l'applicazione di buona parte dei controlli di sicurezza di seguito trattati. Le misure di Sicurezza di un buon sistema di gestione della sicurezza delle informazioni in ottica di Data Protection, si possono rappresentare e sviluppare secondo i seguenti capisaldi:

1. Sicurezza delle Identità
2. Sicurezza dei Dispositivi di accesso
3. Sicurezza delle Reti
4. Sicurezza dei Sistemi
5. Sicurezza Organizzativa
6. Sicurezza Fisica
7. Disaster Recovery e continuità operativa

1. Sicurezza delle Identità

La sicurezza delle identità e degli accessi includono tutte le misure di sicurezza (organizzative, logiche e fisiche) volte a garantire - in maniera univoca - l'identità di un soggetto (persona fisica) accedente ad informazioni digitali e/o cartacee. Tali misure devono garantire inoltre un'associazione certa e tracciabile nel tempo fra l'identità personale del soggetto e tutte le sue credenziali di accesso (logiche o fisiche) all'informazione.

È di fondamentale importanza la possibilità di identificare e riconoscere le persone che utilizzano e trattano i dati, fra cui in modo particolare i dati personali. La responsabilità individuale nei trattamenti è fondamentale per poter prevenire e correggere comportamenti che, sia per errore che per volontà, possano minare

l'integrità, la disponibilità e la riservatezza dei dati. La creazione di un sistema in grado di gestire correttamente l'abbinamento fra l'identità dei soggetti e le attività che gli stessi svolgono nell'ambito delle informazioni non solo è da deterrente per ogni attività dolosa ma contribuisce a creare ed elevare la consapevolezza e responsabilità, che è alla base della sicurezza delle informazioni e del principio di Accountability espresso dal regolamento europeo. La mancanza di un solido impianto per la sicurezza delle identità impedisce una corretta applicazione del modello organizzativo e delle autorizzazioni e deleghe ad operare sul dato personale.

Principali caratteristiche di un sistema di sicurezza delle identità

Di seguito un elenco non esaustivo delle principali caratteristiche di cui deve disporre un sistema di sicurezza delle identità:

1) Ogni soggetto (interno o esterno) che possa avere accesso a qualsiasi informazione classificata (ad esclusione quindi delle informazioni definite pubbliche) deve essere identificato registrando la sua identità in un apposito archivio.
2) L'identità del soggetto deve essere univoca e verificata o attraverso un documento di identità valido o attraverso il riconoscimento per mezzo di sistema pubblico di identità digitale (SPID/CNS/CIE/eIDAS).
3) Le identità digitali devono essere manutenute correttamente nel tempo attraverso un idoneo ciclo di vita.
4) Tutte le credenziali di accesso (digitali o fisiche) alle informazioni devono essere sempre nominali e associate ad una identità certa.
5) Le credenziali di accesso devono essere basate su una logica di profilazione degli utenti in base alla organizzazione aziendale e al ruolo ricoperto dall'utente rispettando comunque il principio del minimo privilegio.
6) Nella progettazione dei profili degli utenti o durante il processo di richiesta di credenziali discrezionali (ah hoc) è necessario prendere in esame gli aspetti di Segregation of duty (SOD) per evitare che un soggetto possa ricevere autorizzazioni applicative potenzialmente in conflitto fra di loro e/o che possano introdurre vulnerabilità nel sistema informativo. Il conflitto fra autorizzazioni può essere inteso sia in senso assoluto (autorizzazioni che non possono mai coesistere su uno stesso soggetto) sia in termini di utilizzo in contemporanea (autorizzazioni che possono essere assegnate e coesistere su un soggetto ma che non possono essere mai accessibili nello stesso istante).
7) Ogni accesso alle risorse informative e servizi dell'ente, di qualsiasi natura e tipologia, necessita di un'autorizzazione formale, fornita (salvo differenti disposizioni particolari) da un Responsabile della struttura organizzativa proprietaria delle informazioni o da un responsabile gerarchico in base ad un modello autorizzativo predefinito. Qualsiasi accesso a risorse informative o servizi aziendali che avvenga senza aver prima richiesto e ottenuto formale autorizzazione è da considerarsi una violazione della sicurezza.
8) Nel caso in cui si creino credenziali di accesso ai sistemi automatici (M2M) queste devono essere ricondotte comunque ad una identità di un soggetto in grado di gestirle e manutenerle nel tempo (es. sistemista, DBA, ecc.) che ne è responsabile.
9) L'accesso a funzioni privilegiate deve essere limitato agli utenti che ne hanno effettiva necessità. La gestione dei profili privilegiati deve rispondere ai seguenti principi:
    a. devono essere identificati gli utenti o le categorie di utenti alle quali devono essere concessi i privilegi;
    b. i privilegi devono essere concessi solo se esiste una reale necessità, caso per caso sulla base di specifiche esigenze.

10) Anche le credenziali utilizzate per attività di gestione e manutenzione dei sistemi e delle reti devono essere nominali e riconducibili ad una identità. Qualora questo non sia possibile per ragione tecniche insuperabili (es. sistemi di rete obsoleti) è necessario gestire comunque la tracciabilità fra l'utilizzo della credenziale generica (es. administrator) l'identità dell'utilizzatore e il periodo di utilizzo.
11) È possibile che un soggetto possegga anche più credenziali per accedere alla medesima fonte informativa sempreché tutte le credenziali facciano capo in modo certo e univoco alla medesima identità.
12) Qualsiasi credenziale che non sia riconducibile ad una identità deve essere immediatamente disabilitata rendendo impossibile l'accesso a qualsiasi tipologia di informazione.
13) Non è possibile riassegnare ad altri credenziali già usate nel passato per soggetti diversi.
14) Le attività dei soggetti all'interno dei sistemi informativi devono essere tracciate compatibilmente con quanto previsto e richiesto dalla normativa vigente e dall'analisi dei rischi. Le attività devono essere ricondotte ad una credenziale di accesso e a sua volta alla identità digitale.
15) Le indicazioni si devono applicare anche per gli accessi fisici ai locali dell'Ente richiedendo sempre l'identificazione del soggetto accedente.
16) Nel caso in cui un soggetto non abbia più nessuna collaborazione con Regione Basilicata e si renda necessario la sua dismissione e relativa chiusura di tutte le sue credenziali è necessario che la sua identità, le sue credenziali e i log delle attività rimangano memorizzate all'interno degli archivi per un tempo necessario a poter garantire la ricostruzione dell'operato del soggetto nel tempo. I tempi di conservazione devono essere comunque conformi alle normative vigenti fra cui in modo particolare il Regolamento UE 679/2016.
17) Tutte le identità e le credenziali devono essere verificate e ricontrollate da parte dei responsabili con cadenza periodica.

2. Sicurezza dei Dispositivi di Accesso

La sicurezza dei dispositivi di accesso è volta a garantire la sicurezza di tutti i dispositivi (pc, smartphone, tablet, ecc) che consentono ad un soggetto (identità) di poter accedere ad una informazione digitale o cartacea visualizzandola, trasferendola e/o memorizzandola in locale (sia sul dispositivo usato per accesso all'informazione sia su dispositivi di memoria removibili).

Per "dispositivi di accesso" si intendono tutti gli apparati hardware e virtuali che consentono la visualizzazione e la modifica di informazioni contenute all'interno dei sistemi attraverso l'utilizzo delle reti. I dispositivi di accesso possono essere dotati di sistemi di memorizzazione locale in grado di archiviare sia informazioni provenienti dai sistemi, sia informazioni create ed elaborate direttamente in locale. Le misure di sicurezza per i dispositivi di accesso impediscono l'uso improprio, accidentale o doloso del dispositivo stesso in grado di generare una vulnerabilità all'interno dei sistemi.

Dispositivi

Trusted vs UnTrusted I dispositivi di accesso ai dati possono essere classificati in due grandi insiemi:

- Dispositivi TRUSTED
- Dispositivi UNTRUSTED

Un dispositivo può essere definito "Trusted" quando è gestito in modo tale da ridurre al minimo i rischi di Sicurezza sui dati legati al suo utilizzo, a causa di errori, dolo o per omissione sia da parte dell'utilizzatore sia di azioni automatizzate (es. dispositivi messi a disposizione e gestiti da parte dell'Amministrazione).

Qualsiasi altro dispositivo che non rientra nella categoria dei "TRUSTED" è da considerarsi, di conseguenza, "Untrusted" e, come tale, deve accedere ai dati attraverso modalità tecniche che garantiscano comunque un

livello di sicurezza non minore di quelle dei dispositivi “Trusted” (in questa categoria rientrano ad esempio i dispositivi di proprietà dei dipendenti, collaboratori e consulenti esterni).

Principali caratteristiche per la sicurezza dei dispositivi di accesso

Di seguito un elenco non esaustivo delle principali caratteristiche di cui deve disporre un sistema di sicurezza dei dispositivi di accesso:

1) Ogni tipologia di dispositivo può accedere o meno ad una categoria di informazione in base alla sua classificazione di riservatezza. L’abbinamento fra la tipologia di dispositivo e la classe di informazione deve essere definita in appositi documenti di dettaglio.
2) Per ogni tipologia di dispositivo potranno essere definite regole di accesso in base alla sua classificazione a rete/sistemi. L’abbinamento fra la tipologia di dispositivo e la rete/sistema deve essere definita in appositi documenti di dettaglio.
3) La possibilità di copiare dei dati dalla rete/sistemi verso un dispositivo di accesso nella sua memoria in locale o al contrario di trasferire dai dati prodotti in locale in un dispositivo verso la rete/sistema deve essere definita ed espressamente autorizzata da appositi documenti di dettaglio.
4) I dati non possono mai risiedere in via esclusiva sui dispositivi di accesso (a prescindere dalla loro classificazione). Il dato master deve risiedere sempre all’interno dei dischi di rete dell’azienda.
5) Devono essere predisposti dei meccanismi automatici di sincronizzazione del dato in locale verso i dischi di rete aziendale al fine di salvaguardare l’integrità e la disponibilità del dato. La copia del dato da locale ai dischi di rete non deve essere lasciata alla mera volontà degli utenti.
6) I dispositivi “Untrusted” non possono, di norma, memorizzare dati in locale provenienti dalla rete/sistemi; eventuali dati memorizzati devono essere cancellati al termine del loro utilizzo
7) L’utilizzo di dispositivi UNTRUSTED all’interno di reti e sistemi della Regione Basilicata deve essere espressamente autorizzato
8) I dispositivi “Untrusted” non possono copiare informazioni prodotte in locale all’interno dei dischi di rete/sistemi.
9) Deve essere garantita, con soluzioni allo stato dell’arte, la riservatezza dei dati da chi non sia in possesso delle credenziali, anche a fronte di azioni dolose (es. cifratura dei dischi
10) Ogni dispositivo aziendale deve essere censito ed assegnato univocamente ad un soggetto utilizzatore o gestore che garantisce il rispetto di tutte le policy di sicurezza e ne è responsabile.
11) I dispositivi non ancora assegnati (magazzino, spare, jolly, ecc) devono essere custoditi in modo da impedire il loro utilizzo.
12) Devono essere emesse policy di utilizzo del dispositivo che garantiscano la continuità operativa e la salvaguardia dei dati in esso eventualmente memorizzati.
13) In caso di restituzione o dismissione di un dispositivo o di un supporto di memoria rimovibile si deve provvedere alla cancellazione in modo sicuro delle informazioni sugli stessi contenute, incluse le eventuali aree-disco temporanee del dispositivo utilizzate per la memorizzazione delle informazioni durante la sessione di lavoro. Il procedimento di rimozione deve avvenire in modo che le informazioni non siano più recuperabili.
14) Compatibilmente con i vincoli tecnologici e di budget è necessario definire degli standard relativamente ai dispositivi hardware, software e alle configurazioni da utilizzarsi al fine di aumentare il livello di sicurezza sia attraverso un maggior controllo delle vulnerabilità (minori variabili in gioco) sia attraverso una maggior intercambiabilità e sostituibilità dei dispositivi in grado di aumentare il livello di continuità operativa.

3. Sicurezza delle Reti

La sicurezza di rete (di telecomunicazioni) garantisce la sicurezza in un insieme di dispositivi collegati l'uno con l'altro da appositi canali di comunicazione (link) tali da permettere lo scambio da un utente all'altro di risorse, informazioni e dati in grado di essere visualizzati e condivisi attraverso dispositivi di accesso.

Le reti, attraverso i dispositivi di accesso, consentono agli utilizzatori (fra cui anche gli stessi elaboratori) di poter accedere al patrimonio informativo. Le misure di sicurezza delle reti sono attuate adottando misure volte a proteggerne la riservatezza, l'integrità e disponibilità delle informazioni in transito attraverso la stessa rete. Le principali misure nell'ambito delle misure di Sicurezza per la rete riguardano i seguenti ambiti:

1) Segregazione tra ambienti di rete
2) Continuità del servizio
3) Controllo degli accessi alla rete e ai sistemi
4) Definizione di contesti classificati per operatività.

Principali caratteristiche per la sicurezza delle Reti

Di seguito un elenco non esaustivo delle principali caratteristiche di cui deve disporre un sistema di sicurezza delle Reti:

1. Le reti devono essere in linea di principio segregate attraverso la creazione ambienti isolati tra loro o separati esclusivamente da un hardware o software con funzionalità di "firewall" che ne regolamenta le eventuali comunicazioni. La segregazione deve evitare il propagarsi di traffico indesiderato o malevolo tra i diversi utenti e tra gli utenti e le reti differenti garantendo il più possibile i principi di riservatezza e disponibilità delle informazioni.
2. La progettazione delle misure di sicurezza per ottenere la segregazione dei diversi Ambienti deve essere eseguita e commisurata con riferimento agli impatti che la mancanza di regole avrebbe sull'esercizio della rete nella sua globalità.
3. Il collegamento di dispositivi a reti che consentono di accedere direttamente a risorse di rete privilegiate (es. applicativi interni, share di rete, ecc.) deve avvenire sempre attraverso un'Autenticazione dell'utente alla rete stessa attraverso l'uso di credenziali autorizzate.
4. Tutti i dispositivi che accedono alla rete Intranet aziendale dovranno essere profilati identificando a quali risorse e servizi possono accedere in una logica di minimo privilegio.
5. L'accesso fisico ai dispositivi di rete (cablati o wireless) deve essere coerente sia con logiche di segregazione dei segmenti di rete (in base ai servizi accedibili) sia con le logiche di segregazione imposte dalle politiche di sicurezza fisica.
6. Deve essere presente un sistema di gestione delle patch che consenta la gestione e distribuzione, preferibilmente centralizzata, degli aggiornamenti del software degli apparati.
7. Deve essere implementato un sistema di backup delle configurazioni che consenta di garantire l'accesso o il ripristino delle configurazioni in tempi brevi.
8. Deve essere implementato un sistema di monitoraggio che consenta la visualizzazione, memorizzazione ed analisi delle performance degli apparati.
9. Deve essere presente un sistema di gestione dei log quale punto di raccolta centralizzato dei log provenienti dagli apparati

4.Sicurezza dei Sistemi

La sicurezza dei sistemi include tutte quelle misure di sicurezza volte a tutelare le informazioni tratte o gestite tramite elaboratori in modo da ridurre al minimo, i rischi:

1) di distruzione o perdita, anche accidentale delle stesse;
2) di accesso non autorizzato;
3) di effettuazione di operazioni non consentite.

Sicurezza dei Sistemi

Le politiche di sicurezza dei Sistemi includono tutte quelle misure di sicurezza volte a garantire la Riservatezza, l'Integrità e la Disponibilità delle informazioni aziendali elaborate e contenute all'interno delle architetture IT in modo da ridurre al minimo, i rischi di distruzione o perdita, anche accidentale delle stesse; di accesso non autorizzato; di effettuazione di operazioni non consentite.

Principali caratteristiche per la sicurezza dei Sistemi

Di seguito un elenco non esaustivo delle principali caratteristiche di cui deve disporre un sistema di sicurezza dei sistemi:

1. In ogni sistema dovrebbe essere presente un sistema di "Log Management" quale punto di raccolta centralizzato dei log provenienti dai dispostivi presenti nell'infrastruttura IT; tra questi i più diffusi sono gli eventi di Sistema Operativo e DataBase, sistemi di sicurezza, network elements e servizi applicativi in genere. La memorizzazione dei log raccolti deve essere basata su di un sistema avanzato di controllo di integrità, per garantire che i log memorizzati non siano stati manomessi.
2. In ogni sistema dovrebbe essere presente un "Security Information and Event Management (SIEM)" in grado di completare le funzionalità di log collecting con quelle di analisi dei log in tempo reale per dare evidenza degli eventi critici di sicurezza nell'infrastruttura IT. Dovrebbero anche essere presenti le funzionalità di analisi dei dati storici e di reportistica sui log memorizzati.
3. Dovrebbe essere presente un sistema di "Discovery and Dependency Mapping" in grado di identificare e mappare le dipendenze dei server aziendali, delle applicazioni e dei dispositivi di rete. La soluzione deve garantire un'integrazione diretta e una sincronizzazione in tempo reale con la componente di Configuration Management Database (CMDB), assicurando che i dati presenti nel CMDB siano sempre aggiornati rispetto alle modifiche apportate.
4. Dovrebbe essere presente un sistema di "Performance, Availability, Event & Impact Management" in grado di semplificare le operazioni del personale IT gestendo e monitorando il funzionamento dell'infrastruttura IT, prevenendo i problemi, identificando automaticamente le possibili cause nei vari silos tecnologici e avviando processi di valutazione e risoluzione dei problemi standardizzati. Il sistema di Performance Management dovrebbe consentire di rilevare automaticamente le relazioni intercorrenti tra i servizi aziendali memorizzate dentro il CMDB al fine di svolgere un'analisi più accurata delle possibili cause con un minor impiego di persone per la valutazione dei problemi.
5. Dovrebbe essere presente un sistema di "Incident and Problem Management" in grado di offrire un insieme di soluzioni integrate (anche al CMDB ed al sistema di monitoring) ed orientate ai servizi che permette di gestire gli incidenti e i problemi con un approccio proattivo, automatico e uniforme, basato sulle best practice dello schema ITIL.
6. I sistemi dovrebbero essere protetti da un appropriato sistema di controllo degli accessi. Il livello di sicurezza richiesto dipende dalla criticità del sistema e delle informazioni in esso contenute e corrisponderà alle scelte effettuate dal Sistema di Gestione della sicurezza dell'informazione e seguirà le procedure emanate da parte del Comitato di sicurezza. Nel caso di accesso a sistemi particolarmente vulnerabili o critici dovranno essere identificati sistemi di autenticazione forte alternativi o complementari ai sistemi di accesso di base.

7. Deve essere presente un sistema di “Identity Access Management (IAM)” in grado di gestire in automatico il ciclo di vita degli utenti basato su policy nonché il controllo degli accessi per l'intero ente.
8. Dovrebbe essere implementato un sistema di “Backup Management” che consenta di garantire, in caso di guasti hardware o di problemi software, l'accesso o il ripristino dei dati aziendali in tempi brevi.
9. Dovrebbe essere implementato un sistema di “Antivirus Management” per la gestione della protezione antivirus della rete IT aziendale (server, desktop e file server).
10. Dovrebbe essere presente un sistema di “Patching Management” che consenta la gestione e distribuzione centralizzate degli aggiornamenti del software, e che automatizza la rilevazione delle vulnerabilità della sicurezza facilitandone il rimedio.
11. Dovrebbe essere presente un sistema di Hardening Management per l’attivazione di un processo di verifica e messa in sicurezza degli host, mediante l’adozione di specifiche tecniche per ridurre i punti di attacco da parte di un hacker.
12. Dovrebbero essere presenti dei servizi di “Reverse Proxy Management” che si occupino di effettuare uno "store and forward" del traffico diretto verso una delle risorse gestite (unico punto di transito e controllo delle chiamate alle varie applicazioni poste in zona demilitarizzata).
13. Dovrebbe essere implementato il protocollo Network Time Protocol (NTP) per consentire di sincronizzare l’orologio interno di un sistema attraverso uno o più time server, rendendo così la data del sistema affidabile e conseguentemente anche quella ridistribuita ai client della rete locale.
14. Dovrebbe essere implementato un sistema di Firewall Management che consenta di proteggere il perimetro della rete IT aziendale dagli attacchi più comuni definendo opportune Access Control List e Policy.
15. Dovrebbe essere implementato un sistema di Vulnerability scanning / assessment in grado di analizzare l'eventuale presenza di vulnerabilità per i sistemi ed i servizi esposti, con identificazione delle possibili ed ulteriori contromisure da attivare.

5. Sicurezza organizzativa

Le Misure di Sicurezza organizzativa integrano i controlli e le contromisure di Sicurezza Logica e Fisica tramite la definizione, l’adozione e gestione di modelli organizzativi comprendenti la separazione funzionale, aspetti di formazione, conformità, metodologie, audit e controllo, analisi vulnerabilità e minacce, ecc.

Obiettivo di tali politiche è quello di integrare i controlli e le contromisure di Sicurezza Logica e Fisica tramite la definizione e la gestione di raccomandazioni organizzative.

Principali caratteristiche per la Sicurezza Organizzativa

Di seguito un elenco non esaustivo delle principali caratteristiche di cui deve disporre un sistema di sicurezza:

1. Conformità alle leggi in vigore. Per garantire tale principio le fonti normative devono costantemente essere monitorate;
2. Conformità alle normative emanate dall’Amministrazione. Per garantire tale requisito deve essere costantemente monitorata l’emissione di Linea Guida e Normative da parte delle strutture dedicate alla gestione della Sicurezza e delle normative dell’Amministrazione;
3. Continuo aggiornamento del Corpo Procedurale in base allo scenario tecnologico, agli incidenti di Sicurezza e alle attività di Auditing e Risk Assessment;
4. Allineamento dei processi di software management alle norme di legge che tutelano il diritto di proprietà intellettuale;

5. Censimento periodico delle informazioni e dei relativi processi e adozione di un sistema di classificazione delle informazioni in grado di suddividere le informazioni Aziendali in relazione al loro livello di riservatezza;
6. Analisi delle minacce attraverso lo studio di tutti gli agenti (esterni o interni) che possono causare un danno (impatto) sugli Asset dell'Amministrazione;
7. Analisi delle vulnerabilità attraverso lo studio dei fattori di debolezza sia interni agli Asset (ovvero dipendenti dalle caratteristiche dell'Asset stesso) che esterni (ovvero dipendenti da carenze nella implementazione delle contromisure poste a protezione dell'Asset);
8. Calcolo periodico del valore del rischio considerando il valore dell'Asset, le vulnerabilità ad esso associate, le minacce a cui è sottoposto e la loro probabilità di accadimento;
9. Individuazione delle contromisure e dei controlli da implementare sulla base del livello di rischio calcolato e di una analisi dei costi/benefici (derivanti dalla implementazione dei controlli e delle contromisure di sicurezza);
10. Pianificazione ed esecuzione periodica dei controlli di sicurezza al fine di monitorare la corretta applicazione delle Politiche Regionali, le normative e le procedure di sicurezza in essere. Revisione delle politiche e del sistema di gestione della sicurezza delle informazioni anche in base agli esiti dei controlli.
11. Definizione di obiettivi per la sicurezza delle informazioni che: a) siano coerenti con le politiche emesse b) siano misurabili c) tengano conto degli elementi emersi dall'analisi dei rischi, d) siano comunicati alla struttura e) siano aggiornati;
12. Formazione di tutto il personale destinato a gestire informazioni aziendali sulla rilevanza strategica di un Sistema di Gestione della sicurezza delle Informazioni;
13. Definizione di accordi di riservatezza e non divulgazione previsti dal contratto di lavoro, dal Codice Etico e dalle disposizioni aziendali sulla privacy per i dipendenti che ricoprono incarichi strategici e/o che hanno necessità di accedere a informazioni aziendali;
14. Informazione ed istruzione di tutto il personale sugli aspetti di sicurezza e sul Corpo Procedurale di Sicurezza attraverso la diffusione di un preciso e definito programma di sensibilizzazione. L'efficacia di tali programmi deve essere verificata periodicamente;
15. Gestione della continuità operativa comprendente tutte le iniziative volte a ridurre a un livello ritenuto accettabile i danni conseguenti a incidenti/catastrofi che colpiscono direttamente o indirettamente l'Azienda;
16. Gestione degli incidenti con particolare attenzione alla definizione di processi e procedure operative per il governo dell'emergenza ed il ripristino della continuità operativa. Definizione dei processi e regole per la segnalazione e registrazione degli incidenti agli organismi interni e ad eventuali organismi esterni quando richiesto dalla legge (es. segnalazioni al garante privacy);
17. Definizione di normative comportamentali volte a regolamentare aspetti quali: Principi generali di comportamento e di controllo, utilizzo delle postazioni di lavoro, Back-up e utilizzo dei supporti magnetici, Eventi lesivi e modalità di segnalazione, Identificazione e autenticazione degli utenti, Utilizzo delle risorse di rete, Utilizzo della Posta Elettronica, Utilizzo di Internet, Clean Desk e Clean Screen Policy, Segnalazione degli incidenti di sicurezza logica, ecc;
18. Tutto il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) deve essere strutturato sulla base di un classico modello PDCA.

6. Sicurezza Fisica

Le misure di sicurezza fisica sono volte a garantire il controllo degli accessi fisici onde impedire l'ingresso a persone non autorizzate che possono creare, volontariamente o no, danni o interferenze. Sono inoltre fondamentali per garantire un sufficiente grado di protezione del patrimonio informatico da eventi di origine naturale o dolosa che possono in qualche misura minare l'integrità e la disponibilità dei sistemi e ovviamente

dei dati. Il perimetro di interesse è esteso sia agli ambienti di lavoro sia agli ambienti tecnologici quali data center, nodi di rete, alle infrastrutture ed agli impianti.

La Sicurezza Fisica definisce e regolamenta le modalità di protezione dei beni fisici Regionali (persone, strutture, macchinari, documentazione).

1) Al fine di garantire il controllo degli accessi dei Dipendenti, Fornitori e utenti della Regione Basilicata e per la sicurezza fisica nel Data Center devono essere identificati diversi livelli di accesso.
2) I livelli di accesso fisico devono essere coerenti con: a) ruolo e responsabilità delle varie tipologie di utenti ammessi. b) accesso alle risorse di rete e sistemi
3) Gli accessi fisici vanno controllati attraverso sistemi di autorizzazione e monitoraggio degli accessi alle sedi, accessi alle sale macchine del Data Center, sistemi antiintrusione, ecc.
4) Ogni soggetto (interno o esterno) che possa avere accesso ai locali dell'Amministrazione deve essere identificato registrando la sua identità in apposito archivio. L'identità del soggetto deve essere verificata o attraverso un documento di identità valido.
5) Ogni accesso ai locali dell'Amministrazione necessita di un'autorizzazione formale, fornita (salvo differenti disposizioni particolari) da un Responsabile in base ad un modello autorizzativo predefinito. Qualsiasi accesso ai locali dell'Amministrazione senza aver prima richiesto e ottenuto formale autorizzazione è da considerarsi una violazione della sicurezza.
6) Il rilascio delle credenziali di accesso (es. badge, chiavi meccaniche, ecc.) deve essere basato su una logica di profilazione degli utenti in base alla organizzazione aziendale e al ruolo ricoperto dall'utente rispettando comunque il principio del minimo privilegio.
7) È necessario mantenere la registrazione di tutti gli accessi effettuati alle aree protette (es. Data Center) associati univocamente alle credenziali (es. badge) utilizzati per l'accesso.
8) Deve essere gestito e manutenuto un inventario di tutti gli apparati installati presso i locali della Regione Basilicata con una particolare attenzione ai locali protetti (es. Data Center). L'inventario deve essere costantemente aggiornato sia per le nuove installazioni sia per le sostituzioni o rimozioni di componenti. Ogni ingresso o uscita di apparecchiature Hardware dai locali protetti (es. Datacenter) deve essere controllato ed espressamente autorizzato.
9) La Sicurezza ambientale va gestita attraverso l'adozione di Sistemi antincendio, Allarmi antiallagamento, continuità dell'alimentazione elettrica, allarmi ambientali, ecc.
10) I locali destinati ad archivi per le copie di sicurezza dei dati vanno protetti attraverso sistemi di serrature a chiave non duplicabile, armadi e casseforti di sicurezza e ignifughe, ecc.
11) i documenti e i supporti contenenti dati sensibili o giudiziari devono essere custoditi in appositi archivi ad essi esclusivamente dedicati;
12) Tutti i dati personali non più necessari, fatto salvo i casi prescritti dalla legge, devono essere distrutti e rimossi dagli archivi.
13) aree a cui si applicano i controlli descritti nella presente linea guida, sono definite "aree protette". In particolare, le "aree protette" sono tutte quelle aree che possiedono almeno una di queste caratteristiche: a. aree in cui sono presenti le postazioni operative per la gestione e monitoraggio del Datacenter e della rete; b. aree in cui sono presenti postazioni dedicate allo sviluppo e test; c. aree in cui sono presenti apparecchiature critiche di rete, del Datacenter e di supporto. Le misure che si adottano per controllare l'accesso a tali "aree protette" sono tese a garantire un adeguato livello di sicurezza, che consenta l'ingresso e la permanenza nei locali esclusivamente del personale in turno di servizio o di personale autorizzato, prevenendo furti e danneggiamenti alle apparecchiature o accesso non autorizzato alle informazioni. I controlli applicati per le diverse aree descritte nelle presenti politiche possono differire in funzione della tipologia delle risorse del Sistema Informativo che vi sono allocate.

7. Disaster Recovery e continuità operativa

Le misure di Disaster Recovery e Continuità Operativa sono rispettivamente tutte quelle misure tecniche utili per affrontare un eventuale disastro che colpisce i sistemi informativi aziendali (es. catastrofi naturali come alluvioni o terremoti, errori umani, furti o attacchi hacker, ecc.) e l'insieme di attività volte a minimizzare gli effetti distruttivi, o comunque dannosi, di un evento che ha colpito un'organizzazione o parte di essa, garantendo la continuità delle attività più in generale.

Le misure di Disaster Recovery indicano tutte le misure tecniche utili per affrontare un eventuale disastro che colpisca i sistemi informativi aziendali e che può avere diversa origine: catastrofi naturali come alluvioni o terremoti, errori umani, furti o attacchi hacker. Il piano di Disaster Recovery stabilisce in primis quali sono i processi aziendali critici per un business, ossia quelli che devono essere maggiormente monitorati e protetti. Definisce poi i parametri di RTO e RPO (tempi di ripristino e livello di perdita dati accettabile) a seconda delle esigenze della specifica azienda e pianifica le azioni da intraprendere per il ripristino totale e più rapido possibile di sistemi, dati e applicazioni in caso di incidente. Le misure di Business Continuity, invece, si riferiscono ad una soluzione globale, che comprende tutte le procedure e i processi che hanno lo scopo di garantire la continuità del business e di evitare l'interruzione delle attività, sia dovute a disservizi del reparto IT che a cause di altra natura, come ad esempio incidenti di origine legale, o fermo dell'attività causato da mancanza di personale. La strategia di Business Continuity tiene conto di tutti gli eventi che possono minacciare la sopravvivenza del business ed è utile anche nel caso di interruzioni minori dell'operatività. In linea di massima, quindi, le misure di Disaster Recovery e Business Continuity sono misure di sicurezza fondamentali per garantire la disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali, e nel contempo garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico come richiesto dall'art. 32 del GDPR.

Principali caratteristiche per la Business Continuity e Disaster Recovery

1. È necessario determinare i propri requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in situazioni avverse, per esempio durante crisi o disastri, individuando i processi per la gestione tempestiva di possibili eventi critici futuri che potrebbero minacciare la sopravvivenza dell'ente.
2. Occorre stabilire, documentare, attuare e mantenere processi, procedure e controlli per assicurare il livello di continuità richiesto per la sicurezza delle informazioni durante una situazione avversa.
3. Occorre verificare ad intervalli di tempo regolari i controlli di continuità della sicurezza delle informazioni stabiliti e attuati, al fine di assicurare che siano validi ed efficaci durante situazioni avverse.
4. Le strutture per l'elaborazione delle informazioni devono essere realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità prevedendo se necessario anche soluzioni di Disaster Recovery.

Misure di sicurezza "specifiche" per la Data Protection

Nonostante il sistema di misure di sicurezza contenuto nel GDPR non preveda più un elenco tassativo e specifico di misure minime (come nel Codice Privacy – Dlgs 196/03 e ss.mm.ii.), in diversi passaggi, primo fra tutti l'art. 32 comma 1 (oltre al considerando nr. 83), si indicano la cifratura dei dati e degli archivi e la pseudonimizzazione delle informazioni, come tecniche suggerite per aumentare la protezione dei dati, soprattutto di quelli di particolari categorie (es. dati giudiziari, dati sanitari, religiosi, ecc.). L'idea è quella che un'eventuale fuga di questi dati faccia sì che le informazioni reperibili siano visibili, ma assolutamente incomprensibili o destrutturate, ossia separate da altre informazioni che sarebbero in grado di dar loro un senso. La crittografia e pseudonimizzazione richiedono comunque la definizione di precise regole ("policy")

per una corretta gestione del sistema e per normare anche i comportamenti degli utenti che altrimenti rischierebbero di inficiare l'efficacia di questi due strumenti di sicurezza. Si tratta quindi di meccanismi che di certo riducono i rischi connessi al trattamento di dati personali e che contribuiscono a rendere i titolari/responsabili del trattamento conformi alle nuove regole sulla privacy aumentando notevolmente il livello di riservatezza, ma che a volte rendono più onerosa la gestione del dato e, in taluni casi, possono introdurre anche potenziali vulnerabilità in ambito disponibilità e integrità dell'informazione. L'uso quindi di tali tecniche non deve essere indiscriminato e condotto a tappeto su tutti i dati e trattamenti, ma deve essere sempre ricondotto ad una valutazione di rischio/opportunità, nella quale rimangono centrali sia i diritti dell'interessato sia le capacità organizzative e di spesa dell'Ente.

Crittografia

La crittografia (o cifratura) si basa, di solito, su un algoritmo di cifratura e su una passphrase e/o token che "aprono" e "chiudono" i dati (di solito al momento dell'autenticazione). Si tratta di una procedura che è trasparente per l'utente ma che protegge l'informazione con modalità che sono, nella maggior parte dei casi, indecifrabili. La cifratura può diventare uno strumento di protezione fondamentale per grandi quantità di dati, per sistemi che gestiscono credenziali, per quelli che trattano dati sensibili (dati sanitari, giudiziari, ecc.), per i computer che processano una grande mole d'informazioni per profilare i consumatori. Peraltro, l'utilizzo della cifratura offre un'ulteriore tutela anche nei confronti del titolare/responsabile che nel caso di data breach (accertato) è molto probabilmente esentato dall'obbligo di comunicare l'evento alle autorità di controllo e agli interessati in considerazione del fatto che è molto improbabile che la violazione dei dati personali (cifrati) presenti un rischio per i diritti e le libertà delle persone fisiche.

Pseudonimizzazione

L'uso di pseudonimi prevede il trattamento dei dati personali in modo tale che essi non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative tese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. Può essere usato, ad esempio, un unico pseudonimo riferito ad un insieme univoco di dati, ma anche un singolo pseudonimo per ogni specifico dato. In sostanza, la pseudonimizzazione perché sia efficace, deve: a. prevedere l'assenza di identificabilità diretta del soggetto interessato (trattamento dei dati personali in modo tale che i dati non possano essere più attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive); b. adottare misure di sicurezza ulteriori da aggiungere alla pseudonimizzazione; c. incorporare la pseudonimizzazione nella privacy-by-design (misure tecniche e organizzative volte a garantire che tali dati personali non siano più attribuibili ad una persona fisica). È importante sottolineare che, se da una parte l'utilizzo delle tecniche di pseudonimizzazione, oltre che essere richiamato e caldeggiato in vari punti del regolamento europeo, rappresenta una delle tecniche più importanti ed interessanti ai fini della protezione del dato personale, dall'altra spesso non garantisce in modo assoluto, (da sola) la protezione del dato personale. Rimane, infatti, fondamentale accertarsi che i dati, resi privi, della loro identificabilità diretta (processo di pseudonimizzazione) non consentano comunque, attraverso la loro interpretazione e correlazione, di ricondurre comunque ad un soggetto univoco.

Anonimizzazione

Mediante l'anonimizzazione, viene rimosso e/o modificato qualsiasi elemento riconoscibile che possa consentire di risalire ad un soggetto specifico identificandolo sia attraverso dati anagrafici/identificativi diretti (es. nome, cognome, codice fiscale, ecc.), sia attraverso la correlazione di informazioni "secondarie" che, opportunamente associate ed elaborate, possono comunque portare all'identificazione del soggetto (altezza, peso, data di nascita, ecc.) A questo punto il dato perde il suo status di dato personale (pur mantenendo comunque una valenza statistica/business) rendendo quindi non necessarie particolari forme di protezione dello stesso. Le tecniche di anonimizzazione possono essere molteplici; si citano, ad esempio, le seguenti:

- Aggiunta del rumore statistico -> tecnica che consiste nell'alterazione degli attributi contenuti in un set di dati in modo tale da renderli meno precisi, mantenendo allo stesso tempo la composizione generale (es. arrotondamento di alcuni valori).
- Generalizzazione -> tecnica che consiste nell'estendere le scale di grandezza, generalizzando gli attributi riferiti ad uno stesso gruppo di soggetti (ad es. un mese al posto di una settimana; una regione al posto di un paese).
- Scrambling -> tecnica che consente di offuscare le lettere dell'alfabeto mescolandole tra loro o sostituendole con simboli e/o lettere speciali. Nei processi di anonimizzazione (per loro natura irreversibili) si tenga presente che i diritti dell'interessato non sono limitati alla sola riservatezza ma spesso anche ai principi di disponibilità ed integrità. Ciò significa che in taluni casi forme di anonimizzazione su alcuni trattamenti potrebbero garantire la riservatezza, ma nel contempo potrebbero ledere i diritti dell'interessato non consentendo più allo stesso di esercitare i propri diritti (es. accesso e portabilità del dato).

REGIONE BASILICATA

ALLEGATO 2

Linee guida Processo gestione degli incidenti di sicurezza

Linee guida Processo gestione degli incidenti di sicurezza

Indice dei contenuti

Processo gestione degli incidenti di sicurezza

Il presente documento descrive in termini di obiettivi, attività, ruoli e responsabilità della procedura di gestione degli incidenti intesi come eventi che hanno avuto effetti negativi in termini di Data Protection o solo hanno messo in evidenza delle criticità all'interno delle misure di sicurezza adottate.

La presente procedura definisce le principali responsabilità ed attività relative agli obblighi di notifica verso gli Organismi di Controllo degli incidenti di Sicurezza delle Informazioni che abbiano come conseguenza la violazione di dati personali.

La procedura è redatta in coerenza con il Regolamento Europeo 679/2016 relativo *"alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"* (altrimenti detto GDPR); in base alle line guida del Gruppo dei garanti (art.29) denominate "WP250 - Guidelines on Personal data breach notification under Regulation 2016/679" del 3 ottobre 2017 e sulla base delle "Indicazioni operative per la definite dal Presidente del CICO con propria nota prot. n. 83134 del 16/05/2019.

Al di là delle misure di sicurezza adottate ed adottabili, che possono essere di natura sia tecnologica che organizzativa, una corretta gestione degli incidenti di sicurezza permette, infatti, di:

- -migliorare continuamente la capacità di prevenire incidenti a tutela della sicurezza dei sistemi e delle informazioni gestite dall'Amministrazione;
- evitare o minimizzare la compromissione dei dati trattati in caso di incidente, migliorando la capacità di risposta agli incidenti stessi.

Riferimenti

Di seguito l'elenco dei documenti che costituiscono il riferimento per le presenti linee guida:

- D.Lgs. n. 196/03 Codice in materia di protezione dei dati personali e successive modifiche e integrazioni;
- Regolamento UE n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati);
- Deliberazione di Giunta Regionale n. 540 del 17 luglio 2021, recante " ATTUAZIONE DEGLI ADEMPIMENTI PREVISTI DALLA NORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI Regolamento (UE) 2016/679 - RIDEFINIZIONE MODELLO ORGANIZZATIVO;
- Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) – WP 250, adottate dal Gruppo di lavoro Art. 29 il 06 febbraio 2018;
- Provvedimento n. 157 del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali;

- Linee guida in materia di notifica delle violazioni di dati personali (Examples regarding Data Breach Notification), adottate dall'European Data Protection Board il 14 gennaio 2021;
- Provvedimento n. 209 del Garante del 27 maggio 2021 sulla Procedura telematica per la notifica di violazioni di dati personali (data breach).

Definizione di violazione di dati personali

Con il termine "violazione dei dati personali" (in inglese "data breach"), art. 4 par. 12 RGPD, si intende una situazione che può comportare, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso a informazioni qualificate dal Regolamento come dati personali trasmessi, memorizzati o elaborati per mezzo di sistemi informatici o di altra natura.

Il Titolare e il Responsabile del trattamento devono garantire:

- la **Riservatezza** (confidentiality) delle informazioni: capacità di tenere protetti dati da chi non è autorizzato a vederli. La protezione dei dati può essere assicurata mediante soluzioni tecniche (es. criptare i dati).
  Pertanto, per garantire la riservatezza devono sussistere le condizioni di accessibilità e di utilizzabilità delle informazioni ma solo da un soggetto autorizzato. Si ratta di una condizione strettamente connessa alla sicurezza e, pertanto, le informazioni devono essere accessibili unicamente a chi è autorizzato;
- **l'Integrità** (integrity) delle informazioni, definita come "proprietà di accuratezza e completezza" (in inglese "property of accuracy and completeness").
  Il termine "accuratezza" ha una portata tecnica e va qualificato come il grado di corrispondenza tra il dato teorico e il dato reale e ciò vuol dire che il dato non deve essere alterato. Il dato che risulta modificato o cancellato non è ovviamente sicuro, posto che siamo in termini di sicurezza;

- la **disponibilità** (availability) delle informazioni, definita come la "proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata" (in inglese "property of being accessible and usable on demand by an authorized entity"). Accessibilità e utilizzabilità sono le prerogative che qualificano la disponibilità di un dato, ma si deve considerare anche l'aspetto della richiesta di un soggetto autorizzato e ciò implica anche l'individuazione dei tempi per l'usabilità". L'espressione "su richiesta" non può essere identificata con "immediatezza", posto che potrebbero essere necessari tempi per rendere accessibile e utilizzabile una determinata informazione.

Di seguito si riportano le principali possibili violazioni di dati personali identificate:

- furto o smarrimento di beni dell'Amministrazione, connesso ad un comportamento negligente di dipendenti/collaboratori, che può verificarsi nel caso in cui venga meno il controllo degli strumenti utilizzati per elaborare i dati personali (i.e. Server, PC/laptop, smartphone, device per l'archiviazione di dati esterni);
- accesso illegale da parte di soggetti terzi, ossia accesso abusivo da parte di terzi, non autorizzati, ai sistemi informatici, ad esempio, mediante:

    - un attacco ransomware, mirato al furto di documenti. Questo tipo di attacco di solito può essere classificato come violazione della disponibilità dei dati personali, ma spesso potrebbe verificarsi anche una violazione della riservatezza degli stessi;
    - attacchi injection (SQL injection, path traversal). Tali attacchi mirano a copiare e abusare dei dati personali. Si tratta principalmente di violazioni della riservatezza, ma spesso potrebbe verificarsi anche una violazione dell'integrità degli stessi;
    - attacchi phising, ossia truffe informatiche effettuate inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati, motivando tale richiesta con ragioni di ordine tecnico. Tali attacchi sono classificati come violazioni della riservatezza dei dati personali;
- errore accidentale da parte di uno dei soggetti che trattano dati personali (i.e. invio di una mail contenente dati personali ad un destinatario errato);
- furto di informazioni, può verificarsi nel caso in cui un dipendente (o ex dipendente) sfrutti la propria conoscenza o le proprie autorizzazioni per sottrarre dolosamente dati/informazioni di carattere personale;
- vigilanza/adozione di misure di sicurezza, qualora, a causa di un'erronea valutazione sul livello di criticità dei dati e/o informazioni ministeriali, non siano state poste in essere le necessarie precauzioni volte alla salvaguardia dei dati medesimi, che sono stati perduti.

Matrice ruoli responsabilità

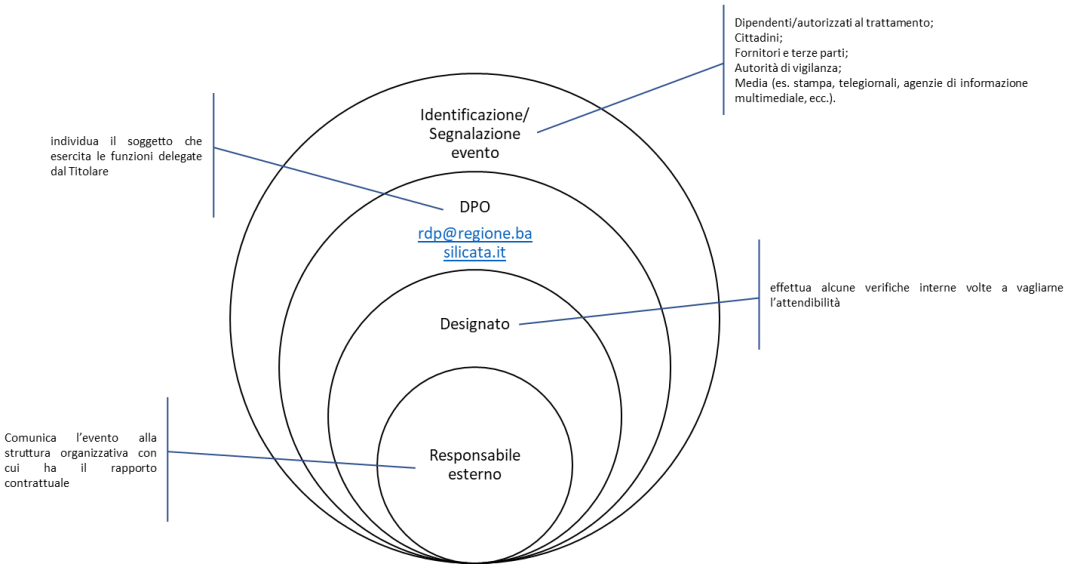
Ruolo / Struttura	**Responsabilità principali relative alla Procedura**
Soggetto che esercita le funzioni di **Titolare (Direttori Generali)** o per il tramite dei Designati (Dirigenti) del trattamento:	- Dopo aver valutato la portata e il livello di rischio della avvenuta violazione di dati personali, si occupa di individuare e adottare possibili misure di rimedio e, ove necessario, di notificare la violazione all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza, salvo che si riveli improbabile che la violazione medesima possa presentare un rischio per i diritti e le libertà delle persone fisiche. - Comunica la violazione agli interessati, qualora la stessa sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Prevede attività di verifiche periodiche volte a garantire l'efficacia delle procedure e degli strumenti di risposta agli incidenti relativi alle violazioni di dati personali.
Responsabile interno del trattamento **(Designato)**: in qualità di Dirigente a capo dell'unità organizzativa dove si è verificata la violazione, supporta il soggetto che esercita le funzioni di Titolare del trattamento nella gestione della violazione dei dati, svolgendo le seguenti attività:	- adotta le misure di sicurezza tecnico/organizzative previste dalla normativa interna; - coordina le attività degli autorizzati al trattamento e si interfaccia con gli Amministratori di Sistema; - ove ritenga che l'incidente occorso possa aver comportato una violazione dei dati personali, informa senza ritardo il soggetto che esercita le funzioni di Titolare del trattamento; - fornisce, con l'ausilio degli autorizzati al trattamento, degli Amministratori di Sistema, e dei referenti privacy, elementi utili all'esercente le funzioni di Titolare per l'eventuale predisposizione delle eventuali comunicazioni da trasmettere al Garante privacy e agli interessati. - ove necessario, collabora con il soggetto che esercita le funzioni di Titolare per la notifica della violazione all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza, salvo che si riveli improbabile che la violazione medesima possa presentare un

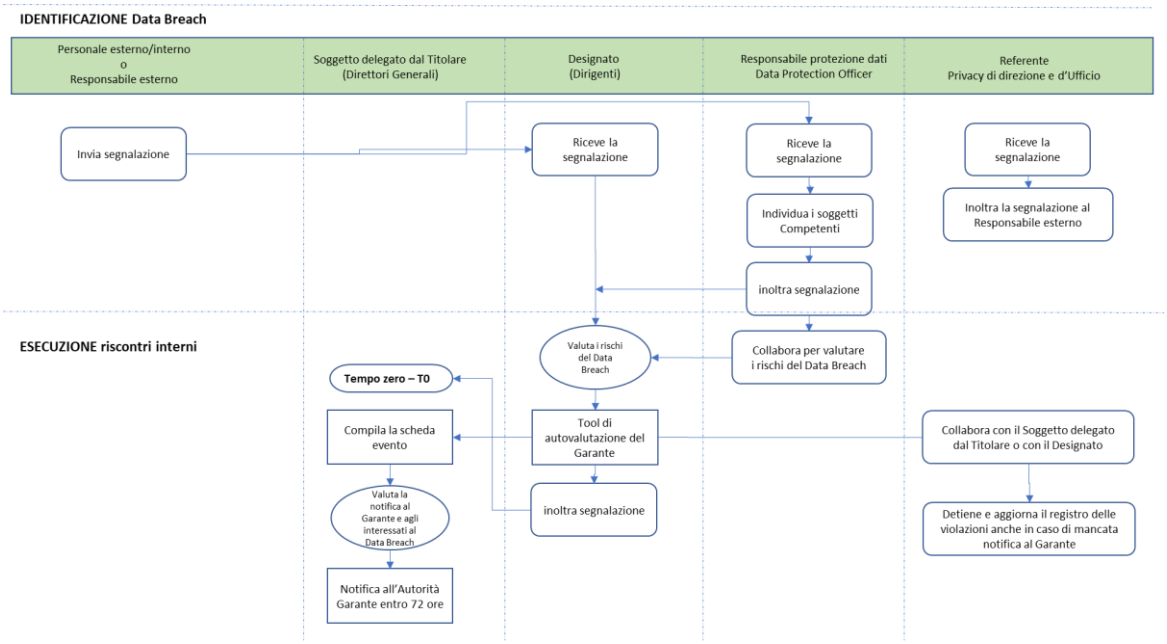
	rischio per i diritti e le libertà delle persone fisiche. - Comunica la violazione agli interessati, qualora la stessa sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Prevede attività di verifiche periodiche volte a garantire l'efficacia delle procedure e degli strumenti di risposta agli incidenti relativi alle violazioni di dati personali.
Responsabile della Protezione dei Dati o Data Protection Officer:	Funge da punto di contatto tra il Titolare, il Garante e gli interessati; nell'ambito della gestione degli incidenti, raccoglie tutte le possibili violazioni di dati personali e individua il soggetto che esercita le funzioni di Titolare che sarà competente per la gestione della eventuale violazione. Avvalendosi della collaborazione delle risorse a sua disposizione e dei referenti privacy, può essere consultato dal soggetto che esercita le funzioni di Titolare nell'attività di valutazione della avvenuta violazione di dati e nella gestione dei rapporti con il Garante. Il RPD ha una funzione di consulenza e supporto, non potendosi in alcun caso sostituire al soggetto che esercita le funzioni di Titolare nell'assolvimento dei compiti e nelle decisioni che spettano a quest'ultimo, salva diversa disposizione di legge.
Referente privacy: svolge attività di supporto al soggetto che esercita le funzioni di Titolare per le questioni relative alla tutela dei dati personali trattati e rappresenta il punto di contatto con il RPD. In tale veste, il referente si occupa di:	- raccogliere le segnalazioni di potenziali data breach, ricevute dal RPD, ovvero da qualsiasi altra fonte esterna o interna, e di trasmettere immediatamente le stesse al responsabile interno coinvolto; - coadiuvare il responsabile interno e colui che esercita le funzioni di Titolare nella valutazione della segnalazione; - tenere e aggiornare il registro delle violazioni (all. 1), secondo le istruzioni illustrate nel prosieguo; - supportare il DPO qualora il soggetto che esercita le funzioni di Titolare abbia richiesto il suo intervento, anche attraverso la messa a disposizione in suo favore di tutti gli elementi valutativi necessari l'espletamento dei suoi compiti.

Autorizzati al trattamento: soggetti preposti materialmente ad una o più attività di trattamento che coadiuvano il responsabile interno/esterno del trattamento coerentemente con le responsabilità attribuitegli, svolgendo le seguenti attività:	- comunicano eventuali violazioni di dati personali di cui sono a conoscenza mediante l'invio di una comunicazione da inviare agli altri appositi strumenti e canali messi a disposizione dalla Regione; - forniscono supporto in fase identificazione dell'incidente, comunicando ai responsabili interni del trattamento informazioni utili per la classificazione delle violazioni verificatesi.
Responsabile Sistemi informativi	- Informa obbligatoriamente il DPO in merito alla rilevazione di incidenti; - Collabora attivamente nella fase di gestione degli incidenti al fine sia della loro risoluzione sia degli adempimenti richiesti dal GDPR ed è responsabile dei tempi di notifica; - Comunica periodicamente al DPO le misure di sicurezza adottate; - Si conforma nei tempi e nei modi indicati dal DPO, per il miglioramento delle misure di sicurezza.
Amministratori di Sistema: soggetti che, in qualità di preposti alle attività di gestione e manutenzione dei sistemi informatici ministeriali, coadiuvano il responsabile interno del trattamento, coerentemente con le responsabilità attribuitegli, svolgendo le seguenti attività:	- monitorano i sistemi di sicurezza; - comunicano in caso di violazione tutte le informazioni necessarie alla sua comprensione e le trasmettono ai Responsabili interni ed esterni del trattamento; - comunicano le eventuali azioni poste in essere per la gestione della violazione ai responsabili interno ed esterno del trattamento e al DPO; - monitorano nel continuo le attività necessarie a prevenire eventuali violazioni/ e le attività che rilevino le eventuali non conformità delle misure di sicurezza; - comunicano ai Responsabili interni ed esterni del trattamento e al DPO eventuali situazioni che potrebbero comportare violazioni di dati personali; - raccolgono le informazioni per quanto di competenza, necessarie a formulare compiutamente le comunicazioni verso il Garante /Interessato.

Responsabile dell'Archivio / Responsabile del patrimonio	- Informa obbligatoriamente il DPO in merito alla rilevazione di incidenti su dati conservati su supporti cartacei; - Collabora attivamente nella fase di gestione degli incidenti al fine sia della loro risoluzione sia degli adempimenti richiesti dal RGPD ed è responsabile dei tempi di notifica; - Comunica periodicamente al DPO le misure di sicurezza adottate;

Procedura di Data breach





Identificazione di un potenziale Data Breach

La fase di identificazione di una violazione di dati personali ha l'obiettivo di rilevare un potenziale data breach derivante dalla perdita, divulgazione non autorizzata, trattamento illecito e/o perdita di disponibilità di dati personali di cui l'Amministrazione è Titolare.
La procedura è attivata da chiunque venga a conoscenza, anche casualmente, di incidenti o potenziali incidenti di sicurezza nell'ambito della sicurezza delle informazioni, che abbiano come conseguenza la violazione di dati personali.
Tutte le possibili violazioni dei dati personali devono essere identificate e indirizzate tempestivamente al Responsabile della protezione dei dati.
Le segnalazioni possono provenire da fonti interne e fonti esterne all'Amministrazione, quali:

- Strumenti informatici di monitoraggio di eventi di sicurezza o attraverso misure tecniche di sicurezza finalizzate alla protezione dei sistemi informativi;
- Dipendenti/autorizzati al trattamento;
- Cittadini;
- Fornitori e terze parti;
- Autorità di vigilanza;
- Media (es. stampa, telegiornali, agenzie di informazione multimediale, ecc.).

Ogni soggetto che presta la propria attività a favore della Regione Basilicata, che venga a conoscenza o sospetti che sia avvenuta una violazione di dati personali, deve darne immediata comunicazione tramite invio di una mail all'indirizzo: rpd@regione.basilicata.it o rpd@cert.regione.basilicata.it.
La comunicazione deve contenere un'indicazione chiara dell'evento verificatosi, delle caratteristiche dei dati personali coinvolti e, ove possibile, dell'unità organizzativa interessata dalla violazione.
Il Responsabile della protezione dei dati, una volta ricevuta la comunicazione sul potenziale data breach, individua il soggetto che esercita le funzioni delegate dal Titolare (Direttore Generale) che sarà competente per la gestione della e dell'eventuale violazione e trasmette senza ritardo la comunicazione al Designato della struttura individuata.
Il Referente privacy inoltra la comunicazione pervenuta al Designato, ai Responsabili esterni, se presenti, e collabora con gli stessi nell'attività di valutazione del livello e delle potenzialità di rischio per gli interessati dell'evento descritto nella comunicazione.
Qualora la presunta violazione sia riferita a dati personali trattati da un Responsabile esterno, sarà dovere dello stesso rilevarla e darne comunicazione alla struttura organizzativa con cui ha il rapporto contrattuale. Pertanto, indipendentemente dal canale di comunicazione, il processo si attiva con l'avvenuto ricevimento della segnalazione al Responsabile esterno.

Esecuzione dei riscontri interni

Il Designato al trattamento interessato, ricevuta la comunicazione della presunta violazione di dati personali, effettua alcune verifiche interne volte a vagliarne l'attendibilità. Al fine di condurre una valutazione sulla presunta violazione, il responsabile si potrà avvalere dell'ausilio del tool di autovalutazione messo a disposizione dei titolari del trattamento dal Garante per la Protezione dei Dati personali e reperibile al seguente link https://servizi.gpdp.it/databreach/s/self-assessment . Il tool supporterà Designato nel valutare se dall'incidente di sicurezza occorso si sia verificata una violazione dei dati personali.
Nell'ambito di tali verifiche, con l'ausilio dei Referenti privacy, nonché avvalendosi della collaborazione degli autorizzati al trattamento e degli Amministratori di sistema, il Designato esegue con urgenza i riscontri preliminari e, in caso di esito positivo, comunica al soggetto che esercita le funzioni di Titolare (Direttori Generali) e al DPO l'avvenuta violazione, con specifica indicazione delle seguenti informazioni, ove disponibili:

- la Struttura coinvolta;
- la data dell'evento e l'ora della violazione anche solo presunta (specificando se è presunta);
- la data e ora in cui si è avuto conoscenza della violazione;
- la fonte di segnalazione;
- la natura dell'evento anomalo;
- una sintetica descrizione dell'evento anomalo;
- il numero e la categoria di interessati coinvolti;
- la categoria e il volume di dati personali di cui si presume la violazione;
- la descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione;
- indicazione dell'eventuale Responsabile esterno del trattamento coinvolto nella gestione del sistema informatico;
- Misure di sicurezza adottate al set di dati oggetto di violazione;
- Misure proposte per la mitigazione della presunta violazione;
- Esito della autovalutazione condotta mediante il tool messo a disposizione dal Garante per la Protezione dei Dati Personali.

La comunicazione del Designato è effettuata utilizzando l'apposita scheda dell'evento (all. 2) e comunicata tramite mail al DPO.
Qualora la violazione sia stata riscontrata dal Responsabile esterno, le verifiche del caso saranno poste in essere dal responsabile medesimo, che provvederà a darne tempestiva comunicazione tramite mail al soggetto che esercita le funzioni di Titolare del trattamento e al DPO.
Dal momento della ricezione di tale comunicazione da parte del soggetto che esercita le funzioni di Titolare del trattamento, ovvero "**Tempo zero – T0**", decorrono le tempistiche previste dal Regolamento per la gestione degli adempimenti connessi alle violazioni accertate.

Valutazione e mitigazione

Il soggetto che esercita le funzioni di Titolare del trattamento, ricevuta la comunicazione della violazione, valuta la complessità della stessa, basandosi sulle informazioni ricevute dal Designato e dal Responsabile esterno (se presente) e provvede ad aggiornare la scheda evento, avvalendosi della collaborazione del referente privacy.
Dovrà essere valutato se l'incidente può comportare un rischio per i diritti e le libertà delle persone fisiche, ovvero se può cagionare un danno fisico, materiale o immateriale alle persone fisiche, tale da provocare una o più tra le seguenti conseguenze:

a. discriminazioni;
b. furto o usurpazione di identità;
c. perdite finanziarie;
d. pregiudizio alla reputazione;
e. perdita di riservatezza dei dati personali protetti da segreto professionale;
f. decifratura non autorizzata della pseudonimizzazione;
g. qualsiasi altro danno economico o sociale significativo.

La violazione è definita complessa quando:

- i dati personali sono di carattere sensibile/particolare e/o di natura finanziaria;
- i sistemi informatici oggetto di violazione sono complessi per qualità/quantità di informazioni elaborate;
- comprende le chiavi di accesso/cifratura in possesso degli interessati (es. password).

Nel caso in cui non ricorrano le caratteristiche di cui sopra, ossia qualora i sistemi informativi coinvolti siano limitati e/o protetti da misure adeguate (es. cifratura), o qualora non siano coinvolti interessati, se non in numero limitato e i dati personali siano parziali e non associati ad altre informazioni (es. nome e cognome senza codice fiscale o carta di credito o numeri telefonici), la violazione può essere definita non complessa.
In questa fase, si raccomanda al soggetto che esercita le funzioni di Titolare del trattamento, in caso di dubbi sulla valutazione, di scegliere lo scenario di maggior tutela per gli interessati.
Per ciascuna violazione dei dati personali, devono essere identificate opportune misure correttive tecniche e organizzative da adottare, al fine di mitigare i relativi effetti e ridurre la probabilità di impatto e ricorrenza. Le misure di mitigazione dovranno essere adeguate alla natura della violazione dei dati personali.
È preferibile che nelle attività di valutazione dell'evento e di individuazione di misure di mitigazione e di rimedio l'esercente le funzioni di Titolare si avvalga della consulenza e del supporto tecnico del Responsabile della Protezione dei Dati.
Nell'ipotesi in cui risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, ossia la violazione sia stata ritenuta non complessa, il soggetto che esercita le funzioni di Titolare del trattamento non è tenuto a notificare la violazione all'Autorità Garante, pur restando fermo il dovere di censire il data breach all'interno del registro delle violazioni.

Notifica all'Autorità Garante

L'esercente le funzioni di Titolare del trattamento si avvarrà del supporto del tool messo a disposizione dei titolari del trattamento dal Garante per la Protezione dei Dati personali e reperibile al seguente link https://servizi.gpdp.it/databreach/s/self-assessment , al fine di verificare se la violazione occorsa possa rappresentare un rischio per i diritti e le libertà degli interessati. Il tool supporterà il soggetto che esercita le funzioni di Titolare nell'individuazione delle azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.
Qualora risulti probabile che il data breach possa rappresentare un rischio per i diritti e le libertà degli interessati, ossia la violazione sia stata ritenuta complessa, il soggetto che esercita le funzioni di Titolare del trattamento è tenuto a notificare l'avvenuta violazione di dati personali all'Autorità Garante entro 72 ore dal T0, di cui al paragrafo "Esecuzione controlli interni".
In questa fase è necessario coinvolgere il responsabile della protezione dei dati, che, è chiamato a esprimere un parere circa la necessità e l'opportunità di notificare l'avvenuta violazione all'Autorità Garante e di comunicare la stessa agli interessati, senza ritardo, stante la necessità di notificare la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare del trattamento è venuto a conoscenza della violazione. A tale scopo, il DPO, con l'ausilio dei referenti privacy, ha la facoltà di svolgere ulteriori riscontri necessari a completare le evidenze mancanti rispetto alle prime analisi condotte. Qualora esprima un parere, il DPO è tenuto ad aggiornare l'apposita scheda evento di cui sopra.
Il soggetto che esercita le funzioni di Titolare del trattamento, ricevuto il parere del RPD, invia la comunicazione all'Autorità Garante entro e non oltre le 72 ore dal T0 tramite l'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ .
Il parere del RPD non ha carattere né obbligatorio né vincolante, sicché l'esercente le funzioni di Titolare è tenuto, in ogni caso, a notificare la violazione al Garante ogni qual volta lo ritenga opportuno, motivando le sue valutazioni all'interno dell'apposita scheda evento.
I tempi di notifica, nonché l'oggetto delle comunicazioni inviate al Garante devono essere formalizzati all'interno del registro delle violazioni.
Nelle ipotesi in cui il soggetto che esercita le funzioni Titolare versi nel dubbio circa la complessità del data breach e ritenga necessari ulteriori riscontri, oltre il termine di 72 ore dal T0, è tenuto a comunicare comunque gli estremi della violazione all'Autorità Garante, indicando nella notifica stessa le informazioni in suo possesso e il termine entro il quale si ritiene termineranno le ulteriori attività istruttorie. Una volta compiute le verifiche necessarie, dovrà essere inviata una seconda comunicazione al Garante, in cui verranno illustrati gli esiti dei successivi riscontri effettuati e le valutazioni compiute in ordine alle conseguenze e ai potenziali rischi dell'avvenuta violazione.

Qualora l'incidente si configuri come atto doloso Il Titolare o suo Delegato in collaborazione con il Responsabile IT e il DPO, procede alla comunicazione dell'evento all'autorità giudiziaria.

Comunicazione agli interessati

Al fine di valutare se la violazione occorsa possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'esercente le funzioni di Titolare del trattamento si avvarrà del supporto del tool messo a disposizione dei titolari del trattamento dal Garante per la Protezione dei Dati personali e reperibile al seguente link https://servizi.gpdp.it/databreach/s/self-assessment .
Qualora l'esito della valutazione rappresenti che la violazione dei dati personali è suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, il soggetto che esercita le funzioni di Titolare del trattamento, con il supporto del DPO, predispone la comunicazione agli interessati e la trasmette al Segretario Generale. Quest'ultimo comunica la violazione all'interessato, o agli interessati, senza ingiustificato ritardo, utilizzando i canali ufficiali di comunicazione a disposizione dell'Amministrazione.
Qualora la comunicazione risulti necessaria, saranno adottate le seguenti misure:

- Il Designato al trattamento, previa consultazione con il DPO e in coordinamento con quest'ultimo, comunica la violazione agli interessati, entro 5 giorni dalla scoperta della violazione;
- La comunicazione avviene preferibilmente su base individuale per e-mail, salvo che sia impossibile procedere in tal modo, nel qual caso la comunicazione viene effettuata tramite il sito istituzionale dell'Amministrazione e/o tramite pubbliche affissioni nelle sedi ministeriali e/o tramite messaggi push inviati da app ad uso interno od esterno, ove disponibili;
- La comunicazione all'interessato deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le seguenti informazioni:
    - una descrizione della natura della violazione;
    - il nome e i dati di contatto del RPD o di altro punto di contatto;
    - una descrizione delle probabili conseguenze della violazione;
    - una descrizione delle misure adottate o di cui si propone l'adozione da parte dell'Amministrazione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Si rammenta che, ai sensi dell'art. 34, par. 3 del Regolamento, non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

1. il soggetto che esercita le funzioni di 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;
2. il soggetto che esercita le funzioni di Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
3. 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.

Nel caso in cui il soggetto che esercita le funzioni di Titolare del trattamento (Direttore Generale) abbia deciso di non comunicare la violazione di dati personali agli interessati, deve far menzione all'interno del registro delle violazioni delle ragioni a fondamento della propria decisione. In tal caso, l'Autorità di controllo, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà degli interessati, può chiedere che colui che esercita le funzioni di Titolare provveda alla comunicazione ovvero può ritenere che una delle condizioni più sopra menzionate sia soddisfatta.

Aggiornamento del Registro delle violazioni

Il soggetto che esercita le funzioni di Titolare del trattamento, con il supporto dei referenti privacy, una volta terminate le fasi precedenti, procede all'aggiornamento del registro delle violazioni. Segnatamente, il registro dovrà contenere le seguenti informazioni:

Codice Identificativo data breach	
Data in cui è avvenuta la violazione	
Data, orario e modalità in cui si è avuta conoscenza della violazione	
Natura e causa della violazione	
Descrizione del data breach	
Categoria di interessati coinvolti	
Numero di interessati coinvolti (anche approssimativo)	
Categoria di dati personali coinvolti	
Numero di dati personali coinvolti (anche approssimativo)	
Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione	
Misure di sicurezza tecniche e organizzative adottate al momento della violazione	
Responsabili esterni del trattamento coinvolti, ove applicabile	
Possibili conseguenze della violazione sugli interessati	
Potenziali effetti negativi per gli interessati	
Azioni intraprese in risposta all'incidente per mitigare il danno e ridurre la probabilità di una recidiva simile	
Stima della gravità della violazione	
Indicazione dell'avvenuta notifica all'Autorità Garante (nei casi in cui non si sia proceduto con tale notifica, è necessario specificarne le ragioni)	
Comunicazione della violazione agli interessati (ove necessario)	
Numero di interessati a cui è stata comunicata la violazione	
Canale utilizzato per la comunicazione agli interessati	
Eventuale notifica ad altre autorità di controllo, organismi di vigilanza o di controllo o all'autorità giudiziaria o di polizia.	

Definizione del piano di rimedio

Una volta concluso il processo di notifica e comunicazione della violazione di dati personali agli interessati, il soggetto che esercita le funzioni di Titolare del trattamento, supportato dal DPO, svolge le seguenti attività:

- Analizza le cause che hanno determinato la violazione di dati personali;
- Valuta le opportunità di miglioramento dei presidi e dei processi di monitoraggio delle violazioni dei dati personali, al fine di mettere in atto misure tecniche e organizzative adeguate a garantire il rispetto del Regolamento;
- Definisce un piano di rimedio al fine di garantire un livello di sicurezza adeguato ai rischi in ordine alla protezione dei dati personali trattati.

Per ciascuna violazione di dati personali, il Designato al trattamento è tenuto a verificare se l'incidente è il risultato di un errore umano o di un problema di natura tecnica o organizzativa e valutare misure correttive volte a prevenire il ripetersi dell'evento. È, altresì, necessario che il soggetto che esercita le funzioni di Titolare del trattamento preveda attività di verifica periodiche volte a garantire l'efficacia delle procedure e degli strumenti di risposta agli incidenti relativi alle violazioni di dati personali.
Il Designato al trattamento, insieme ai responsabili interni di riferimento e con il supporto del DPO, deve periodicamente monitorare quelle violazioni che hanno maggiore probabilità di verificarsi, in modo da applicare azioni correttive specifiche a fronte delle situazioni rilevate. In merito all'esito di tali test, qualora gli stessi evidenzino dei gap procedurali/organizzativi o tecnici, è opportuno che il DPO, con la collaborazione dei referenti privacy, identifichi azioni ed interventi di rimedio da sottoporre al soggetto che esercita le funzioni di Titolare del trattamento.

Obblighi di comunicazione dell'Amministrazione qualora operi in qualità di Responsabile del trattamento

Quando la Regione Basilicata agisce in qualità responsabile del trattamento, in caso di violazione dei dati personali deve informare il Titolare del trattamento, senza ingiustificato ritardo secondo i tempi e i modi concordati negli accordi per il trattamento dei dati personali.

Allegato 1 - Registro delle violazioni

Codice data breach	
Data in cui è avvenuta la violazione	
Data, orario e modalità in cui si è venuti a conoscenza della violazione	
Natura della violazione	
Causa della violazione	
Descrizione data breach	
Categoria di interessati coinvolti	
Numero di interessati coinvolti (anche approssimativo)	
Categoria di dati personali coinvolti	
Numero di dati personali coinvolti (anche approssimativo)	
Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente	
Misure di sicurezza tecniche e organizzative adottate al momento della violazione	
Responsabili Esterni del Trattamento Coinvolti (Se Applicabile)	
Possibili conseguenze della violazione sugli interessati in caso di perdita di: - Riservatezza - Integrità - Disponibilità	
Potenziali effetti negativi per gli interessati	
Stima della gravità della violazione	
Azioni intraprese in risposta all'incidente	
Notifica al Garante oppure specificare le ragioni della mancata segnalazione	
Data della notifica al Garante	
Comunicazione all'interessato oppure specificare le ragioni della mancata comunicazione	
Numero di interessati a cui è stata comunicata la violazione	
Canale utilizzato per la comunicazione agli interessati	
Data della comunicazione all'interessato	
Specificare se la notifica è stata inviata ad altre autorità di controllo, organismi di vigilanza o di controllo o all'autorità giudiziaria o di polizia	
Eventuali note	

Allegato 2 – Scheda dell'evento

Direzione coinvolta	
Data evento e ora della violazione anche solo presunta (specificando se è presunta)	
Data e ora in cui si è avuto conoscenza della violazione	
Fonte di segnalazione	
Natura dell'evento anomalo	
Descrizione dell'evento anomalo	
Numero e categoria di interessati coinvolti	
Categoria e volume dei dati personali di cui si presume la violazione	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	
Eventuale Responsabile esterno del trattamento coinvolto nella gestione del sistema informatico	
Misure di sicurezza adottate al set di dati oggetto di violazione	
Misure proposte per la mitigazione della presunta violazione	
Esito della autovalutazione condotta mediante il *tool* messo a disposizione dal Garante per la Protezione dei Dati Personali	

REGIONE BASILICATA

ALLEGATO 3

Linee guida sui controlli per la Cybersecurity e la Data Protection

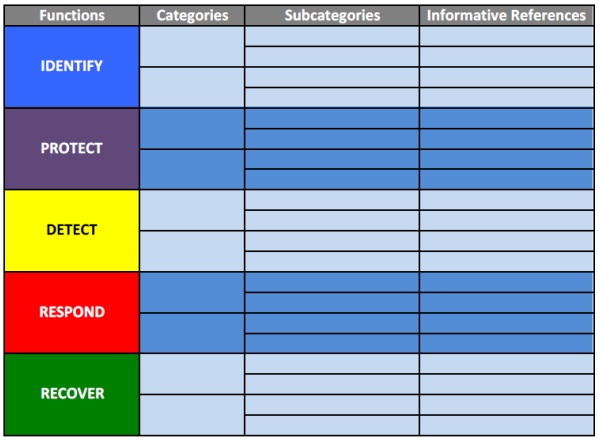
Indice dei contenuti

Il *Framework Nazionale per la Cybersecurity*, frutto della collaborazione tra accademia, enti pubblici, e imprese private. Il Framework, ispirato al Cybersecurity Framework ideato dal NIST (National Institute of Standards and Technology), fornisce uno strumento operativo per organizzare i processi di cybersecurity adatto alle organizzazioni pubbliche e private, di qualunque dimensione.
Il Framework Core rappresenta la struttura del ciclo di vita del processo di gestione della cybersecurity, sia dal punto di vista tecnico che organizzativo ed è strutturato gerarchicamente in *function*, *category* e *subcategory*. Per ogni function, category e subcategory, le attività abilitanti, quali processi e tecnologie, da realizzare per gestire la singola function.
Il Framework rappresenta un valido strumento di supporto alla pianificazione delle attività necessarie per adeguarsi alla normativa e di successivo monitoraggio per la corretta implementazione e gestione delle stesse.

Al fine di garantire un livello adeguato di sicurezza di seguito le check list di controllo che tutti coloro che sono responsabili di Sistemi Informativi o Trattano dati personali sono tenuti a porre in essere.

Elementi fondamentali del Framework

Il Framework eredita le tre nozioni fondamentali del Cybersecurity Framework NIST: *Framework Core, Profile e Implementation Tier*. Di seguito ne diamo una breve descrizione:
Framework Core – Il core rappresenta la struttura del ciclo di vita del processo di gestione della cybersecurity, sia dal punto di vista tecnico sia organizzativo. Il core è strutturato gerarchicamente in *function*, *category* e *subcategory*.
Le function, concorrenti e continue, sono:
IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER e costituiscono le principali tematiche da affrontare per operare una adeguata gestione del rischio cyber in modo strategico.
Il Framework quindi definisce, per ogni function, category e subcategory, le attività abilitanti, quali processi e tecnologie, da mettere in campo per gestire la singola function. Il Framework Core presenta inoltre delle *informative reference*, dei riferimenti che legano la singola subcategory alle pratiche di sicurezza note previste da standard di settore (ISO, SP800-53r4, COBIT-5, SANS20 e altri) o da regolamentazioni generali vigenti (Regolamento UE 2016/679 General Data Protection Regulation, Direttiva UE 2016/1148 NIS). Tali riferimenti hanno principalmente uno scopo illustrativo e non devono essere interpretati come esaustivi. La struttura del Framework Core.
Il core del Framework Nazionale per la Cybersecurity è strutturato gerarchicamente in function, category e SUBCATEGORY e rappresenta la struttura del ciclo di vita del processo di gestione della cybersecurity.



IDENTIFY *- La function IDENTIFY è legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati. Tale comprensione permette a un'organizzazione di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali. Le category all'interno di questa function sono: Asset Management, Business Environment; Governance, Risk Assessment, Risk Management Strategy, Supply Chain Risk Management e Data Management.*

PROTECT - *La function PROTECT è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica. Le category all'interno di questa function sono: Identity Management, Authentication and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology.*

DETECT - *La function DETECT è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica. Le category all'interno di questa function sono: Anomalies and Events, Security Continuous Monitoring, Detection Processes.*

RESPOND - *La function RESPOND è associata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica. Le category all'interno di questa function sono: Response Planning, Communications, Analysis, Mitigation, Improvements.*

RECOVER - *La function RECOVER è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations. Le category all'interno di questa function sono: Recovery Planning, Improvements, Communications.*

Controlli Essenziali di Cybersecurity

Di fatti rappresentano un vademecum composto da 15 controlli definiti come “essenziali” di facile e, quasi sempre, economica implementazione e che rappresentano le pratiche di sicurezza che non possono essere ignorate.

Per raggiungere un livello adeguato di protezione contro la minaccia cyber è necessario partire da una base di semplice e relativamente economica implementazione. In quest’ottica nell’Italian Cybersecurity Report del 2016 sono stati proposti 15 Controlli Essenziali di Cybersecurity derivati dal Framework Nazionale attraverso un processo di progressiva semplificazione. È evidente che la sola implementazione di questi 15 controlli non assicura un livello adeguato di sicurezza. Essi rappresentano un insieme minimo di pratiche di sicurezza che non possono essere ignorate e una base dalla quale deve partire un percorso di miglioramento progressivo che porti ad allinearsi con la metodologia di gestione della cybersecurity basata sul Framework Nazionale.

Tematiche	**Controlli Essenziali di Cybersecurity**	**RISPOSTA**
Inventario dispositivi e software	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.	
Governance	5 Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l’azienda.	
Protezione da malware	6 Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.	
Gestione password e account	7 Le password sono diverse per ogni account, della complessità adeguata e viene valutato l’utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).	
	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.	
Formazione e consapevolezza	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.	
Protezione dei dati	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	
Protezioni delle reti	13 Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software antintrusione).	
Prevenzione e mitigazione	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.	

Inventario dispositivi e software

Relazione dei Controlli Essenziali della tematica "Inventario dispositivi e software" con il Framework Nazionale per la Cybersecurity e la Data Protection.

FUNCTION	CATEGORY	SUBCATEGORYY	CONTROLLO	RISPOSTA
IDENTIFY (ID)	**Asset Management (ID.AM)**: I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	1 - Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.	
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	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.	
		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti alla cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	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.	
		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)		
		DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati	3 - Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.	

Governance

Relazione del Controllo Essenziale della tematica "Governance" con il Framework Nazionale per la Cybersecurity e la Data Protection.

FUNCTION	CATEGORY	SUBCATEGORYY	CONTROLLO	RISPOSTA
IDENTIFY (ID)	**Governance (ID.GV)**: Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**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	5 - Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.	

Gestione delle identità, protezione, formazione e consapevolezza

I Controlli Essenziali dal 6 al 13 abbracciano le seguenti tematiche:

- Protezione da malware
- Gestione password e account
- Formazione e consapevolezza
- Protezione dei dati
- Protezione delle reti

La maggior parte di essi impattano su subcategory della function PROTECT e riguardano l'adozione di misure di sicurezza efficaci tanto contro il rischio cyber quanto contro quello legato alla data protection. La protezione dei dati personali, invero, non può prescindere dalla protezione dei sistemi cyber che li gestiscono.

Prevenzione e mitigazione

Relazione tra i Controlli Essenziali in "Prevenzione e mitigazione" con il Framework Nazionale per la Cybersecurity e la Data Protection.

FUNCTION	CATEGORY	SUBCATEGORYY	CONTROLLO	RISPOSTA
RESPOND (RS)	**Communications (RS.CO)**: Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**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	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.	
	Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per risolvere l'incidente.	**RS.MI-1**: In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto		
		RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti		
		RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	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.	

Applicazione del Framework al GDPR

Il Framework, contestualizzato alla pianificazione delle attività necessarie per adeguarsi agli elementi fondamentali al GDPR e di successivo monitoraggio per la corretta implementazione e gestione delle stesse.

La presente guida è organizzata nelle seguenti aree di indirizzo:
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

1. Ruoli e responsabilità

Di questa area di indirizzo fanno parte i controlli che definiscono ruoli e responsabilità per le figure inerenti al trattamento e alla protezione dei dati personali. Nel contesto GDPR queste figure sono:

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**	**RISPOSTA**
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)	

2. Registri delle attività di trattamento

Questa area di indirizzo prevede un solo controllo che riguarda la tenuta dei registri delle attività di trattamento da parte del titolare del trattamento e del responsabile del trattamento. In particolare, occorrerà prestare la massima attenzione alle informazioni che il titolare e il responsabile del trattamento devono includere nei relativi registri.

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**	**RISPOSTA**
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)	

3. Principi

Quest'area di indirizzo riguarda i principi applicabili al trattamento dei dati personali previsti dal Regolamento e comprende due controlli. Il primo controllo prevede che vengano definiti e gestiti processi che permettano di garantire che i trattamenti di dati personali rispettino i principi del Regolamento (vedi art. 5). Il secondo controllo richiede che il titolare sia anche in grado di dimostrare il rispetto dei principi e la conformità dei trattamenti al Regolamento (accountability). Questi controlli di sicurezza si mappano nella subcategory relativa alla comprensione e gestione dei requisiti legali.

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**	**RISPOSTA**
ID.GV-3-01: Sono definiti e gestiti processi volti 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)	

4. Valutazione d'impatto sulla protezione dei dati personali

In quest'area di indirizzo vengono proposti una serie di controlli legati alla valutazione d'impatto sulla protezione dei dati personali. Il primo controllo specifica che la valutazione d'impatto debba essere eseguita ogni qual volta un tipo di trattamento di dati personali presenti un rischio elevato per i diritti e le libertà degli interessati. In questo caso il titolare del trattamento dovrà consultarsi con il responsabile della protezione dei dati, tra le cui responsabilità c'è quella di fornire pareri in merito alle valutazioni d'impatto. Il secondo controllo richiede che il titolare del trattamento si assicuri che la valutazione d'impatto contenga almeno quanto previsto dal Regolamento. Il controllo **DP-ID.RA-7-03** richiede che il titolare del trattamento, nel valutare l'impatto dei trattamenti, tenga in considerazione l'eventuale rispetto di codici di condotta ed eventualmente senta il parere degli interessati o dei loro rappresentanti circa i trattamenti. Il controllo **DP-ID.RA-7-04** prevede che la valutazione d'impatto venga svolta periodicamente e comunque ogni volta che insorgano variazioni del rischio associato ai trattamenti. Infine, il controllo **DP-ID.RA-7-05** richiede che il titolare del trattamento consulti preventivamente l'autorità di controllo, qualora dalla valutazione d'impatto risulti che un trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare per ridurre il rischio.

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**	**RISPOSTA**
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)	

5. Informazioni all'interessato

Quest'area di indirizzo contiene un unico controllo (**DP-ID.DM-2-01**) che richiede l'adozione di processi per fornire all'interessato tutte le informazioni inerenti al trattamento dei dati personali che lo riguardano, oltre all'esistenza e alle modalità di esercizio dei diritti previsti dal Regolamento. Nell'adottare tali misure occorrerà tenere in considerazione le differenti informazioni da fornire qualora i dati siano stati raccolti presso l'interessato (art. 13 del Regolamento) o presso terzi (art. 14 del Regolamento). Questo controllo trova collocazione nella subcategory **DP-ID.DM-2** del Framework inerente ai processi di informazione dell'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**	**RISPOSTA**
DP-ID.DM-2-01: Il titolare del trattamento adotta processi per fornire all'interessato tutte le informazioni inerenti al 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	

6. Consenso dell'interessato

In quest'area di indirizzo vengono riuniti i controlli che riguardano i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati. Il primo controllo (**DP-ID.DM-3-01)** pone all'attenzione la creazione da parte del titolare del trattamento di un insieme di processi che permettano di dimostrare, per tutti i trattamenti basati sul consenso, l'avvenuto ottenimento dello stesso da parte del titolare del trattamento. Il secondo controllo (**DP-ID.DM-3-02**) ha per oggetto il processo di revoca del consenso (**DP-ID.DM-3-02**).

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**	**RISPOSTA**
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	

7. Diritti dell'interessato

In quest'area di indirizzo sono definiti i controlli che riguardano l'implementazione e la documentazione di tutti i processi inerenti all'esercizio dei diritti da parte dell'interessato così come sancito dal Regolamento. Il controllo **DP-ID.DM-4-01** impone la creazione di un processo che permetta al titolare del trattamento di fornire conferma all'interessato che sia o meno in corso un trattamento di dati personali che lo riguardano. Il controllo **DP-ID.DM-4-02** richiede la creazione di processi per permettere all'interessato del trattamento di accedere ai propri dati personali ed alle informazioni relative al trattamento, qualora ne venga fatta richiesta in forma elettronica.

Il controllo **DP-ID.DM-4-03** richiede la messa in atto di processi per garantire all'interessato l'esercizio del diritto di rettifica dei dati personali. Il controllo **DP-ID.DM-4-04** riguarda la definizione di processi per la cancellazione dei dati personali qualora l'interessato ne faccia richiesta.

Il controllo **DP-ID.DM-4-05**, facente riferimento al controllo **DP-ID.DM-4-04** concerne il caso in cui i dati personali di cui è stata richiesta la cancellazione siano stati resi pubblici, e richiede al titolare del trattamento di adottare misure ragionevoli, anche tecniche, per cancellare qualsiasi link, copia o riproduzione degli stessi.

Il controllo **DP-ID.DM-4-06** richiede la creazione di processi atti a garantire all'interessato del trattamento il diritto alla limitazione del trattamento dei dati personali, qualora sussistano le condizioni previste (esattezza, non liceità, accertamento in sede giudiziaria, opposizione), ed a trattare i dati personali dal momento della richiesta di limitazione in accordo a quanto previsto nel Regolamento.
Il controllo **DP-ID.DM-4-07** richiede da parte del titolare del trattamento la comunicazione a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate 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.
Il controllo **DP-ID.DM-4-08** richiede la creazione di processi che garantiscano all'interessato il diritto alla portabilità dei dati personali in accordo a quanto sancito nel Regolamento. Il controllo **DP-ID.DM-4-09** richiede la creazione di processi per garantire all'interessato il diritto all'opposizione al trattamento di dati personali in accordo a quanto sancito nel Regolamento.
L'interessato deve essere informato di questo diritto in forma chiara e separata da altre informazioni, al più tardi alla prima comunicazione con l'interessato.
Il controllo **DP-ID.DM-4-10** richiede la creazione di processi che garantiscano all'interessato il diritto di non essere sottoposto ad una decisione basata esclusivamente sul trattamento automatizzato che produca effetti giuridici o abbia effetto sulla sua persona fisica.
Connesso al precedente, Il controllo **DP-ID.DM-4-11** richiede l'attuazione di misure appropriate per tutelare i diritti e le libertà 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.

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**	**RISPOSTA**
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, 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	Art. 18(1-3)	

esclusivamente nelle circostanze previste dal Regolamento (es. consenso dell'interessato, accertamento diritti in sede giudiziaria, ecc.).		
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)	

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

In quest'area di indirizzo sono definiti controlli per l'implementazione, documentazione e gestione dei processi di trasferimento dei dati in ambito internazionale.

Il controllo **DP-ID.DM-5-01** richiede la definizione di un processo per regolare il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali in conformità al principio di adeguatezza (art. 44) e senza che il livello di protezione delle persone fisiche sia pregiudicato.

In tal senso assume notevole importanza la verifica delle condizioni di adeguatezza (art. 45) affinché un trasferimento di dati possa avvenire, gestito tramite un processo definito nel controllo **DP-ID.DM-5-02**.

Il controllo **DP-ID.DM-5-03** richiede la creazione di un processo riguardante la verifica dell'adeguatezza delle garanzie fornite dal paese terzo verso cui si vogliono trasferire dati personali qualora non vi sia stata decisione da parte della Commissione ai sensi dell'art. 45 par.

Il processo dovrà considerare gli elementi di valutazione forniti nell'art. 46 parr. 2 e 3. Qualora anche questi non siano sufficienti a prendere una decisione, si farà capo a quanto sancito nell'art. 49.

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**	**RISPOSTA**
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.	Artt. 46, 47 e 49	

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

In quest'area di indirizzo sono definiti controlli per la gestione, documentazione e comunicazione delle violazioni di dati personali.

Il controllo **DP-RS.CO-6-01** richiede di istituire un processo con cui il titolare del trattamento è in grado, a seguito di una violazione di dati personali, di notificare la violazione all'autorità di controllo competente, senza ingiustificato ritardo, ovvero entro 72 ore dal momento in cui ne è venuto a conoscenza. Per la comunicazione della violazione all'interessato del trattamento, in accordo a quanto richiesto dal controllo **DP-RS.CO-6-02**, occorre effettuare una valutazione del rischio per i diritti e le libertà delle persone fisiche al fine di valutare se esso sia o meno elevato e supportare quindi la decisione di comunicare o meno la violazione all'interessato.

Il controllo **DP-RS.CO-6-03** richiede al responsabile del trattamento di informare il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza di una violazione di dati personali.

Il controllo **DP-RS.CO-6-04** richiede di documentare (ad esempio, in un registro) tutte le violazioni di dati personali, in particolare in merito alle circostanze, alle conseguenze per gli interessati ed alle azioni intraprese per porvi rimedio.

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**	**RISPOSTA**
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 per il GDPR

Per ogni subcategory del Framework core è definita la relativa classe e la priorità di implementazione tra le seguenti opzioni:

- **OBBLIGATORIA**: la subcategory deve essere necessariamente inclusa;
- **CONSIGLIATA**: si suggerisce l'inclusione della subcategory;
- **LIBERA**: l'inclusione della subcategory è lasciata alla libera.

Function	Category	Subcategory	Classe	Livello di Priorità
IDENTIFY (ID)	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	**Libera**	
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	**Libera**	
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	**Libera**	
		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	**Libera**	
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono prioritizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	**Libera**	
		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	**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**
		DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati	**Obbligatoria**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
IDENTIFY (ID)	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È identificata e resa nota una policy di cybersecurity	**Libera**	
		ID.GV-2: Ruoli e responsabilità inerenti la cybersecurity sono coordinati ed allineati con i ruoli interni ed i partner esterni	**Libera**	
		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**
		ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity	**Libera**	
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-1:** Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	**Libera**	
		ID.RA-2: L'organizzazione riceve informazioni su minacce e vulnerabilità da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing)	**Libera**	
		ID.RA-3: Le minacce, sia interne che esterne, sono identificate e documentate	**Libera**	
		ID.RA-4: Sono identificati i potenziali impatti sul business e le relative probabilità di accadimento	**Libera**	
		ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	**Libera**	
		ID.RA-6: Sono identificate e prioritizzate le risposte al rischio	**Libera**	
		DP-ID.RA-7: Viene effettuata una valutazione di impatto sulla protezione dei dati personali	**Obbligatoria**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
IDENTIFY (ID)	**Risk Management Strategy (ID.RM):** Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale.	**ID.RM-1:** I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili dell'organizzazione (c.d. stakeholder)	**Libera**	
		ID.RM-2: Il rischio tollerato dall'organizzazione è identificato ed espresso chiaramente	**Libera**	
		ID.RM-3: Il rischio tollerato è determinato tenendo conto del ruolo dell'organizzazione come infrastruttura critica e dei rischi specifici presenti nel settore industriale di appartenenza	**Libera**	
	Supply Chain Risk Management (ID.SC): Le priorità, i vincoli, le tolleranze al rischio ele ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	**Libera**	
		ID.SC-2: I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber	**Libera**	
		ID.SC-3: I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber	**Libera**	
		ID.SC-4: Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	**Libera**	
		ID.SC-5: La pianificazione e la verifica della risposta e del ripristino sono condotti con i fornitori e i partner terzi	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
IDENTIFY (ID)	**Data Management (DP-ID.DM):** i dati personali sono trattati attraverso processi definiti, in coerenza con le normative di riferimento.	**DP-ID.DM-1:** Il ciclo di vita dei dati è definito e documentato	**Consigliata**	
		DP-ID.DM-2: Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati	**Obbligatoria**	**ALTA**
		DP-ID.DM-3: Sono definiti, implementati e documentati i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati	**Obbligatoria**	**ALTA**
		DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato	**Obbligatoria**	**ALTA**
		DP-ID.DM-5: Sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale	**Obbligatoria**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi, ed è gestito in maniera consistente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	**Consigliata**	**ALTA**
		PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato	**Consigliata**	**ALTA**
		PR.AC-3: L'accesso remoto alle risorse è amministrato	**Consigliata**	**ALTA**
		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**
		PR.AC-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	**Consigliata**	**ALTA**
		PR.AC-6: Le identità sono comprovate, associate a credenziali e verificate durante le interazioni	**Consigliata**	**ALTA**
		PR.AC-7: Le modalità di autenticazione (es. autenticazione a singolo o multi fattore) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)	**Consigliata**	**ALTA**
	Awareness and Training (PR.AT): Il personale e le terze parti sono sensibilizzate e formate in materia di cybersecurity e ricevono adeguata preparazione, coerente con le politiche, le procedure e gli accordi esistenti, per svolgere correttamente i compiti e le responsabilità legate alla cybersecurity	**PR.AT-1:** Tutti gli utenti sono informati e addestrati	**Libera**	
		PR.AT-2: Gli utenti privilegiati (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità	**Libera**	
		PR.AT-3: Tutte le terze parti (es. fornitori, clienti, partner) comprendono i loro ruoli e responsabilità	**Libera**	
		PR.AT-4: I dirigenti ed i vertici aziendali comprendono i loro ruoli e responsabilità	**Libera**	
		PR.AT-5: Il personale addetto alla sicurezza fisica e alla cybersecurity comprende i suoi ruoli e responsabilità	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
PROTECT (PR)	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati e le informazioni memorizzate sono protetti	**Consigliata**	**ALTA**
		PR.DS-2: I dati sono protetti durante la trasmissione	**Consigliata**	**ALTA**
		PR.DS-3: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	**Consigliata**	**ALTA**
		PR.DS-4: I sistemi hanno adeguate risorse a disposizione per poter garantire la disponibilità	**Consigliata**	**MEDIA**
		PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	**Consigliata**	**ALTA**
		PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità deidati per verificare l'autenticità di software, firmware e delle informazioni	**Consigliata**	**ALTA**
		PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	**Libera**	
		PR.DS-8: Sono impiegati meccanismi di controllo dell'integrità per verificare l'integrità del hardware	**Consigliata**	BASSA

Function	Category	Subcategory	Classe	Livello di Priorità
PROTECT (PR)	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	**Libera**	
		PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).	**Consigliata**	BASSA
		PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni	**Consigliata**	**MEDIA**
		PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati	**Consigliata**	**ALTA**
		PR.IP-5: Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione	**Consigliata**	**MEDIA**
		PR.IP-6: I dati sono distrutti in conformità con le policy	**Consigliata**	**ALTA**
		PR.IP-7: I processi di protezione sono sottoposti a miglioramenti	**Consigliata**	**MEDIA**
		PR.IP-8: L'efficacia delle tecnologie di protezione viene condivisa	**Consigliata**	**BASSA**
		PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Responsee Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	**Consigliata**	**ALTA**
		PR.IP-10: I piani di risposta e recupero a seguito di incidenti/disastri sono verificati nel tempo	**Consigliata**	**MEDIA**
		PR.IP-11: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, deprovisioning)	**Consigliata**	**MEDIA**
		PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità	**Consigliata**	**ALTA**
	Maintenance (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	**Libera**	
		PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
PROTECT (PR)	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1:** Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi	**Consigliata**	**MEDIA**
		PR.PT-2: I supporti di memorizzazione removibili sono protetti ed il loro uso è ristretto in accordo alle policy	**Consigliata**	**ALTA**
		PR.PT-3: Viene adottato il principio di minima funzionalità configurando i sistemi in modo che forniscano solo le funzionalità necessarie	**Consigliata**	**MEDIA**
		PR.PT-4: Le reti di comunicazione e controllo sono protette	**Consigliata**	**ALTA**
		PR.PT-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di raggiungere i requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	**Consigliata**	**ALTA**

Function	Category	Subcategory	Classe	Livello di Priorità
DETECT (DE)	**Anomalies and Events (DE.AE):** Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.	**DE.AE-1:** Sono definite, rese note e gestite delle pratiche di riferimento (c.d. baseline) inerenti l'utilizzo della rete ed i flussi informativi attesi per utenti e sistemi	**Libera**	
		DE.AE-2: Gli eventi rilevati vengono analizzati per comprendere gli obiettivi e le metodologie dell'attacco	**Libera**	
		DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	**Libera**	
		DE.AE-4: Viene determinato l'impatto di un evento	**Libera**	
		DE.AE-5: Vengono definite delle soglie di allerta per gli incidenti	**Libera**	
	Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	**Libera**	
		DE.CM-2: Viene svolto il monitoraggio degli spazi fisici per rilevare potenziali eventi di cybersecurity	**Libera**	
		DE.CM-3: Viene svolto il monitoraggio del personale per rilevare potenziali eventi di cybersecurity	**Libera**	
		DE.CM-4: Il codice malevolo viene rilevato	**Libera**	
		DE.CM-5: Il codice non autorizzato su dispositivi mobili viene rilevato	**Libera**	
		DE.CM-6: Viene svolto il monitoraggio delle attività dei service provider esterni per rilevare potenziali eventi di cybersecurity	**Libera**	
		DE.CM-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	**Libera**	
		DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità	**Libera**	
	Detection Processes (DE.DP): Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	**DE.DP-1:** Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	**Libera**	
		DE.DP-2: Le attività di monitoraggio soddisfano tutti i requisiti applicabili	**Libera**	
		DE.DP-3: I processi di monitoraggio vengono testati	**Libera**	
		DE.DP-4: L'informazione relativa agli eventi rilevati viene comunicata	**Libera**	
		DE.DP-5: I processi di monitoraggio sono oggetto di periodici miglioramenti e perfezionamenti	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
RESPOND (RS)	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	**Consigliata**	**ALTA**
	Communications (RS.CO): Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	**Libera**	
		RS.CO-2: Sono stabiliti dei criteri per documentare gli incidenti	**Libera**	
		RS.CO-3: Le informazioni sono condivise in maniera coerente con il piano di risposta	**Libera**	
		RS.CO-4: Il coordinamento con le parti interessate dell'organizzazione avviene in coerenza con i piani di risposta	**Libera**	
		RS.CO-5: È attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)	**Libera**	
		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**
	Analysis (RS.AN): Vengono condotte analisi per assicurare un'efficace riposta e supporto alle attività di ripristino.	**RS.AN-1:** Le notifiche provenienti dai sistemi di monitoraggio vengono sempre visionate e analizzate	**Libera**	
		RS.AN-2: Viene compreso l'impatto di ogni incidente	**Libera**	
		RS.AN-3: A seguito di un incidente viene svolta un'analisi forense	**Libera**	
		RS.AN-4: Gli incidenti sono categorizzate in maniera coerente con i piani di risposta	**Libera**	
		RS.AN-5: Sono definiti processi per ricevere informazioni, analizzare e rispondere a vulnerabilità rese note all'organizzazione da fonti interne o esterne (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)	**Libera**	
	Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per risolvere l'incidente.	**RS.MI-1:** In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto	**Libera**	
		RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti	**Libera**	
		RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	**Libera**	
	Improvements (RS.IM): Le attività di risposta sono migliorate incorporando le "lesson learned" da attività precedenti di monitoraggio e risposta.	**RS.IM-1:** I piani di risposta agli incidenti tengono in considerazione le esperienze passate (lesson learned	**Libera**	
		RS.IM-2: Le strategie di risposta agli incidenti sono aggiornate	**Libera**	

Function	Category	Subcategory	Classe	Livello di Priorità
RECOVER (RC)	**Recovery Planning (RC.RP):** I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.	**RC.RP-1:** Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente	**Libera**	
	Improvements (RC.IM): I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "lesson learned" per le attività future.	**RC.IM-1:** I piani di riprisitino tengono in considerazione le esperienze passate (lesson learned)	**Libera**	
		RC.IM-2: Le strategie di recupero sono aggiornate	**Libera**	
	Communications (RC.CO): Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT).	**RC.CO-1:** A seguito di un incidente vengono gestite le pubbliche relazioni	**Libera**	
		RC.CO-2: A seguito di un incidente viene ripristinata la reputazione	**Libera**	
		RC.CO-3: Le attività di ripristino condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione	**Libera**	

REGIONE BASILICATA

ALLEGATO 4

Modelli tipo Data Protection Agreement

Indice

MODELLO LETTERA AUTORIZZATO-INCARICATO DATI

Prot. n._____ del _____

LETTERA DI DESIGNAZIONE ED ISTRUZIONI PER LE PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI SOTTO L'AUTORITA' DIRETTA DEL TITOLARE O DEL DESIGNATO - art. 4, c.10 e art. 29 DEL REGOLAMENTO GENERALE EUROPEO PER LA PROTEZIONE DEI DATI PERSONALI (GENERAL DATA PROTECTION REGULATION REGULATION) - GDPR - (UE) 2016/679.

Richiamati:

l'art. 4 del Regolamento UE 2016/679:

comma 1), «dato personale», "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale";

comma 2), «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione";

comma 7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

comma 8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

comma 9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati 4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

comma 10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

l'art. 29 del predetto Regolamento UE 2016/679 "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento". Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare 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.

l'art 37 del predetto Regolamento UE 2016/679 "Designazione del responsabile della protezione dei dati ". Il Titolare con la Deliberazione di Giunta Regionale n. 431 del 17/05/2018, ha designato il Dott. Nicola Petrizzi quale Responsabile della Protezione Dati (RPD ovvero DPO Data Protection Officer) per le aree istituzionali "Presidenza Giunta" e "Giunta Regionale" della Regione Basilicata.
l'art. 2-quaterdecies del D.lgs 101/2018 (Attribuzione di funzioni e compiti a soggetti designati);

la Giunta Regionale con al Deliberazione n. 540 del 19/07/2021 "ATTUAZIONE DEGLI ADEMPIMENTI PREVISTI DALLA NORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI Regolamento (UE) 2016/679 - RIDEFINIZIONE MODELLO ORGANIZZATIVO" ha proceduto ad approvare il nuovo modello organizzativo finalizzato alla gestione del trattamento dati con il quale il Titolare del trattamento ha designato i dirigenti degli Uffici, secondo l'organigramma attualmente vigente, al trattamento dei dati personali, ai sensi del predetto articolo 2 quaterdecies del D.lgs. 101/2018.

Premesso che:

Il Dirigente protempore dell'Ufficio ***(da specificare…….)*** della Regione Basilicata risulta già nominato quale Designato al trattamento ai sensi della DGR 540/2021;
la Regione Basilicata si avvale della Società ***(da specificare…….)*** per il servizio di ***(da specificare…….)*** per ……..;

- tali servizi sono forniti ai sensi del contratto/Convenzione Rep. N. ***(da specificare…….)*** sottoscritto in data ***(da specificare…….)*** e con scadenza in data ***(da specificare…….)***.
- al ruolo di dipendente dell'Azienda ***(da specificare…….)***, ai sensi dell'art. 4 comma 10 del Reg. UE 2016/679, può essere attribuita la qualifica di persona autorizzata al trattamento o Incaricato del Trattamento dei dati Personali;
- la formalizzazione della qualifica di persona autorizzata o Incaricato al trattamento è indispensabile per attribuire specifiche responsabilità a tutela della legittimità delle operazioni di trattamento dei dati personali nell'ambito delle competenze dell'Ufficio o Struttura organizzativa dell'Amministrazione, ed evitare che siano comminate sanzioni civili, amministrative e penali (salvo il caso di dolo o colpa) nei confronti di personale non autorizzato;
- è necessario impartire a tutti coloro che effettuano trattamenti di dati personali le istruzioni ai sensi dell'art.29 del Regolamento GDPR, così come riportato nell'Allegato "Informazioni e istruzioni agli autorizzati".

Il sottoscritto Dott.....,

in qualità di Designato al trattamento dei dati personali per l'Ufficio:

.....,

AUTORIZZA

il Dott./Sig……., nato a ……. Il ……. C.F.[1]

…… Dipendente della Società/Azienda XXXXXXXXXXXXXXXX in servizio presso il precitato Ufficio,

ad effettuare i trattamenti dei dati personali e particolari (già sensibili e/o giudiziari), con accesso ai dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati:

[1] Riportare il codice fiscale nel caso che il designato non sia un dipendente dell'Amministrazione Regionale ma un consulente, part time ecc.

Banca Dati/Archivio cartaceo	Trattamenti[2]	Compiti[3]	Natura dei dati[4]		Revoca[5]
			P	G	

Il trattamento dei dati dovrà effettuarsi nel rispetto della normativa comunitaria vigente in materia di protezione dei dati personali, del Codice Privacy, delle direttive/circolari e delle istruzioni allegate al presente atto di nomina e successivamente nel corso della prestazione lavorativa.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati personali trattati permangono anche a seguito di modifica delle mansioni del soggetto incaricato o di cessazione del rapporto di lavoro.

Si rimanda per tutto quanto non chiaramente specificato nella presente lettera di incarico al rispetto di quanto prescritto dal Regolamento UE 2016/679 (GPDR) e dal D.lgs 196/2003 ss.mm.ii..

Le allegate istruzioni impartite costituiscono elementi di valutazione della condotta del personale e l'inosservanza delle stesse può comportare forme di responsabilità disciplinare oltre che responsabilità penale e civile nei casi previsti dalla normativa.

Data _____

Il Designato al Trattamento dati personali

_____

Letto firmato e sottoscritto per presa visione

L'Autorizzato (incaricato)

_____

[2] Indicare i trattamenti ai quali l'incaricato è abilitato:
CRE(Creazione); Crea ed organizza l'archivio, raccoglie, registra ed inserisce nuovi dati
MOD(Modifica); Modifica, estrae, elabora e cancella (in senso logico, non fisico) i dati
LET(Lettura); Seleziona, raffronta e consulta i dati
COM(Comunicazione / Diffusione); Diffonde e comunica l'informazione
ARC(Archiviazione); Archivia i dati
ELA(Elaborazione/ Conservazione); Elabora e conserva i dati in formato digitale
COMPLETO; Abilitato a tutti i trattamenti previsti

[3] Indicare i compiti lavorativi da svolgere

[4] Indicare se la banca dati/archivio cartaceo a cui è consentito l'accesso contiene dati particolari (già sensibili o giudiziari), apponendo una X nell'apposita casella.

[5] Inserire la data di un'eventuale revoca della designazione.

MODELLO INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI

1. **Premessa**

   Ai sensi dell'art. 13 del Regolamento Generale Europeo per la protezione dei dati personali (GDPR) General Data Protection Regulation (UE) 2016/679, la Regione Basilicata, in qualità di "Titolare" del trattamento, è tenuta a fornirle informazioni in merito all'utilizzo dei suoi dati personali. Il trattamento dei dati acquisiti per lo svolgimento di funzioni istituzionali e nell'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri da parte della Regione Basilicata è lecito ai sensi dell'art. 6 "Liceità del trattamento".

2. **Fonte dei dati personali**

   La raccolta dei suoi dati personali viene effettuata registrando i dati da lei stesso forniti, in qualità di interessato, al momento della compilazione della modulistica per la presentazione dell'istanza per il rilascio di autorizzazioni. In particolare, i dati trattati sono i dati anagrafici, *(da specificare…….)*

3. **Finalità del trattamento e base giuridica**

   I dati personali sono trattati esclusivamente per le seguenti finalità:

   (da specificare…….)

   La base giuridica è rappresentata *(da specificare……..)*

4. **Modalità di trattamento dei dati**

   In relazione alle finalità descritte, il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità sopra evidenziate e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi in conformità alle disposizioni previste dall'articolo 32 GDPR.

5. **Facoltatività del conferimento dei dati**

   Il conferimento dei dati è facoltativo, ma in mancanza non sarà possibile adempiere alle finalità descritte al punto 3 ("Finalità del trattamento").

6. **Periodo di conservazione**

   I dati forniti saranno conservati nel rispetto del principio di proporzionalità e comunque per il periodo necessario all'espletamento delle già menzionate finalità e per adempiere ad altri obblighi di Legge.

7. **Categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati**

   dai funzionari della Regione Basilicata e *(da specificare…….)*, individuati quali autorizzati e/o Incaricati del trattamento. Esclusivamente per le finalità previste al paragrafo 3 (Finalità del trattamento), possono venire a conoscenza dei dati personali società terze fornitrici di servizi per la Regione Basilicata, previa designazione in qualità di Responsabili esterni del trattamento e garantendo il medesimo livello di protezione. Alcuni dati personali da Lei comunicati alla Regione Basilicata, nel rispetto della normativa di cui al D. Lgs. 33/2013 sono soggetti alla pubblicità sul sito istituzionale della Regione Basilicata.

8. Trasferimento dati

I dati personali sono conservati su server ubicati in Regione Basilicata *(in caso contrario specificare…….)*, all'interno dell'Unione Europea. Resta in ogni caso inteso che il Titolare, ove si rendesse necessario, avrà facoltà di spostare i server, comunque all'interno dell'Unione Europea.

9. Diritti dell'Interessato

In quanto interessato/ta al trattamento dati, La informiamo che potrà esercitare, nei confronti del Titolare del trattamento, i diritti di cui agli articoli dal 15 al 22 del Regolamento UE n. 2016/679, ove applicabili; fra questi, il diritto di chiedere la rettifica o la cancellazione dei dati di registrazione, la limitazione del trattamento o di opporsi al trattamento, nei casi previsti.

10. Titolare e Designati al trattamento

Il Titolare del trattamento dei dati personali di cui alla presente Informativa è la Giunta Regionale di Basilicata, che ha individuato, con DGR 540/2021, quale Designato al trattamento, il Dirigente protempore dell'Ufficio *(da specificare…….)*. Lo stesso è responsabile del riscontro, in caso di esercizio dei diritti sopra descritti. Al fine di semplificare le modalità di inoltro e ridurre i tempi per il riscontro si invita a presentare le richieste, di cui al precedente paragrafo, alla Regione Basilicata, per Posta Elettronica Certificata: *(da specificare…….)*, per iscritto all'indirizzo Regione Basilicata – Via V. Verrastro n,4 85100 Potenza ovvero recandosi direttamente presso gli sportelli Urp presenti sul sito istituzionale (www.regione.basilicata.it sezione URP).

11. Diritto di reclamo

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti effettuato attraverso questo sito avvenga in violazione di quanto previsto dal Regolamento hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).

12. Responsabile della protezione dati

Il Responsabile della Protezione dei Dati (DPO è raggiungibile al seguente indirizzo: Via Vincenzo Verrastro n. 6, IT-85100, Potenza (Email: rpd@regione.basilicata.it PEC: rpd@cert.regione.basilicata.it).

ACCORDO DI CONTITOLARITÀ DEL TRATTAMENTO AI SENSI DELL'ART. 26 DEL REGOLAMENTO UE 2016/679 (GDPR)

Accordo di contitolarità del trattamento ai sensi dell'art. 26 DEL Regolamento UE 2016/679 (GDPR) relativo a _____ [specificare Procedimento amministrativo/Convenzione/Protocollo d'intesa ecc. di riferimento]

TRA

La Regione Basilicata, rappresentata nel presente atto dal dott. _____, *(specificare se Direttore generale o Dirigente)* della struttura regionale _____, con sede in Potenza, via _____, (C.F. 80017210727), Designato al trattamento dei dati giusta DGR n. 540 del 19/07/2021 (d'ora innanzi Designato);

E

L'Ente/la Società/altro soggetto pubblico o privato _____, rappresenta dal dott. _____ in qualità di rappresentante legale, con sede in _____, via _____, (C.F. _____), per le attività relative dell'affidamento/contratto/convenzione/protocollo d'intesa _____ _____ (indicare estremi dell'affidamento/contratto/convenzione/protocollo d'intesa).

Premesso che:

- Il Dirigente della Struttura regionale _____ è Designato al trattamento in base alla DGR del 19 luglio, n. 540;
- Il Reg. UE 679/2016 (GDPR) non esclude la possibilità che in talune circostanze uno o più soggetti possano determinare congiuntamente le finalità e i mezzi del trattamento dei dati: in tal senso si esprime il relativo art. 26, che configura tali soggetti quali "contitolari" del trattamento con rispettive responsabilità da ripartire e definire in modo trasparente mediante un accordo interno;
- Al fine di verificare l'eventuale sussistenza di un rapporto di contitolarità è possibile utilizzare i criteri dettati dal Comitato Europeo di Protezione dei Dati (European Data Protection Board – EDPB, già WP 29) nel "Parere 1/2010 sui concetti di "Responsabile del trattamento" e "Incaricato del trattamento", adottato il 16 febbraio 2010 e tuttora utile sia pure con i dovuti adeguamenti alle nuove definizioni del GDPR, in base al quale: "Nel contesto della corresponsabilità, comunque, la partecipazione delle parti alla determinazione congiunta può assumere varie forme e non deve essere necessariamente ripartita in modo uguale. In effetti, quando vi è una pluralità di attori, questi possono avere una relazione molto stretta (condividendo, ad esempio, tutte le finalità e tutti gli strumenti di un trattamento) o più distante (condividendo ad esempio solo le finalità o i mezzi, o una parte di essi). Va quindi esaminata un'ampia varietà di tipologie di corresponsabilità e ne vanno analizzate le rispettive conseguenze giuridiche, lasciando una certa flessibilità per tenere conto della crescente complessità della realtà attuale del trattamento dei dati". Alla luce di tale impostazione, i rapporti tra contitolari possono quindi articolarsi in modo asimmetrico, nel senso che in alcune situazioni i soggetti coinvolti possono determinare in misura diversa le finalità e/o i mezzi del trattamento e, conseguentemente, ciascuno di essi risponde solo per una parte del trattamento.

ART. 1 – Oggetto dell'accordo

Il presente accordo stabilisce gli obblighi e le responsabilità dei contitolari del trattamento dei dati in relazione alle operazioni di trattamento poste in essere. Il presente accordo si applica a tutte le attività di trattamento di dati personali poste in essere dagli autorizzati e dai responsabili del trattamento di ciascuna delle parti del medesimo accordo. Con il presente accordo le parti stabiliscono congiuntamente le finalità e/o i mezzi del trattamento in oggetto, come di seguito descritti _____ (*specificare nel dettaglio le finalità e/o i mezzi del trattamento che sono oggetto di individuazione condivisa*). Con il presente accordo le parti determinano le fasi del processo di trattamento dei dati personali effettuate in contitolarità, come di seguito descritte _____ (*specificare nel dettaglio le fasi del processo di trattamento*). Per le restanti fasi del processo per cui non esiste una determinazione comune delle finalità e mezzi, ogni parte è un titolare autonomo ai sensi dell'art. 4, punto 7 del GDPR.

ART. 2 – Attività di trattamento dei dati da parte di ciascun Titolare e relativa base giuridica

Nell'ambito della contitolarità, la Regione Basilicata svolge le seguenti attività di trattamento nell'ambito del procedimento amministrativo/convenzione/protocollo d'intesa ecc. di riferimento _____ [*specificare*]. Nell'ambito della medesima contitolarità, l'Ente/la Società/altro soggetto pubblico o privato _____ svolge le seguenti attività di trattamento nell'ambito (*del procedimento amministrativo/convenzione/protocollo d'intesa ecc.*) di riferimento _____ [*specificare*]. La base giuridica del trattamento in questione è rappresentata da _____ [*specificare la/e base/i giuridica/he*], ed è riferita alle seguenti tipologie/categorie di dati_____ [*specificare*].

ART. 3 – Sicurezza del trattamento e Valutazione d'impatto (DPIA)

Le parti sono tenute, se ricorrono i presupposti, alla predisposizione ed attuazione congiunta delle misure tecniche ed organizzative volte a garantire la sicurezza del trattamento secondo quanto previsto dall'art. 32 del GDPR . Qualora, ad esito dell'analisi dei rischi connessi al trattamento oggetto del presente accordo, si renda necessaria una valutazione di impatto sulla protezione dei dati ex art. 35 del Regolamento UE 2016/679, le parti collaborano a tale valutazione di impatto al fine di garantirne l'efficacia.

Le Parti eseguiranno un monitoraggio periodico sul livello di sicurezza raggiunto, al fine di renderlo sempre adeguato al rischio.

In riferimento:

- alle misure organizzative, le Parti presiederanno a tutti i trattamenti. Le Parti individueranno le misure organizzative idonee per l'espletamento del servizio specialmente in riferimento ai partner scelti designati con accordi per iscritto, con atto vincolante, come responsabili del trattamento secondo l'art 28 del GDPR. Il trattamento dei dati personali sarà effettuato solo da figure espressamente designate secondo l'art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati) del Codice della Privacy italiano, come integrato dal D.lgs. 101/201;
- alle misure tecniche, le Parti metteranno in campo tutte le misure tecniche idonee al trattamento dei dati personali e sensibili come pseudonimizzazione, criptazione dei dati, attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione; integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR, e tutelare i diritti degli interessati garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, garantendo che non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica, la capacità di assicurare su base permanente

la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento procedure per la gestione delle violazioni dei dati personali nella gestione dei siti informatici. Entrambe le organizzazioni dovranno adottare misure di comunicazione cifrate nel caso in cui si trasmettano dati personali;

Il Contitolare del Trattamento adotterà tutte le misure di sicurezza tecniche e organizzative per il tempestivo recupero della disponibilità dei dati personali in caso di incidente fisico o tecnico.

ART. 4 – Protezione dei dati

Le parti garantiscono la protezione dei dati del trattamento in oggetto fin dalla progettazione ed assicurano altresì che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, ai sensi dell'art. 25 del GDPR.

ART. 5 - Informativa Trattamento Dati

I Contitolari si impegnano a fornire, in sede di raccolta del dato, le informazioni di cui all'art. 13 del Regolamento UE 2016/679. In particolare, l'Informativa per il trattamento dati congiunta dei Contitolari va resa in forma coincisa, trasparente ed intelligibile, nonché facilmente accessibile sui Portali web di ciascun Contitolare, consentendo ai soggetti interessati di prenderne visione.

ART. 6 – Trasparenza dell'accordo

I Contitolari si impegnano a mettere a disposizione degli interessati, su richiesta, il contenuto essenziale del presente accordo.

ART. 7 – Principi del trattamento ed esercizio dei diritti da parte degli interessati

Ciascuno dei Titolari è tenuto a garantire la liceità di tutti i trattamenti di dati da esso effettuati, compresi quelli effettuati in contitolarità. I Contitolari adottano le misure tecniche ed organizzative utili affinché i diritti degli interessati di cui agli articoli da 15 a 22 del GDPR possano essere esercitati in qualsiasi momento secondo quanto previsto dalle citate disposizioni. Gli interessati, ai sensi dell'art. 26, comma 3 del GDPR, potranno fare riferimento a ciascuno dei Contitolari per l'esercizio dei propri diritti. Al fine di agevolare gli interessati, le richieste di questi ultimi per l'esercizio dei propri diritti saranno gestite, per conto e nell'interesse di tutti i Contitolari, dal Contitolare _____ [*specificare*], rivolgendosi al relativo Responsabile della Protezione dei Dati (DPO), contattabile al seguente punto di contatto: _____ [specificare]. Ciascun Contitolare si impegna a trasmettere tempestivamente all'altro Contitolare la richiesta relativa all'esercizio di diritti da parte dell'interessato, ed il Contitolare ricevente si impegna a fornire tempestivamente al Contitolare richiedente le informazioni necessarie richieste, qualora non in possesso dell'altro Contitolare.

ART. 8 – Gestione eventi di Data Breach

Responsabile della gestione di eventuali eventi di violazione dati personali (data breach) è il Contitolare _____ [*specificare*], che è tenuto a notificare al Garante Privacy ed agli interessati, ove ne ricorrano le condizioni, la violazione dei dati personali ai sensi degli artt. 33 e 34 del GDPR per tutte le attività di cui all'art. 2 del presente accordo. A tal fine, le parti sono tenute ad informarsi reciprocamente e tempestivamente degli eventuali casi di violazioni di dati, scambiandosi senza ritardo le informazioni necessarie per l'attuazione della notifica entro le 72 dalla conoscenza della violazione come previsto dal GDPR. Le parti si impegnano inoltre alla massima collaborazione, onde mitigare gli eventuali impatti derivanti dalle violazioni sui diritti e libertà degli interessati.

ART. 9 – Individuazione del Responsabile del trattamento

Le parti si impegnano a procedere, nell'ambito del presente accordo, alla nomina di Responsabili del trattamento ex art. 28 GDPR solo previa autorizzazione scritta dell'altra parte. Le parti si impegnano altresì ad informarsi reciprocamente rispetto a qualsiasi modifica o sostituzione dei Responsabili del trattamento.

ART. 10 – Responsabilità Le parti sono responsabili in solido nei confronti degli interessati per i danni causati da un trattamento non conforme al GDPR.

Nei rapporti fra le parti, ciascun Contitolare è responsabile solo per i danni derivanti dalla rispettiva organizzazione.

ART. 11 - DISPOSIZIONI CONCLUSIVE

Eventuali modifiche al presente Accordo dovranno essere apportate per iscritto e potranno essere modificate solo attraverso una dichiarazione scritta concordata tra le Parti.

L'invalidità, anche parziale, di una o più delle clausole del presente Accordo non pregiudica la validità delle restanti clausole.

Con il presente Accordo le Parti intendono espressamente revocare e sostituire ogni altro contratto o accordo tra esse esistente, relativo al trattamento dei dati personali.

Le Parti hanno letto e compreso il contenuto del presente Accordo e sottoscrivendolo esprimono pienamente il loro consenso.

Specificare (*se Il Direttore Generale Delegato dal Titolare o Dirigente Designato*	Il Contitolare del trattamento)
per Regione Basilicata	(Ente/Società/altro soggetto)
dott. _____	dott. _____

ATTO GIURIDICO DI NOMINA QUALE RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679

DISCIPLINA DEI TRATTAMENTI: COMPITI E ISTRUZIONI PER IL TRATTAMENTO

Premesso che:

Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati (di seguito solo "**GDPR**") disciplina, all'art. 28, i casi in cui un trattamento debba essere effettuato, per conto del titolare del trattamento, da un responsabile, per tale dovendosi intendere la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che offre garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato, e a cui il titolare ricorre per il trattamento;

l'art. 28, comma 1, del GDPR stabilisce che "Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato";

l'art. 28 comma 3. del GDPR stabilisce che, i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento;

l'art. 28, comma 3, lett. b) del GDPR stabilisce che, nell'ambito del contratto o da altro atto giuridico a norma del punto precedente, sia previsto, in particolare, che il Responsabile "garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza";

l'art. 29 del GDPR stabilisce che il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare 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;

l'art. 9 del GDPR definisce "categorie particolari di dati personali" i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

l'art. 4 del GDPR definisce al:

comma 1), «dato personale», "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno

o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale";

al considerando numero 81 del GDPR che prevede che "Per garantire che siano rispettate le prescrizioni del presente regolamento riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del titolare del trattamento, quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento….. L'esecuzione dei trattamenti da parte di un responsabile del trattamento dovrebbe essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincoli il responsabile del trattamento al titolare del trattamento, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato…..Dopo il completamento del trattamento per conto del titolare del trattamento, il responsabile del trattamento dovrebbe, a scelta del titolare del trattamento, restituire o cancellare i dati personali salvo che il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento prescriva la conservazione dei dati personali".

comma 2), «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione";

comma 7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

comma 8) «**responsabile del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

comma 9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati 4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

comma 10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Richiamato il Decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, integrato con le modifiche introdotte dal:

- D.lgs. 10 agosto 2018, n. 101, recante “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)” (in G.U. 4 settembre 2018 n.205);
- D.L. 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205 e dal decreto-legge 30 settembre 2021, n. 132, convertito, con modificazioni, dalla legge 23 novembre 2021, n. 178;

la Giunta Regionale con al Deliberazione n. 540 del 19/07/2021 “ATTUAZIONE DEGLI ADEMPIMENTI PREVISTI DALLA NORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI Regolamento (UE) 2016/679 - RIDEFINIZIONE MODELLO ORGANIZZATIVO” ha proceduto ad approvare il nuovo modello organizzativo finalizzato alla gestione del trattamento dati con il quale il Titolare del trattamento ha designato i dirigenti degli Uffici, secondo l’organigramma attualmente vigente, al trattamento dei dati personali, ai sensi del predetto articolo 2 quaterdecies del D.lgs. 101/2018.

la Regione, ai sensi dell’art. 24 del GDPR, è Titolare del trattamento dei dati personali di cui all’oggetto della Convenzione/Contratto tra la Regione Basilicata e *(da specificare…….)*- Rep. n. *(da specificare……)* del *(da specificare…….)* per *(da specificare…….)* (in appresso anche più brevemente “Regione” o, congiuntamente a “*(da specificare…….)*”, "le Parti");

per l’espletamento dei servizi oggetto della Convenzione/Contratto, il Dirigente dell’Ufficio *(da specificare…….)*, designato dal Titolare, intende nominare *(da specificare…….)*, Responsabile per il trattamento dei dati personali;

(da specificare…….) rientra tra i soggetti che per esperienza, capacità ed affidabilità forniscono garanzie sufficienti del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza, per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell’interessato;

(da specificare…….) , in qualità di Responsabile, tratterà i dati personali, anche appartenenti alle “categorie particolari di dati personali” ai sensi dell’9 del GDPR, oggetto della convenzione attenendosi ai compiti e alle istruzioni impartite dal Titolare o suo Designato;

tutto ciò premesso, il Dirigente protempore dell’Ufficio *(da specificare…….)*, Designato dal Titolare del trattamento dei dati personali di cui alla DGR 540/2021 (di seguito, per brevità, solo il “Designato”),

NOMINA

ai sensi e per gli effetti dell’art. 28 del GDPR, *(da specificare…….)*, rappresentato dal *(da specificare…….)*, quale “Responsabile del trattamento” (di seguito, per brevità, solo il “Responsabile”) per l’espletamento dei servizi previsti dalla Convenzione/Contratto per *(da specificare…….)*

(da specificare…….) in persona del *(da specificare…….)*, con la sottoscrizione del presente Atto dichiara espressamente di accettare la nomina e dichiara di conoscere gli obblighi che, per effetto di tale accettazione, assume in relazione a quanto prescritto dal GDPR, dalla normativa nazionale in materia e dalle prescrizioni del Garante per la protezione dei dati personali (di seguito, per brevità, solo il "Garante").

Dalla sottoscrizione dell'Atto di nomina, il Responsabile si vincola alla scrupolosa osservanza, oltre che delle apposite istruzioni ricevute dal Designato – a partire da quelle contenute nello stesso nell'Atto di nomina e, successivamente, di quanto a tal fine indicato dal Titolare - delle disposizioni contenute nel GDPR, in particolare per quanto concerne le modalità con cui effettuare le operazioni affidate, la sicurezza dei dati oggetto del trattamento, gli adempimenti e le responsabilità nei confronti degli interessati, dei terzi e dell'Autorità del Garante.

(da specificare…….) , in qualità di Responsabile, assicura che i dati personali vengano utilizzati per fini non diversi da quelli previsti dalle disposizioni normative vigenti e limitatamente ai trattamenti strettamente connessi agli scopi di cui al presente Accordo nell'ambito delle condizioni di liceità richiamate a fondamento dello stesso.

Ai sensi dell'art. 5 del GDPR, i dati dovranno essere trattati nel rispetto dei principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Anche se necessario, attraverso l'implementazione e/o l'adozione delle misure tecniche ed organizzative previste per legge o regolamento e comunque di quelle volte a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei dati, dei servizi e dei sistemi impiegati durante le operazioni di trattamento, garantendo un elevato standard di sicurezza e protezione dei dati.

È fatto divieto a *(da specificare…….)* di utilizzare i dati per scopi diversi da quelli previsti dalla Convenzione/Contratto, nonché da quelli consentiti dalla normativa vigente in materia di consultazione delle banche dati, con particolare riferimento alla tutela della riservatezza delle persone. *(da specificare…….)* assicura altresì che i dati medesimi non siano divulgati, comunicati, ceduti a terzi, né in alcun modo riprodotti.

In conformità a quanto al precedente comma, *(da specificare…….)* avrà cura di designare i propri operatori quali "Persone autorizzate".

(da specificare…….) , in qualità di "Responsabile", impartisce precise e dettagliate istruzioni alle "Persone autorizzate" e, in tale ambito, provvede a richiamare l'attenzione sulle responsabilità connesse all'uso illegittimo dei dati e sul corretto utilizzo delle funzionalità dei collegamenti.

Le Parti assicurano piena collaborazione e si scambiano tempestivamente ogni informazione utile in ordine a qualsiasi violazione dei dati o incidenti informatici, eventualmente occorsi nell'ambito dei trattamenti effettuati, che possano avere un impatto significativo sui dati personali, in modo che si adempia, nei termini prescritti, alla dovuta segnalazione di c.d. "data breach" al Garante in osservanza di quanto disposto dall'articolo 33 del GDPR e dal Provvedimento n. 393 del 2 luglio 2015 dell'Autorità Garante.

Compiti del Responsabile del trattamento

Il Designato dal Titolare affida al Responsabile le operazioni di trattamento dei dati personali - anche appartenenti alle "categorie particolari di dati personali" ai sensi dell'9 del GDPR -, esclusivamente per le finalità indicate nella medesima Convenzione/Contratto.

Il Responsabile conferma la sua diretta ed approfondita conoscenza degli obblighi che assume in relazione alle disposizioni contenute nel GDPR ed assicura che la propria struttura organizzativa è idonea ad effettuare il trattamento dei dati di cui alla convenzione nel pieno rispetto delle prescrizioni legislative, ivi compreso il profilo della sicurezza e si impegna a realizzare, ove mancante, tutto quanto ritenuto utile e necessario per il rispetto e l'adempimento di tutti gli obblighi previsti dal GDPR, nei limiti dei compiti che gli sono affidati.

Il Responsabile si vincola a comunicare al Titolare per il tramite del Designato qualsiasi mutamento delle garanzie offerte o gli elementi di valutazione in ordine all'incertezza del mantenimento delle stesse, con riferimento all'adozione delle misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato, considerato che la sussistenza di tali garanzie è presupposto per la presente nomina a Responsabile e per il suo mantenimento.

Il Titolare per il tramite del Designato comunicherà al Responsabile qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei dati. Il Responsabile e i soggetti autorizzati al trattamento sotto la sua diretta autorità non potranno effettuare nessuna operazione di trattamento dei dati, compresi anche quelli appartenenti alle "categorie particolari di dati personali" ai sensi dell' 9 del GDPR, al di fuori delle regole previste nella Convenzione/Contratto e osserveranno, in ogni fase del trattamento, il rispetto dei principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, sanciti dall'art. 5 del GDPR.

Modalità di espletamento dei compiti

Il Responsabile si impegna a trattare i dati personali solo per le finalità e i tempi strettamente necessari all'erogazione dei servizi forniti per conto del Titolare, come previsti nella Convenzione/Contratto, nel pieno rispetto sia della normativa vigente - con particolare riguardo alle norme del GDPR – sia delle istruzioni fornite

dal Titolare per il tramite del Designato, a cominciare da quelle indicate nel presente Atto, nonché le ulteriori eventualmente contenute in successive comunicazioni che, a tale fine, gli saranno formalizzate.

Il Responsabile avrà particolare riguardo ad attenersi alle modalità indicate dal Titolare per il tramite del Designato per effettuare le operazioni affidate, alla tutela della sicurezza dei dati oggetto del trattamento, agli adempimenti e alle responsabilità nei confronti degli interessati, dei terzi e del Garante.

Laddove il Responsabile rilevi la sua impossibilità a rispettare le istruzioni impartite dal Titolare per il tramite del Designato, anche per caso fortuito o forza maggiore, deve tempestivamente informare il Titolare per il tramite del Designato per concordare eventuali ulteriori misure di protezione. In tali casi, comunque, il Responsabile adotterà tempestivamente ogni possibile e ragionevole misura di salvaguardia.

Il Responsabile si impegna ad adottare le misure di sicurezza per la protezione dei dati idonee a garantirne la riservatezza, l'integrità, la disponibilità e la custodia in ogni fase del trattamento così da ridurre al minimo i rischi di perdita e distruzione, anche accidentale, dei dati stessi, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità dei servizi oggetto della convenzione. In tale ambito il Responsabile adotta un sistema di sicurezza, anche per l'identificazione ed autenticazione dei soggetti autorizzati alle operazioni sui dati, mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio presentato dal trattamento in linea con le disposizioni di cui all'art. 32 del GDPR.

Il Responsabile deve inoltre essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste le sanzioni amministrative e penali stabilite di cui all'art. 83 del GDPR e agli artt. 166, 167, 167 bis e 167 ter del D.lgs. 196/2003 e s.m.i..

Persone autorizzate al trattamento

Il Responsabile assicura che il trattamento affidato sarà svolto esclusivamente da persone preventivamente autorizzate. Il Responsabile si impegna ad individuare e nominare le persone fisiche autorizzate al trattamento dei dati quali "Persone autorizzate", scegliendo tra i propri dipendenti e collaboratori, che operano sotto la sua diretta autorità, quelli reputati idonei ad eseguire le operazioni di trattamento, nel pieno rispetto delle prescrizioni legislative, impartendo loro, per iscritto, le idonee indicazioni per lo svolgimento delle relative mansioni, con l'assegnazione di apposite credenziali e uno specifico profilo di abilitazione e attraverso la definizione di regole e modelli di comportamento.

Il Responsabile indica precise e dettagliate istruzioni alle persone autorizzate e, in tale ambito, provvede a richiamare l'attenzione sulle responsabilità connesse all'uso illegittimo dei dati e sul corretto utilizzo delle funzionalità dei collegamenti; in tale ambito, il Responsabile impegna le "Persone autorizzate" al trattamento alla riservatezza anche attraverso l'imposizione di un adeguato obbligo legale di riservatezza.

Il Responsabile deve provvedere, nell'ambito dei percorsi formativi predisposti per i soggetti autorizzati al trattamento dei dati, alla specifica formazione sulle modalità di gestione sicura e sui comportamenti prudenziali nella gestione dei dati personali, specie con riguardo all'obbligo legale di riservatezza cui gli stessi sono soggetti.

Il Responsabile, in osservanza dell'art. 32, paragrafo 4, del GDPR, assicura che chiunque agisca sotto la sua autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Designato del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Il Titolare per il tramite del Designato eseguirà controlli, anche a campione, finalizzati ad una verifica dell'applicazione delle istruzioni impartite al Responsabile nonché della conformità delle operazioni di trattamento alla normativa di riferimento in materia. Qualora tali controlli implichino l'accesso ai locali del Responsabile, quest'ultimo si impegna a consentire l'accesso ai rappresentanti del Titolare, salvo preavviso di almeno cinque giorni lavorativi. Detti controlli si svolgeranno con modalità tali da non interferire con la regolare attività del Responsabile. A tal fine il Titolare per il tramite del Designato potrà richiedere al Responsabile di essere relazionato per iscritto attraverso regolari report.

Comunicazione e diffusione dei dati

Il Responsabile, al di fuori dei casi previsti da specifiche norme di legge, non può comunicare e/o diffondere dati senza l'esplicita autorizzazione del Designato o del Titolare.

Obblighi di collaborazione con il Titolare/Designato

Il Responsabile:

- si impegna a comunicare tempestivamente al Titolare per il tramite del Designato qualsiasi richiesta di esercizio dei diritti dell'interessato ricevuta ai sensi degli artt. 15 e seguenti del GDPR, per consentirne l'evasione nei termini previsti dalla legge, e ad avvisarlo immediatamente in caso di ispezioni, di richiesta di informazioni e di documentazione da parte del Garante, fornendo, per quanto di competenza, il supporto eventualmente richiesto;
- a norma dell'art. 33, paragrafo 2, del GDPR, deve informare senza ritardo il Titolare per il tramite del Designato, fornendo ogni informazione utile, in caso di violazione dei dati o incidenti informatici eventualmente occorsi nell'ambito dei trattamenti effettuati per conto del Titolare, che possano avere un impatto significativo sui dati personali, in modo che il medesimo Titolare per il tramite del Designato adempia, nei termini prescritti, alla dovuta segnalazione di c.d. "data breach" al Garante per la protezione dei dati personali in osservanza al GDPR;
- tenendo conto della natura del trattamento e delle informazioni di cui dispone, deve assistere il Titolare per il tramite del Designato nel garantire il rispetto di tutti gli obblighi di cui agli artt. da 32 a 36 del GDPR. In particolare, conformemente all'art. 28, paragrafo 3, lett. f) del GDPR, deve assistere il Titolare per il tramite del Designato nell'esecuzione della valutazione d'impatto sulla protezione dei dati e fornire tutte le informazioni necessarie;
- coopera con il Titolare per il tramite del Designato per garantire agli interessati, per quanto di propria competenza, un effettivo ed efficace esercizio dei diritti di cui agli artt. 15 e successivi del GDPR;

- È dovere del Responsabile assistere il Titolare per il tramite del Designato, con misure tecniche e organizzative adeguate, nell'adempimento dei suoi obblighi di riscontro alle richieste degli interessati, sia fornendo allo stesso tutte le informazioni e i dati in suo possesso, sia adoperandosi materialmente per consentire al Titolare per il tramite del Designato di dar seguito alle istanze ricevute. Qualora l'implementazione di dette misure di sicurezza tecniche e organizzative rientrino nell'ambito degli obblighi contrattuali il Responsabile provvede direttamente ad effettuarne l'implementazione dandone comunicazione al Titolare per il tramite del Designato. Qualora, invece, queste non rientrino nell'ambito contrattuale in essere, provvede in ogni caso a comunicare al Titolare per il tramite del Designato la necessità di provvedere all'implementazione, fornendo le opportune informazioni per valutarne i costi.

Ulteriori disposizioni

Il Responsabile adotta tutte le necessarie misure e gli accorgimenti circa le funzioni di "amministratori di sistema" in conformità al Provvedimento Generale del Garante del 27 novembre 2008, così come modificato in base al provvedimento del 25 giugno 2009; in particolare, designa individualmente per iscritto gli "amministratori di sistema" (e funzioni assimilate), con elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, attribuendo tali funzioni previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato. Il Responsabile conserva l'elenco degli amministratori di sistema, con gli estremi identificativi e le funzioni loro attribuite e, qualora richiesto, comunica tale elenco al Titolare per il tramite del Designato (ad esclusione delle attività di competenza del Centro Tecnico Regionale).

Nel caso in cui il Responsabile del trattamento trasferisca i dati personali trattati verso un Paese terzo o un'Organizzazione internazionale per adempiere ad un obbligo giuridico di cui è soggetto dovrà informare della circostanza il Titolare per il tramite del Designato prima dell'inizio delle attività di trattamento o del trasferimento stesso, salvo che ciò sia vietato da rilevanti motivi d'interesse pubblico o obblighi di legge o regolamento.

Il Responsabile designato potrà avvalersi di un altro soggetto per lo svolgimento di parte delle attività di trattamento a lui delegate (cosiddetto "sub-responsabile") previa autorizzazione scritta, specifica o generale da parte del Titolare per il tramite del Designato del trattamento. L'incarico conferito dovrà essere disciplinato da un atto di designazione a Responsabile del trattamento conforme a quanto previsto dall'Articolo 28, comma 2 e 4, del GDPR. In caso di autorizzazione scritta generale, il Responsabile dovrà informare il Titolare per il tramite del Designato di eventuali designazioni o sostituzioni dei sub-responsabili del trattamento; il Titolare per il tramite del Designato si riserva la facoltà di opporvisi nel termine di 30 giorni dal momento in cui viene informato della circostanza da parte del Responsabile.

Il Responsabile risponde dei danni causati nel corso delle operazioni di trattamento dall'operato dei soggetti da lui autorizzati, fatto salvo il diritto di rivalersi nei loro confronti.

Il Responsabile garantisce al Titolare per il tramite del Designato che gli Autorizzati al trattamento dei dati personali da lui designati sono vincolati al più stretto riserbo sulla base di atti negoziali (es. codici di condotta interni, accordi di riservatezza specifiche, ecc.) o disposizioni normative previste dal diritto dell'Unione o dal diritto nazionale cui il Responsabile e gli Autorizzati al trattamento dei dati personali sono soggetti.

Disposizioni finali

Con la sottoscrizione del presente Atto, il Responsabile accetta la nomina attenendosi alle istruzioni ivi indicate e alle disposizioni di legge ed eventuali successive modifiche ed integrazioni e ad ogni altra normativa vigente in materia di protezione di dati personali.

Fatta eccezione per quanto diversamente previsto, il presente Atto di Nomina cesserà, comunque, di produrre i suoi effetti allo scadere naturale della stessa/o ovvero e/o allo scadere dell'estensione della Convenzione/Contratto.

Il presente atto di nomina ha durata pari alla durata del contratto e si intende concluso allo scadere naturale dello stesso ovvero allo scadere dell'estensione del contratto stesso. Il presente atto di nomina si intende revocato allo scioglimento, per qualsiasi causa, del medesimo vincolo legale.

Alla scadenza della Convenzione/Contratto, indicato precedentemente, qualora non rinnovato, il Responsabile dovrà restituire al Titolare per il tramite del Designato tutti i dati personali elaborati per suo conto e cancellarli in modo permanente dai sistemi informativi nella sua disponibilità, salvo che lo stesso non sia soggetto a specifici obblighi di conservazione ai sensi di legge o regolamento.

Per tutto quanto non espressamente previsto nel presente Atto e nella Convenzione/Contratto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Il Designato al Trattamento **XXXXXXXXXXXX**

per accettazione dell'incarico

INFORMAZIONI E ISTRUZIONI AGLI AUTORIZZATI

In ottemperanza alle disposizioni del Codice in materia di protezione dei dati personali D.lgs 196/03 e s.m.i. recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 (RGPD) ed in relazione alle attività svolte nell'ambito istituzionale l'*autorizzato*, dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni e ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal *Titolare del Trattamento* o dal *Designato al Trattamento* presso il quale opera.

I dati personali devono essere trattati:

a) in osservanza dei criteri di riservatezza;
b) in modo lecito e secondo correttezza;
c) per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
d) nel pieno rispetto delle misure di sicurezza definite, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le misure di sicurezza definite sono obbligatorie, e sono state anche distinte in funzione delle seguenti modalità di trattamento dei dati:

1. **Con l'ausilio di strumenti elettronici** (es. PC, notebook, tablet o smartphone);
2. **Senza l'ausilio di strumenti elettronici** (es. dati in archivi cartacei o su supporti magnetici/ottici);
3. **Di carattere generale.**

Trattamenti dati con Strumenti Elettronici

Gli autorizzati al trattamento dovranno attenersi alle seguenti misure di sicurezza:

- accedere ai sistemi informativi esclusivamente per mezzo di credenziali di autenticazione personali; le credenziali di autenticazione consistono in un codice (user id o username) per l'identificazione dell'autorizzato, associato ad una parola chiave (password) conosciuta solo dall'autorizzato;
- utilizzare la password con una lunghezza minima di otto caratteri, composte sia da numeri che lettere e caratteri speciali (o, se il sistema informativo in uso non lo permette, dal numero massimo di caratteri consentito) e differente dallo user id;
- ove non definito dall'Amministratore della rete, nella generazione della password non utilizzare elementi o notizie facilmente riconducibili all'autorizzato e non utilizzare password simili alla precedente;
- ove non definito dall'Amministratore della rete, modificare la password al primo utilizzo del sistema informativo, quindi ogni volta che viene richiesto dal sistema (al massimo 6 mesi, 3 mesi se i dati trattati sono particolari - ad. es. di salute - e/o giudiziari) e nel caso vi sia il dubbio che la stessa password abbia perso il carattere di segretezza;
- qualora il sistema non renda obbligatoria la modifica della password nel rispetto dei predetti termini, provvedere autonomamente a tale variazione;
- adottare particolari cautele per assicurare la segretezza della password (evitare la digitazione in presenza di terzi, conservarne i riferimenti in luogo non accessibile a terzi) custodendola con diligenza e riservatezza;

- per le banche dati automatizzate che utilizzano il proprio codice di accesso personale, evitare di operare su altre postazioni di lavoro al fine di non incorrere in trattamenti non autorizzati;
- tenere un comportamento corretto durante la navigazione in internet, così come previsto dalle disposizioni interne sulla modalità di utilizzo dei servizi di rete e non è consentito navigare sui siti web non attinenti allo svolgimento delle mansioni assegnate;
- non aprire messaggi di posta provenienti da soggetti esterni *non accreditati* e non utilizzare l'indirizzo di posta elettronica istituzionale per fini personali;
- non comunicare la mail istituzionale a siti per i quali non siete interessati per fini lavorativi;
- non trasmettere dati particolari (ex sensibili) via e-mail. Nel caso in cui sia strettamente necessaria tale forma di trasmissione per ragioni d'ufficio, occorrerà porre in essere gli accorgimenti atti ad impedire la visione del contenuto del file da parte di soggetti non autorizzati o non legittimati al trattamento, che siano diversi dai destinatari delle comunicazioni elettroniche. In particolare, si raccomanda il ricorso all'uso di tecniche di criptazione o di cifratura dei messaggi, ovvero il ricorso all'uso di codificazione dei dati contenuti nel testo delle comunicazioni;
- bloccare la propria postazione di lavoro informatica durante la pausa pranzo, ovvero in tutte le occasioni in cui ci si assenti o ci si allontani anche temporaneamente dalla propria postazione di lavoro; nel caso in cui fosse necessario mantenere accesa la postazione di lavoro, utilizzare i metodi messi a disposizione dal sistema per bloccare la stessa, come ad esempio il blocco sessione o il salvaschermo con password;
- adottare tutte le cautele necessarie atte ad evitare l'accesso ai dati personali trattati o in trattamento anche cartaceo a dipendenti o altri autorizzati;
- non lasciare la propria stazione di lavoro incustodita e collegata alla rete e/o ai sistemi informativi con il proprio account (nome utente) e password;
- non alterare in alcun modo la configurazione software della postazione di lavoro, evitando di installare qualunque software sconosciuto o non autorizzato dal competente reparto ICT;
- non utilizzare la rete dell'Amministrazione per fini personali e non espressamente autorizzati.

Trattamenti senza l'ausilio di Strumenti Elettronici

Gli autorizzati al trattamento dovranno attenersi alle seguenti istruzioni:

- garantire sempre la corretta custodia dei dati personali; i documenti non devono essere lasciati incustoditi sulla propria scrivania e/o in luoghi aperti al pubblico in assenza di altri autorizzati addetti al medesimo trattamento; non devono essere altresì consultati da altri autorizzati non abilitati al trattamento; non possono essere riprodotti o fotocopiati se non per esigenze connesse alla finalità del trattamento;
- per il tempo necessario allo svolgimento delle operazioni di trattamento, si dovrà diligentemente controllare e custodire gli atti e documenti contenenti dati personali per evitare visione, possesso, utilizzo non autorizzati; conservare i documenti o gli atti che contengono dati particolari (ex dati sensibili) e/o giudiziari in archivi ad accesso controllato (armadi/schedari/contenitori chiusi da apposita serratura oppure soggetti a sorveglianza da parte di personale preposto);
- al termine delle operazioni di trattamento, restituire tempestivamente la documentazione prelevata dagli archivi ed assicurarsi che questa venga opportunamente riposta;
- in caso di utilizzo di stampante, fotocopiatrice o fax condivisi da vari utenti e collocati al di fuori dei locali ove è posta la singola postazione di lavoro, le stampe devono essere o immediatamente raccolte e custodite con le modalità sopra descritte; Qualora i documenti da stampare contengano dati particolari è necessario, nei limiti del possibile, presenziare la fase di stampa o utilizzare la modalità di stampa protetta;
- non gettare via copie cartacee contenenti dati personali, senza averle prima distrutte in modo opportuno o comunque avere reso l'identificazione dell'interessato impossibile;
- adottare misure che siano idonee a limitare la conoscenza dei dati personali e/o particolari qualora essi siano presenti nei flussi documentali dell'amministrazione garantendo il rispetto della riservatezza dei dati degli interessati, ad esempio riponendo, i documenti in cassetti o armadi debitamente chiusi a chiave.
- è assolutamente vietato cedere a soggetti esterni i dati personali di cui si è venuti a conoscenza durante lo svolgimento dell'incarico.

Misure di carattere generale

Gli autorizzati al trattamento dovranno attenersi alle seguenti istruzioni:

- assicurare la riservatezza opportuna e necessaria affinché il trattamento dei dati, sia effettuato in conformità alle disposizioni del RGPD e del D.lgs 196/2003 e s.m.i.;
- assicurare la somministrazione dell'informativa al trattamento dati ogni qual volta venga coinvolto un nuovo interessato;
- assicurarsi, quando previsto, che sia stato rilasciato il consenso al trattamento dati da parte dell'interessato;
- rispettare, se presente, il documento sulla sicurezza dei dati, predisposto dall'Amministrazione;
- è consentita la trasmissione di dati all'interno dell'Amministrazione per i compiti ed i fini stabiliti dalla stessa per mezzo del Titolare, agendo sotto la sua diretta autorità, allo stesso modo sono autorizzati i trattamenti di dati pseudonimizzati;
- sono consentite le comunicazioni di dati personali che avvengono nell'ambito di un rapporto contrattuale/convenzionale instaurato dall'Amministrazione con terzi per l'esternalizzazione di attività/funzioni/servizi, a condizione che il terzo sia stato nominato Responsabile (esterno) del trattamento dei dati;
- è vietata ogni comunicazione/diffusione di dati verso l'esterno dell'Amministrazione senza preventiva autorizzazione; il divieto permane anche dopo la cessazione dell'incarico e/o del rapporto di lavoro;
- è vietato l'utilizzo improprio di documenti, dati, informazioni a qualsiasi titolo posseduti, ricevuti o trasmessi;
- è vietato raccogliere, registrare e conservare i dati personali presenti negli atti e documenti contenuti nei fascicoli e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- è vietato cedere ad altri dati personali di cui si è venuti a conoscenza durante lo svolgimento dell'incarico;
- è necessario astenersi dall'effettuare operazioni di trattamento dei dati personali, di cui si è venuti a conoscenza durante lo svolgimento dell'incarico, evitando di conservarli, duplicarli, comunicarli o cederli ad altri, dopo la cessazione del rapporto di lavoro;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- informare tempestivamente il proprio Dirigente di ogni questione rilevante in relazione al trattamento di dati personali effettuato e di eventuali richieste pervenute dagli interessati;
- nel caso in cui si constati o si sospetti un disguido o un incidente che abbia messo o possa mettere a repentaglio la sicurezza e/o la riservatezza dei dati trattati, darne immediata comunicazione al proprio Dirigente;
- segnalare al proprio Dirigente eventuali circostanze, che richiedano il necessario ed opportuno aggiornamento delle misure di sicurezza adottate, al fine di ridurre al minimo i rischi di diffusione, distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- fornire al Titolare o al Designato, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro una adeguata azione di controllo e verifica di eventuali incidenti che possano essersi verificati;
- eseguire qualsiasi operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- recepire nuove indicazioni fornite dal Titolare del Trattamento o dal Designato anche partecipando a percorsi formativi quando previsti;

- trattare i dati personali, eventualmente riferiti a categorie particolari (art. 9) o relativi a condanne penali e reati (art. 10), è ammesso se lecito (art. 6) e cioè quando:
    - l'interessato ha espresso il consenso al trattamento dei propri dati personali;
    - il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
    - il trattamento è necessario per adempiere ad un obbligo di legge cui è tenuto il Titolare o per salvaguardare gli interessi vitali dell'interessato;
    - il trattamento è necessario per il perseguimento del legittimo interesse del Titolare;
- garantire all'interessato l'esercizio dei diritti sui propri dati personali secondo quanto previsto dal Regolamento RGPD (es: diritto di accesso, di rettifica, di limitazione, di portabilità, di opposizione, ecc.) segnalando al proprio referente qualsiasi richiesta in questo senso.

Le presenti istruzioni rivestono carattere generale e sono suscettibili di essere integrate, specificate e aggiornate dal "Titolare" del trattamento dei dati, nel rispetto di quanto previsto dalla normativa vigente in materia di protezione dei dati personali e pubblicate nella sezione "Trattamento dati personali e Privacy" nella intranet dell'Amministrazione.

REGIONE BASILICATA

ALLEGATO 5

Lista controlli per la piena aderenza ai requisiti di sicurezza del datacenter e per la qualificazione di servizi cloud e delle infrastrutture

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Critici	**AFFIDABILITA'**		A.DC-3: Sono disponibili soluzioni di Disaster Recovery con tempi di ripristino garantiti	1.Provider di infrastruttura: L'infrastruttura digitale è dotata di soluzioni di DR e deve garantire tempi di ripristino (RTO e RPO) variabili in funzione della criticità dell'applicazione ospitata conformemente con quanto definito nella BR. Devono comunque essere garantiti almeno i seguenti parametri di ripristino in caso di disastro: RTO 12 ore e RPO 12 ore.			
Critici	**AFFIDABILITA'**		A.DC-3: Sono disponibili soluzioni di Disaster Recovery con tempi di ripristino garantiti	2.Public Cloud provider: devono essere presenti servizi cloud di Disaster Recovery.			
Critici	DATACENTER SECURITY	**Data Center security**	A.DC-1: La progettazione/realizzazione del Data Center garantisce la manutenibilità a caldo, conformemente agli standard di mercato	1. L'infrastruttura digitale deve aderire ai parametri del certificato ANS1/TIA 942B con rating "Concurrent Maintainability" oppure a quello di Tier III dell'Uptime Institute. In alternativa deve essere conforme alle caratteristiche costruttive, degli impianti meccanici, elettrici e antincendio riportati alla Tabella 2.			
Critici	**DETECT (DE)**	**Detection Processes (DE.DP):** Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	**DE.DP-1:** Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	1. Le nomine di cui alla sottocategoria 1D-AM-6 sono rese note all'interno del soggetto.			
Critici	**DETECT (DE)**	**Detection Processes (DE.DP):** Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	**DE.DP-1:** Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	2. 1 ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sull'Infrastruttura digitale sono ben definiti e resi noti alle articolazioni competenti del soggetto.			
Critici	**DETECT (DE)**	**Detection Processes (DE.DP):** Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	**DE.DP-1:** Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	3. Esiste un documento aggiornato di dettaglio che indica almeno: a.i ruoli, i processi e le responsabilità di cui al punto 2; b.i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti 1 e 2.			
Critici	**DETECT (DE)**	**Detection Processes (DE.DP):** Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	**DE.DP-1:** Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	4. È definito ed implementato un sistema per la notifica all'Amministrazione degli eventi anomali che coinvolgono le applicazioni e l'infrastruttura sottostante, identificati sulla base di metriche previamente concordate.			
Critici	**DETECT (DE)**		**DE.AE-3**: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	1. Ai fini di rilevare tempestivamente incidenti con impatto dell'infrastruttura, sono adottati gli strumenti tecnici e procedurali per: a.acquisire le informazioni da più sensori e sorgenti; b.ricevere e raccogliere informazioni inerenti alla sicurezza dell'infrastruttura rese note dal CSIRT Italia, da fonti interne o esterne al soggetto; c.analizzare e correlare, anche in maniera automatizzata, i dati e le informazioni di cui alle lettere a), b) e c), per rilevare tempestivamente eventi di interesse.			
Critici	**DETECT (DE)**		**DE.AE-3**: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	2. Le attività di analisi e correlazione di cui al punto precedente sono monitorate e registrate. La relativa documentazione, anche elettronica, è conservata per almeno 24 mesi.			
Critici	**DETECT (DE)**		**DE.AE-3**: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	3. Sono definite: a.le politiche applicate per individuare i sensori e le sorgenti di cui al punto 1, lettera a); b.le procedure e gli strumenti tecnici per ottenere le informazioni di cui al punto 1, lettere a) e b); c.le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui al punto 1, lettera c). d.i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al punto 2.			
Critici	**DETECT (DE)**		**DE.AE-3**: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	4. Sono presenti politiche e procedure di Jogging, monitoraggio, sicurezza e conservazione di registri di accesso, le quali dovranno essere aggiornate almeno su base annuale.			
Critici	**DETECT (DE)**		**DE.AE-3**: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	5. È adottato un sistema di auditing per il rilevamento di informazioni inerenti alla sicurezza, il monitoraggio degli accessi, modifiche o cancellazioni non autorizzate di dati o metadati.			
Critici	**DETECT (DE)**		**DE.AE-3**: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	6. Sono definiti e valutati processi, procedure e misure tecniche per la segnalazione di anomalie e guasti del sistema di monitoraggio e in grado di fornire una notifica immediata al soggetto responsabile.			
Critici	**DETECT (DE)**		**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	1.Con riferimento alla sottocategoria PR.AC-3, viene rilevata la presenza di personale con potenziale accesso fisico o remoto non autorizzato alle risorse. A tal fine, sono presenti sistemi di sorveglianza e controllo di accesso, anche automatizzati.			
Critici	**DETECT (DE)**		**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	2.Con riferimento alla sottocategoria ID.AM-1, vengono rilevati dispositivi (anche fisici) non approvati. A tal fine, fatti salvi documentati limiti tecnici, sono presenti almeno dei sistemi di controllo di accesso di rete.			
Critici	**DETECT (DE)**		**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	3, Gli strumenti tecnici di cui ai punti 1 e 2 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.1P e PR.MA e concorrono al rispetto delle politiche di cui alle categorie 1DAM, ID.GV, ID.SC, PR.AC e PR.DS.			
Critici	**DETECT (DE)**		**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	4. Esiste un documento aggiornato che descrive, almeno: a.le politiche di sicurezza adottate in relazione ai punti 1 e 2; b.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	DETECT (DE)		**DE.AE-3:** Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	9. Esiste un repository centralizzato che contiene i log di accesso degli utenti del soggetto, gestito direttamente dal soggetto e segregato a livello logico rispetto ai sistemi a cui terze parti hanno accesso diretto			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	5. Il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali sono monitorati e correlati al fine di identificare eventi di cybersecurity.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	6. Gli strumenti tecnici di cui ai punti 1, 3, 4 e 5 sono aggiornati, manutenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.1P e PR.MA e concorrono al rispetto delle politiche di cui alla categoria ID.AM,ID.GV, ID.SC, PR.AC e PR.DS.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	7. Gli strumenti tecnici di cui ai punti 1, 3, 4 e 5sono impiegati anche per i fini di cui alla categoria DE.AE			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	8. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 1, 3, 4 e 5; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	4. Sono configurati appositi software firewall su tutti i dispositivi.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	5. I file in ingresso (tramite posta elettronica, download, dispositivi removibili, etc.) sono analizzati, anche tramite sandbox.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	6. Gli strumenti tecnici di cui ai punti 1,4 e 5 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie 1D.AM, ID.GV, ID.SC, PR.AC e PR.DS.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	7. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 1, 2 e 3; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	1. Con riferimento alla sottocategoria PR.AC-3, viene rilevata la presenza di personale con potenziale accesso fisico o remoto non autorizzato alle risorse. A tal fine, sono presenti sistemi di sorveglianza e controllo di accesso, anche automatizzati.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	2. Con riferimento alla sottocategoria 1D.AM-1, vengono rilevati dispositivi (anche fisici) non approvati. A tal fine, fatti salvi documentati limiti tecnici, sono presenti almeno dei sistemi di controllo di accesso di rete.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	3. Gli strumenti tecnici di cui ai punti le 2 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie 1D.AM, ID.GV, ID.SC. PR.AC e PR.DS.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	4. Esiste un documento aggiornato che descrive, almeno: a. !e politiche di sicurezza adottate in relazione ai punti 1 e 2; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-8:** Vengono svolte scansioni per l'identificazione di vulnerabilità	1. In base all'analisi del rischio, sulle piattaforme e sulle applicazioni software ritenute critiche sono eseguiti penetration test e vulnerability assessment, prima della loro messa in esercizio.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-8:** Vengono svolte scansioni per l'identificazione di vulnerabilità	2. Sono eseguiti periodicamente penetratron test e vulnerability assessment in relazione alla criticità delle piattaforme e delle applicazioni software.			
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-8:** Vengono svolte scansioni per l'identificazione di vulnerabilità	3. Esiste un documento aggiornato recante la tipologia di penetration test e vulnerability assessment previsti.			

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Critici	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-8:** Vengono svolte scansioni per l'identificazione di vulnerabilità	4. Esiste un registro aggiornato dei penetration test e vulnerability assessment eseguiti corredato dalla relativa documentazione.			
Critici	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-2:** Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	1. Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto.			
Critici	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-2:** Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	2. L'installazione delle piattaforme e delle applicazioni software è consentito esclusivamente per quelle approvate.			
Critici	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-2:** Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	3. Esistono politiche che limitino l'aggiunta, rimozione o aggiornamento, nonché gestione non autorizzata degli asset dell'organizzazione.			
Critici	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	5.Esiste un elenco contenente tutto il personale interno ed esterno impiegato nei processi di cybersecurity aventi specifici ruoli e responsabilità. L'elenco è disseminato presso le articolazioni competenti del soggetto.			
Critici	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	6.Esiste un elenco delle figure analoghe all'incaricato di cui al punto 2 e al referente tecnico di cui al punto 3 presso terze parti, in relazione alle dipendenze esterne, e presso lo stesso soggetto, in relazione alle dipendenze interne. Le competenze dell'incaricato e del referente tecnico devono essere rivalutate in funzione della tipologia di dipendenza. L'elenco è disseminato presso le articolazioni competenti del soggetto.			
Critici	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	7.L'incaricato di cui al punto 2 assicura, inoltre, la collaborazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), anche in relazione alle attività connesse all'articolo 5 del decreto-legge 105/2019 e alle attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la CyberSicurezza (NCS) di cui al decreto-legge 82/2021, e alle attività di verifica e ispezione			
Critici	IDENTIFY (ID)	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È indetificata e resa nota una policy di cybersecurity	2. 11 Documento di cui al punto 1 deve essere approvato dal soggetto e aggiornato almeno su base annuale o in corrispondenza di sostanziali variazioni all'interno dell'organizzazione.			
Critici	IDENTIFY (ID)	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-4:** La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity	1. Esiste un programma formale di Enterprise Risk Management (ERM) che include politiche e procedure per l'identificazione, la valutazione, la proprietà, il trattamento e l'accettazione dei rischi di sicurezza e privacy dell'Infrastruttura.			
Critici	IDENTIFY (ID)	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente all'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui	**ID.RA-5:** Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	4. Esiste un documento aggiornato di valutazione del rischio (risk assessment) che comprende almeno: a.l'identificazione delle minacce, sia interne che esterne, opportunamente descritte e valutate e le relative probabilità di accadimento; b.le vulnerabilità di cui alla sottocategoria ID.RA-1 e alla sottocategoria DE.CM-8; c.i potenziali impatti ritenuti significativi sull'infrastruttura digitale, opportunamente descritti e valutati; d.l'identificazione, l'analisi e la ponderazione del rischio			
Critici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	1. Esiste un documento aggiornato di dettaglio che descrive i processi di gestione del rischio inerente la catena di approvvigionamento cyber. 2. Tali processi sono validati e approvati da parte dei vertici del soggetto.			
Critici	IDENTIFY (ID)		**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	5. I nominativi e gli estremi di contatto dell'incaricato di cui al punto 2 e del referente tecnico di cui al punto 4- sono comunicati dal soggetto all'Agenzia per la Cybersicurezza Nazionale (ACN).			
Critici	IDENTIFY (ID)		**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	6. Esiste un elenco contenente tutto il personale interno ed esterno impiegato nei processi di cybersecurity aventi specifici ruoli e responsabilità. L'elenco è disseminato presso le articolazioni competenti del soggetto.			
Critici	IDENTIFY (ID)		**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	7. Esiste un elenco delle figure analoghe all'incaricato di cui ai punto 2 e al referente tecnico di cui al punto 3 presso terze parti, in relazione alle dipendenze esterne, e presso lo stesso soggetto, in relazione alle dipendenze interne. Le competenze dell'incaricato e del referente tecnico devono essere rivalutate in funzione della tipologia di dipendenza. L'elenco è disseminato presso le articolazioni competenti del soggetto.			
Critici	IDENTIFY (ID)		**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	8. L'incaricato di cui al punto 2 assicura, inoltre, la collaborazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), anche in relazione alle attività connesse all'articolo 5 del decreto-legge 105/2019 e alle attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la CyberSicurezza (NCS) di cui al decreto-legge 82/2021.			
Critici	IDENTIFY (ID)	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È indetificata e resa nota una policy di cybersecurity	3. Ogni scostamento dai livelli minimi di sicurezza definito internamente nel documento di cui al punto 1 deve essere identificato, gestito ed eventualmente autorizzato dal soggetto attraverso un processo di governa nce strutturato			
Critici	IDENTIFY (ID)	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È indetificata e resa nota una policy di cybersecurity	4. Esiste un documento aggiornato recante indicazioni in merito alla pianificazione, ai ruoli, all'implementazione, operazione, valutazione, e miglioramento di programmi di cybersecurity sia in relazione al personale interno che per eventuali terze parti			
Critici	IDENTIFY (ID)	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-1:** Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	3. Le relazioni periodiche delle verifiche e dei test di cui al punto 1 devono contenere almeno: a. la descrizione generale delle tipologie di verifiche effettuate e gli esiti delle stesse; b. la descrizione dettagliata delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza; c. il livello di esposizione delle risorse del sistema cui è possibile accedere a seguito dello sfruttamento delle vulnerabilità.			
Critici	IDENTIFY (ID)	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-1:** Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	4. Esiste un documento per la correzione delle vulnerabilità che prevede anche, la notifica alle parti interessate.			
Critici	IDENTIFY (ID)	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-5:** Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	4. Esiste un documento aggiornato di valutazione del rischio (risk assessment) che comprende almeno: a. l'identificazione delle minacce, sia interne che esterne, opportunamente descritte e valutate e le relative probabilità di accadimento; b. le vulnerabilità di cui alla sottocategoria 1D.RA-1 e alla sottocategoria DE.CM-8; c. i potenziali impatti ritenuti significativi sui servizio cloud, opportunamente descritti e valutati; d. l'identificazione, l'analisi e la ponderazione del rischio			
Critici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	3. Sono presenti politiche e procedure per la definizione, implementazione e applicazione del modello di responsabilità della sicurezza condivisa (Shared Security Responsibility Modei-SSRM] all'interno dell'organizzazione, le quali dovranno essere riviste e aggiornate almeno su base annuale.			
Critici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	4. Il modello SSRM è applicato a tutta la catena di approvvigionamento cyber, ivi inclusi altri servizi cloud utilizzati dall'organizzazione.			
Critici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	5. È fornita una chiara definizione in merito alla condivisione delle responsabilità.			
Critici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-2:** I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber	1. In merito all'affidamento di forniture per i servizi cloud sono adottate misure in materia di sicurezza della catena di approvvigionamento cyber attraverso: a. il coinvolgimento dell'organizzazione di cybersecurity, tra cui l'incaricato di cui alla sottocategoria ID.AM•6, punto 2, nel processo di fornitura, già a partire dalla fase di progettazione; b. fatti salvi documentati limiti tecnici, il rispetto del requisito di fungibilità, con la possibilità di ricorrere alla scadenza ad altro fornitore; c. fatti salvi documentati limiti tecnici, la diversificazione dei fornitori e la conseguente resilienza del servizio cloud; d. la valutazione dell'affidabilità tecnica dei fornitori e dei partner terzi, con riferimento alle migliori pratiche in materia e tenendo conto almeno: i. della qualità dei prodotti e delle pratiche di sicurezza cibernetica del fornitore e dei partner terzi, anche considerando il controllo degli stessi sulla propria catena di approvvigionamento e la priorità data agli aspetti di sicurezza; ii. della capacità del fornitore e dei partner terzi di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo.			
Critici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-2:** I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber	2. Esiste un elenco aggiornato dei fornitori e partner terzi affidatari per la fornitura di servizi cloud, nonché di dipendenze esterne, corredato dalla relativa documentazione del processo di valutazione di cui al punto 1.			
Critici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-3:** I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber	1. Le misure di sicurezza implementate dal soggetto in relazione a dipendenze interne sono coerenti, anche in relazione agli esiti dell'analisi del rischio, con le misure di sicurezza applicate al servizio cloud. A tal fine, i contratti, gli accordi o le convenzioni sono aggiornati di conseguenza.			
Critici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-4:** Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	1. Esiste un documento aggiornato che descrive i! processo, le modalità, la cadenza delle valutazioni per i fornitori e partner terzi, proporzionate agli esiti dell'analisi del rischio effettuata.			
Critici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-4:** Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	2. Esiste una pianificazione aggiornata degli audit, delle verifiche o di altre forme di valutazione previste, nonché un registro di quelli effettuati e la relativa documentazione.			
Critici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-4:** Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	3. È definito ed implementato un processo di Audit Management al fine di consentire lo svolgimento di valutazioni indipendenti e di garanzia, nel rispetto dei principali standard di settore, almeno su base annuale e secondo una pianificazione che tenga conto del rischio			

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Critici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-4:** Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	4. Le politiche e procedure di audit e garanzia degli standard, devono essere stabilite, documentate, approvate, mantenute e riviste almeno annualmente.			
Critici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-4:** Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	5. È definito, documentato, approvato, comunicato, applicato e mantenuto un piano di Reniediation.			
Critici	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	7. Esiste un documento aggiornato di dettaglio contenente almeno: a.le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e le procedure di cui ai punti 1, 2, 3, 4, 5, 6, b.le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e delle credenziali di accesso per gli utenti; c.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-2:** L'accesso fisico alle risorse è protetto e amministrato	3. E' definito un perimetro di sicurezza tra le aree amministrative e le aree di data storage e processing.			
Critici	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-3:** L'accesso remoto alle risorse è amministrato	5. Esiste un documento aggiornato di dettaglio contenente almeno: a.le politiche di sicurezza adottate per la definizione delle attività consentite tramite l'accesso remoto e le misure di sicurezza adottate; b.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-4:** I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	4. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1.			
Critici	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-5:** L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	1.Sono presenti politiche e procedure per la sicurezza dell'infrastruttura di rete, le quali dovranno essere aggiornate almeno su base annuale.			
Critici	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-5:** L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	2.È definito un piano per il monitoraggio della disponibilità, qualità e l'adeguata capacità delle risorse al fine di fornire le prestazioni di sistema richieste.			
Critici	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-7:** Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)	1. Sono definite e implementate politiche e procedure per l'accesso ai sistemi, alle applicazioni e ai dati, compresa l'autenticazione multifattoriale almeno per gli utenti privilegiati e l'accesso a dati.			
Critici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	1. Sono definite in relazione alla categoria I D.AM: a.le politiche di sicurezza adottate per la registrazione della manutenzione e riparazione delle risorse e dei sistemi; b.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-2:** La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	3. Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi.			
Critici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-2:** La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	4. Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili.			
Critici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-2:** La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	5. Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.			
Critici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1:** Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi	1.I log sono conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi.			
Critici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1:** Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi	2.Sono definite: a.le politiche di sicurezza adottate per la gestione dei log dei sistemi; b.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza con particolare riguardo all'integrità e alla disponibilità dei log.			
Critici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-5:** Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	1.In relazione ai piani previsti dalla sottocategoria PR.IP-9: a. sono adottate architetture ridondate di rete, di connettività, nonché applicative;			
Critici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-5:** Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	2.Esistono meccanismi per garantire la continuità operativa, nel rispetto delle misure di sicurezza qui elencate.			
Critici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-5:** Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	3.Sono definite: a.le politiche di sicurezza adottate in relazione ai punti 1 e 2; b.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	**PROTECT (PR)**		**PR.DS-2:** I dati sono protetti durante la trasmissione	1. Sono utilizzati canali di comunicazione sicuri e criptati durante la migrazione di server, servizi, applicazioni o dati in ambienti cloud. Tali canali devono includere solo protocolli aggiornati e approvati.			
Critici	**PROTECT (PR)**		**PR.DS-3:** Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	1. Sono definite in relazione alla categoria ID.AM, almeno: a.le politiche di sicurezza adottate per il trasferimento fisico, la rimozione e la distruzione di dispositivi atti alla memorizzazione di dati; b.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	**PROTECT (PR)**		**PR.DS-7:** Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	1. Sono definite in relazione alla categoria i D.AM, almeno: a.l'architettura di massima per cui gli ambienti sono separati e, negli eventuali punti di contatto, come la separazione è realizzata; b.le politiche di sicurezza adottate per garantire la separazione dell'ambiente di sviluppo e test da quello di produzione; c.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	**PROTECT (PR)**		**PR.IP-3:** Sono attivi processi di controllo della modifica delle configurazioni	1. Sono definite: a.le politiche di sicurezza adottate per l'aggiornamento delle configurazioni dei sistemi [T e di controllo industriale e per il controllo della modifica delle configurazioni in uso rispetto a quelle previste; b.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	**PROTECT (PR)**		**PR.IP-3:** Sono attivi processi di controllo della modifica delle configurazioni	2. E implementata una procedura per la gestione delle eccezioni, incluse emergenze, nel processo di modifica e configurazione			
Critici	**PROTECT (PR)**		**PR.IP-3:** Sono attivi processi di controllo della modifica delle configurazioni	3. Sono definiti e implementati piani di ripristino allo stato precedente (cd. rollback) in caso di errori o problemi di sicurezza.			
Critici	**PROTECT (PR)**		**PR.IP-4:** I backup delle informazioni sono eseguiti, amministrati e verificati	3. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria 1D.AM, almeno: a.le politiche di sicurezza adottate per il backup delle informazioni; b.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	**PROTECT (PR)**		**PR.IP-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	1. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi l'infrastruttura digitale.			
Critici	**PROTECT (PR)**		**PR.IP-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	2. Esiste un documento aggiornato di dettaglio contenente i piani di continuità operativa, nonché quelli di risposta in caso di incidenti, che comprende almeno: a.le politiche e i processi impiegati per identificare le priorità degli eventi; b.le fasi di attuazione dei piani; c.i ruoli e le responsabilità del personale; d.i flussi di comunicazione e reportistica; e.il raccordo con il CSIRT Italia.			
Critici	**PROTECT (PR)**		**PR.IP-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	3. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.			

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Critici	**PROTECT (PR)**		**PR.IP-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	4. 1 piani di business continuity sono collaudati e comunicati alle parti interessate.			
Critici	**PROTECT (PR)**		**PR.IP-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	5. La documentazione di cui al punto 2 è resa disponibile all'Amministrazione e rivista periodicamente.			
Critici	**PROTECT (PR)**		**PR.IP-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	6. L'impatto derivante da interruzioni ed eventuali rischi è determinato al fine di stabilire i criteri per sviluppare strategie e capacità di business continuity.			
Critici	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	7. Esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e le procedure di cui ai punti 1, 2, 3, 4, 5, 6; b. le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e delle credenziali di accesso per gli utenti; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-3:** L'accesso remoto alle risorse è amministrato	5. Esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per la definizione delle attività consentite tramite l'accesso remoto e le misure di sicurezza adottate; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-4:** I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	4. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1.			
Critici	**PROTECT (PR)**	**Awareness and Training (PR.AT):** Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti	**PR.AT-1:** Tutti gli utenti sono informati e addestrati	3. Per ogni membro del personale del soggetto, esiste un registro aggiornato, comprensivo delle istruzioni ricevute.			
Critici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	7. Nel caso di dati e di servizi critici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui alla sezione 2.2.7, PR.DS-1, punto 2. Con riferimento alle infrastrutture impiegate per l'erogazione del servizio cloud, nonché al trattamento dei dati e dei servizi dell'Amministrazione, ivi inclusi i metadati, resta fermo, pertanto, quanto previsto dall'allegato B al Regolamento, requisito SC-SI-PR.DS-1-01.			
Critici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	8. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza			
Critici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	9. Il servizio cloud supporta un meccanismo di cifratura di tipo Bring Your Own Key (BYOK), che consente all'Amministrazione di generare autonomamente, almeno la chiave principale di cifratura (root key), attraverso un HSM ospitato, alternativamente, presso: a. propria infrastruttura b. infrastruttura messa a disposizione dal fornitore all'Amministrazione in modalità dedicata c. infrastruttura di una terza parte scelta dall'Amministrazione.			
Critici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	10. Il soggetto mette a disposizione la funzionalità di importazione sicura delle chiavi di cui al punto 10 nel cloud, per l'esercizio di tutte le operazioni di gestione delle chiavi e della cifratura nel cloud.			
Critici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	11. Sono definite ed implementate procedure e misure tecniche misure per la distruzione delle chiavi memorizzate al di fuori di un ambiente sicuro e revocare le chiavi memorizzate nei moduli di sicurezza hardware (HSM) quando non sono più necessari, in conformità con requisiti legali e normativi.			
Critici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	12. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1.			
Critici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-3:** Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	2. Sono abilitate capacità di geo-localizzazione remota per tutti i dispositivi mobili gestiti [SaaSj			
Critici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.		3. Sono definite ed implementate adeguate tecniche di cancellazione dei dati dell'Amministrazione da remoto [SaaS]			
Critici	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	2. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per lo sviluppo di configurazioni di sistemi [T e il dispiegamento delle sole configurazioni adottate; b. l'elenco delle configurazioni dei sistemi 1T e impiegate e il riferimento alle relative pratiche di riferimento; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. [SaaS]			
Critici	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	3. Sono definiti e documentati requisiti di base per la sicurezza delle diverse applicazioni			
Critici	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	4. Sono definite ed implementate metriche tecniche e operative in linea con i requisiti di sicurezza e gli obblighi di conformità			
Critici	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	5. Esiste un processo di mitigazione e ripristino per la sicurezza delle applicazioni, automatizzando la mitigazione automatizzata delle vulnerabilità quando possibile.			
Critici	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	6. È presente un processo per la convalida della compatibilità del dispositivo con sistemi operativi e applicazioni [PaaS, SaaS]			
Critici	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	7. È presente un sistema di gestione delle variazioni in termini di sistema operativo, patching e/o applicazioni [PaaS, SaaS].			
Critici	**PROTECT (PR)**	**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-2:** Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).	1. Sono implementate linee guida e misure tecniche/organizzative per lo sviluppo sicuro del servizio cloud, in aderenza alle linee guida OWASP in merito alla sicurezza nello sviluppo del software (requisiti, progettazione, implementazione, test e verifica). Devono essere resi disponibili all'Agenzia per la Cybersicurezza Nazionale (ACH) e alla Amministrazione i report sui test OWASP condotti, garantendo l'assenza di vulnerabilità di tipo "high" o "criticai".			
Critici	**PROTECT (PR)**	**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-4:** I backup delle informazioni sono eseguiti, amministrati e verificati	5. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria 1D.AM, almeno: a. le politiche di sicurezza adottate per il backup delle informazioni; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Critici	**PROTECT (PR)**	**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-4:** I backup delle informazioni sono eseguiti, amministrati e verificati	6. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto I.			
Critici	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	6. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi dal servizio cloud e, se previsti, dalle hot replica e/o cold-replica nonché dal sito(i) di disaster recovety,			
Critici	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	7. Esiste un documento aggiornato di dettaglio contenente i piani di disaster recoveiy, nonché quelli di risposta e di recupero in caso di incidenti, che comprende almeno: a. !e politiche e i processi impiegati per identificare le priorità degli eventi; b. le fasi di attuazione dei piani; c. i ruoli e le responsabilità del personale; d. i flussi di comunicazione e reportistica; e. il raccordo con il CS1RT Italia			
Critici	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	8. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.			
Critici	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	9. Le strategie di disaster recovery sono collaudate e comunicate alle parti interessate.			
Critici	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	10. I dispositivi critici per il funzionamento del servizio cloud sono ridondati e, se situati in località diverse, ad una distanza in linea con le migliori pratiche del settore			

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Critici	**PROTECT (PR)**	**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-12:** Viene sviluppato e implementato un piano di gestione delle vulnerabilità	3. Sono definite ed implementate misure tecniche per l'identificazione degli aggiornamenti per le applicazioni che usano librerie di terze parti o open, nel rispetto delle politiche interne di vulnerability management			
Critici	**PROTECT (PR)**	**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.		4. Il documento di cui al punto 1 della misura PR.1P-12 dovrà essere aggiornato su base semestrale.			
Critici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	2. Esiste un documento aggiornato di dettaglio recante i p3rocessi e le politiche di cui al punto 1.			
Critici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	3. Le attività di cui al punto 3 sono volte a verificare anche aspetti di sicurezza.			
Critici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	4. Gli aggiornamenti software sono consentiti solo da fonti pre-autorizzate.			
Critici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	5. Tutti i log relativi alle attività di manutenzione e aggiornamento sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze che svolgono tali attività.			
Critici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	6. Esiste un documento aggiornato che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 3,4 e 5.			
Critici	**PROTECT (PR)**		**PR.PT-5:** Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	1 bis. In relazione ai piani previsti dalla sottocategoria PRA P-9: b. sono adottate architettura ridondate di rete, di connettività, nonché applicative. a. esiste un sito di disaster recovery.			
Critici	**RECOVER (RC)**	**Recovery Planning (RC.RP):** I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.	**RC.RP-1**: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity	1: Esiste un piano di ripristino (recovery pian) e viene eseguito durante o dopo un incidente di cybersecurity			
Critici	**RECOVER (RC)**	**Recovery Planning (RC.RP):** I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.	**RC.RP-1**: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity	2. Il piano di ripristino viene testato, su base semestrale, nell'ambito di due esercitazioni annuali.			
Critici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	1. I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di cui al punto 1 sono ben definiti e resi noti alle articolazioni competenti del soggetto.			
Critici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	2. Sono eseguite periodicamente esercitazioni.			
Critici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	3. Esiste un documento aggiornato di dettaglio che indica almeno: a.le fasi, i processi, i ruoli e le responsabilità di cui ai punti 1 e 2; b.i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilità di cui ai punti 1 e 2; c.le modalità per le esercitazioni di cui al punto 3.			
Critici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-5:** È attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)	1. Sono definiti e mantenuti contatti con gruppi di interesse legati all'infrastruttura digitale e altre entità rilevanti e in linea con il contesto del soggetto in relazione all'infrastruttura digitale.			
Critici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-5:** È attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)	2. Sono definiti e mantenuti punti di contatto con le autorità di regolamentazione applicabili, le forze dell'ordine nazionali e locali e altre autorità giurisdizionali legali.			
Critici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	1. Il piano di risposta prevede l'esecuzione tempestiva della valutazione degli eventi rilevati tramite l'analisi e la correlazione di cui alla categoria DE, nonché la disseminazione immediata degli esiti verso le articolazioni competenti del soggetto, anche ai fini della notifica all'Amministrazione e, su base volontaria al CSIRT Italia, degli incidenti con impatto sull'infrastruttura digitale.			
Critici	**RESPOND (RS)**		**RS.AN-5:** Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)	1.Gli esiti delle valutazioni di cui alla sottocategoria DE.AE-3 e dei penetration test e vulnerability assessment di cui alla sottocategoria DE.CM-8, qualora disponibili, sono diffusi alle articolazioni competenti del soggetto.			
Critici	**RESPOND (RS)**		**RS.AN-5:** Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)	2.1 canali di comunicazione del CSIRT Italia di cui all'articolo 4 del decreto del Presidente del Consiglio dei ministri 8 agosto 2019, dell'Autorità di riferimento del proprio settore produttivo, nonché di eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento sono monitorati.			
Critici	**RESPOND (RS)**		**RS.AN-5:** Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)	3.Esiste un documento aggiornato che descrive, almeno: a.le modalità per ricevere, analizzare e rispondere almeno alle informazioni raccolte tramite le attività di cui ai punti 1 e 2; b.i processi, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2			
Critici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	2. Le politiche e procedure per la gestione tempestiva degli incidenti di sicurezza sono riviste almeno su base annuale.			
Critici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	3. Il piano di risposta e le politiche e procedure di cui ai punti 1 e 2 includono dipartimenti interni critici, l'Amministrazione (se impattata) e tutte le terze parti interessate.			
Critici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	4. I piani di risposta agli incidenti sono collaudati e aggiornati ad intervalli pianificati o in caso di cambiamenti organizzativi o ambientali significativi			
Critici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	5. Sono definite e monitorate le metriche degli incidenti rilevanti in materia di cybersecurity.			
Critici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	6. Sono definiti e implementati processi. procedure e misure di supporto ai processi aziendali per il triage degli eventi legati alla sicurezza.			
Critici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	7. Deve essere implementato un Computer Emergency Response Team (CERT), a coordinamento della fase di risoluzione degli incidenti e in aderenza a quanto definito dalle linee guida ISO/IEC 27035-2. Inoltre, deve essere previsto il coinvolgimento periodico dell'Amministrazione in momenti di condivisione e revisione dello stato degli incidenti di interesse e, ove opportuno, nella risoluzione di tali incidenti, anche secondo gli accordi contrattuali in materia.			
Critici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	4. Esiste un registro aggiornato delle esercitazioni effettuate e dei partecipanti, con le relative lezioni apprese (lessons learned).			
Critici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	5. Sono presenti politiche e procedure per la gestione degli incidenti di sicurezza, E-Discovery e Cloud Forensics, le quali dovranno essere riviste e aggiornate almeno su base annuale.			
Critici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	6. Sono definiti ed implementati processi, procedure e misure tecniche per le notifiche di violazione della sicurezza.			
Critici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	7. È previsto un meccanismo di segnalazione per ogni violazione della sicurezza, reale o presunta, comprese eventuali violazioni inerenti la supply chain, nel rispetto di SLA, leggi e regolamenti applicabili.			
Critici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	8. Le attività di risposta condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione In particolare, le attività di ripristino a seguito di un incidente sono comunicate alle parti interne ed esterne interessate (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT), ivi incluse le articolazioni competenti del soggetto, anche ai fini dell'eventuale interlocuzione con il CSIRT Italia.			
Critici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.MI-3:** Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	1. Le vulnerabilità sono mitigate secondo quanto previsto dal piano di gestione delle vulnerabilità (PR.IP-12), ovvero ne viene documentato e accettato il rischio residuo derivante dalla mancata mitigazione.			
Critici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.MI-3:** Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	2. Sono definite ed implementate procedure e misure tecniche per consentire azioni di risposta (programmate o al sopraggiungere di emergenze) in caso di vulnerabilità identificate, in base al rischio.			
Ordinari	**AFFIDABILITA'**	**Alta affidabilità**	**A.AA-1** Disponibilità dell'infrastruttura	1. L'indice di disponibilità dell'infrastruttura Digitale deve essere stato almeno pari al valore di riferimento corrispondente per il servizio (S L1) 99,98% al netto dei fermi programmati (ovvero pari a 17h, 31m, 53s in un anno solare) 99,6 % comprendendo i fermi programmati (ovvero pari a 1 giorno 11h, 3m, 47s in un anno solare)			
Ordinari	**AFFIDABILITA'**	**Alta affidabilità**	**A.AA-2** Disponibilità di soluzioni per la configurazione dei servizi in alta affidabilità	1. Il Centro di elaborazione dati (CED) deve essere dotato di soluzioni hardware e software (apparati di rete e sicurezza, storage, servizi di virtualizzazione, etc.) per la configurazione dei servizi in alta affidabilità. Devono essere inoltre messe a disposizione capability e funzionalità a supporto di configurazioni dei servizi in alta affidabilità quali: a. Scelta della replica locale dei dati per un servizio storage; b. Presenza di servizi di bilanciamento di carico; c. Meccanismi di anti-affinity per la distribuzione delle istanze computazionali.			
Ordinari	**AFFIDABILITA'**	**Governace e processi**	**A.GP-1**I Servizi IT sono gestiti conformemente agli standard di settore	1. Sono adottati processi e procedure in linea con le best practice indicate dalla ISO/IEC 20000-2			
Ordinari	**AFFIDABILITA'**	**Governace e processi**	**A.GP-2:** È garantito il rispetto degli indicatori di servizio obbligatori	1. Il soggetto deve garantire per i servizi del Centro di elaborazione dati (CED) offerti attività di supporto in conformità con gli obiettivi (SLO) identificati per i corrispondenti indicatori di servizio (SU)			
Ordinari	**AFFIDABILITA'**	**Governace e processi**	**A.GP-2:** È garantito il rispetto degli indicatori di servizio obbligatori	2. Il servizio di supporto deve essere: a. fornito esclusivamente in lingua italiana durante le business hours b. accessibile preferenzialmente tramite i seguenti canali: recapito telefonico ed e-mail.			
Ordinari	**AFFIDABILITA'**	**Performance e scalabiltià**	**A.PS-1:** Sono garantite caratteristiche minime di connettività	1. Il soggetto deve fornire connettività su rete pubblica e rete privata. La rete privata deve consentire al soggetto di fruire di servizi di connettività dedicati e con le seguenti prestazioni minime garantite: bandwidth di base 500 Mbps, con possibilità di incrementare la banda fino a 10 Gbps			
Ordinari	CAPACITA' ELEBORATIVA	**Capacità elaborativa**	**CECE-0I:** Gestione della capacità di elaborazione conformemente agli standard o le best practice di settore	1. La capacità elaborativa dell'Infrastruttura Digitale è gestita attraverso un processo formale aderente alle best practice sul capacity management 1T1 L o alle linee guida presenti alla I SO/IEC 20000-2			
Ordinari	DATA CENTER SECURITY	**Data Center security**	**S.DC-01: I** Centri di elaborazione dati (CED) rispettano livelli minimi di sicurezza fisica e infrastrutturale	1.Il soggetto garantisce il presidio operativo del Data Center 24/7/365.			
Ordinari	DATA CENTER SECURITY	**Data Center security**	**S.DC-01: I** Centri di elaborazione dati (CED) rispettano livelli minimi di sicurezza fisica e infrastrutturale	2.Il Data Center è stato progettato e realizzato secondo standard di riferimento infrastrutturali, ad esempio ANSI/BICSI 002, TIA−942, EN 50600, Uptime Institute Tier Certification o analoghi.			
Ordinari	DATA CENTER SECURITY	**Data Center security**	**S.DC-01: I** Centri di elaborazione dati (CED) rispettano livelli minimi di sicurezza fisica e infrastrutturale	3.Nei locali ospitanti i Data Center sono presenti pavimenti flottanti qualora la distribuzione dell'alimentazione elettrica e del cablaggio non avvenga per via aerea			
Ordinari	DATA CENTER SECURITY	**Data Center security**	**S.DC-01: I** Centri di elaborazione dati (CED) rispettano livelli minimi di sicurezza fisica e infrastrutturale	4.Il soggetto garantisce le caratteristiche antincendio del Data Center in conformità alle norme antincendio vigenti.			
Ordinari	DATA CENTER SECURITY	**Data Center security**	**S.DC-01: I** Centri di elaborazione dati (CED) rispettano livelli minimi di sicurezza fisica e infrastrutturale	5.Il soggetto garantisce che tutti i server dei Data Center sono connessi ad apparati per la continuità elettrica (UPS).			
Ordinari	DATA CENTER SECURITY	**Data Center security**	**S.DC-02:** Sono adottate misure di sicurezza fisica e ambientale	1.Esiste un documento di dettaglio che definisce politiche e procedure inerenti allo spostamento sicuro di supporti fisici. Queste policy e procedure dovranno essere riviste su base almeno annuale.			
Ordinari	DATA CENTER SECURITY	**Data Center security**	**S.DC-02:** Sono adottate misure di sicurezza fisica e ambientale	2.Sono implementati, manutenuti e adottati sistemi di sorveglianza all'esterno dei data center e in tutti i punti di ingresso e uscita al fine di rilevare ogni tentativo di ingresso non autorizzato.			
Ordinari	DATA CENTER SECURITY	**Data Center security**	**S.DC-02:** Sono adottate misure di sicurezza fisica e ambientale	3.Sono implementati, mantenuti e adottati, all'interno dei Data Center. i sistemi di controllo ambientale al fine di monitorare e testare l'adeguatezza delle temperature e le condizioni di umidità all'interno dell'area, nel rispetto dei principali standard di settore.			
Ordinari	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	1.Sono presenti sistemi di rilevamento delle intrusioni (Intrusion Detection Systems - IDS).			
Ordinari	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	2.Sono presenti dei processi per il monitoraggio degli eventi relativi alla sicurezza delle applicazioni e dell'infrastruttura sottostante			
Ordinari	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	1.Sono implementati ed utilizzati appositi strumenti per la prevenzione e il rilevamento di malware, nonché sistemi di protezione delle postazioni terminali (Endpoint Protection Systems - EPS)			

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Ordinari	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	2.Sono presenti politiche di protezione anti-malware, le quali dovranno essere riviste almeno su base annuale.			
Ordinari	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-8:** Vengono svolte scansioni per l'identificazione di vulnerabilità	1.In base all'analisi del rischio, sulle piattaforme e sulle applicazioni software ritenute critiche sono eseguiti penetration test e vulnerability assessment, prima della loro messa in esercizio.			
Ordinari	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-8:** Vengono svolte scansioni per l'identificazione di vulnerabilità	2.Sono eseguiti periodicamente penetration test e vulnerability assessment in relazione alla criticità delle piattaforme e delle applicazioni software.			
Ordinari	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-8:** Vengono svolte scansioni per l'identificazione di vulnerabilità	3.Esiste un documento aggiornato recante la tipologia di penetration test e vulnerability assessment previsti.			
Ordinari	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-8:** Vengono svolte scansioni per l'identificazione di vulnerabilità	4.Esiste un registro aggiornato dei penetration test e vulnerability assessment eseguiti corredato dalla relativa documentazione.			
Ordinari	DETECT (DE)		**DE.AE-3:** Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	1. Ai fini di rilevare tempestivamente incidenti con impatto sul servizio cloud, sono adottati gli strumenti tecnici e procedurali per: a. acquisire le informazioni da più sensori e sorgenti; b. ricevere e raccogliere informazioni inerenti alla sicurezza del servizio cloud rese note dal CS1RT Italia, da fonti interne o esterne al soggetto; c. analizzare e correlare, anche in maniera automatizzata, i dati e le informazioni di cui alle lettere a) e b), per rilevare tempestivamente eventi di interesse.			
Ordinari	DETECT (DE)		**DE.AE-3:** Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	2. Le attività di analisi e correlazione di cui al punto precedente sono monitorate e registrate. La relativa documentazione, anche elettronica, é conservata per almeno 24 mesi.			
Ordinari	DETECT (DE)		**DE.AE-3:** Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	3. Sono definite: a. le politiche applicate per individuare i sensori e le sorgenti di cui al punto 1, lettera a); b. le procedure e gli strumenti tecnici per ottenere le informazioni di cui al punto 1, lettere a) e b); c. le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui ai punto 1, lettera c); d. i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al punto 2.			
Ordinari	DETECT (DE)		**DE.AE-3:** Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	4. Sono presenti politiche e procedure di logging, monitoraggio, sicurezza e conservazione di registri di accesso, le quali dovranno essere aggiornate almeno su base annuale.			
Ordinari	DETECT (DE)		**DE.AE-3:** Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	5. È adottato un sistema di auditing per il rilevamento di informazioni inerenti alla sicurezza, il monitoraggio degli accessi, modifiche o cancellazioni non autorizzate di dati o metadati			
Ordinari	DETECT (DE)		**DE.AE-3:** Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	6. Sono definiti e valutati processi, procedure e misure tecniche per la segnalazione di anomalie e guasti del sistema di monitoraggio e in grado di fornire una notifica immediata al soggetto responsabile.			
Ordinari	DETECT (DE)		**DE.AE-3:** Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	7. Nell'ambito delle attività di logging e monitoraggio, in relazione al servizio cloud sono forniti strumenti di gestione degli errori e logging che consentono all'Amministrazione di definire il periodo di custodia (retention) desiderato e di ottenere informazioni sullo stato di sicurezza del servizio cloud, nonché sui dati e le funzioni che fornisce. Le informazioni devono essere sufficientemente dettagliate da consentire la verifica dei seguenti aspetti, nella misura in cui sono applicabili al servizio cloud: a. Quali dati, servizi o funzioni disponibili per l'utente all'interno del servizio cloud sono stati consultati da chi e quando (Audit Logs); b. Malfunzionamenti durante l'elaborazione di azioni automatiche o manuali.			
Ordinari	DETECT (DE)		**DE.AE-3:** Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	8. Per il servizio oggetto di qualificazione deve essere garantita la possibilità di integrare i log nel sistema SIEM di gestione e monitoraggio dell'Amministrazione e che i file di log siano facilmente esportabili dall'Amministrazione, preferibilmente tramite API.			
Ordinari	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	1. Sono presenti sistemi di rilevamento delle intrusioni (Intrusion Detection Systems - 1DS).			
Ordinari	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	2. Sono presenti dei processi per il monitoraggio degli eventi relativi alla sicurezza delle applicazioni e dell'infrastruttura sottostante.			
Ordinari	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	3. È previsto un sistema di monitoraggio dei degli accessi al fine di rilevare attività sospette e stabilire un processo definito per l'adozione di azioni appropriate e tempestive in risposta alle anomalie rilevate			
Ordinari	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	1. Sono implementati ed utilizzati appositi strumenti per la prevenzione e il rilevamento di malware, nonché sistemi di protezione delle postazioni terminali (Endpoint Protection Systems - EPS).			
Ordinari	DETECT (DE)	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	2. Sono presenti politiche di protezione anti-malware, le quali dovranno essere riviste almeno su base annuale.			
Ordinari	DETECT (DE)	**Detection Processes (DE.DP):** Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	**DE.DP-1:** Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	1. Le nomine di cui alla sottocategoria 1D.AM-6 sono rese note all'interno del soggetto.			
Ordinari	DETECT (DE)	**Detection Processes (DE.DP):** Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	**DE.DP-1:** Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	2. I ruoli, i processi e le responsabilità per !e attività propedeutiche al rilevamento di incidenti con impatto sul servizio cloud sono ben definiti e resi noti alle articolazioni competenti del soggetto.			
Ordinari	DETECT (DE)	**Detection Processes (DE.DP):** Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	**DE.DP-1:** Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	3. Esiste un documento aggiornato di dettaglio che indica almeno: a. i ruoli, i processi e le responsabilità di cui al punto 2; b. i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti i e 2.			
Ordinari	DETECT (DE)	**Detection Processes (DE.DP):** Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	**DE.DP-1:** Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	4. E definito ed implementato un sistema per la notifica all'Amministrazione degli eventi anomali che coinvolgono le applicazioni e l'infrastruttura sottostante, identificati sulla base di metriche previamente concordate (PaaS, SaaS).			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	2. Tutti i sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete è consentito esclusivamente a quelli approvati.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-3:** I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	1. Tutti i flussi informativi, inclusi quelli verso l'esterno e relativi all'Infrastruttura digitale, sono identificati e approvati da attori interni al soggetto.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	1. È definita e resa nota alle articolazioni competenti del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	2. È nominato, nell'ambito dell'articolazione di cui al punto 1, un incaricato, e un eventuale sostituto, con il compito di gestire l'attuazione delle disposizioni del Regolamento in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico del soggetto ed assicura l'efficace implementazione delle misure di sicurezza previste			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	3.Sono nominati, nell'ambito dell'articolazione di cui al punto 1, un referente tecnico, e almeno un suo sostituto, in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, per lo svolgimento delle funzioni di interlocuzione con il CSIRT Italia ai fini della gestione degli incidenti aventi impatto sull'infrastruttura.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti,	4.L'incaricato di cui al punto 2 e il referente tecnico di cui al punto 3 operano in stretto			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	4.L'incaricato di cui al punto 2 e il referente tecnico di cui al punto 3 operano in stretto raccordo.			
Ordinari	**IDENTIFY (ID)**	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È indetificata e resa nota una policy di cybersecurity	1. Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di cybersecurity			
Ordinari	**IDENTIFY (ID)**	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-1:** Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	1. Esiste un piano aggiornato di verifica e test di sicurezza che descrive l'insieme delle attività finalizzate alla valutazione del livello di sicurezza cibernetica dell'Infrastruttura digitale e dell'efficacia delle misure di sicurezza tecniche e procedurali che contiene, inoltre, la periodicità e le modalità di esecuzione.			
Ordinari	**IDENTIFY (ID)**	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-1:** Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	2. Esistono procedure, da aggiornare almeno su base annuale, per !a gestione dei rischi associati a variazioni nell'ambito di asset organizzativi, ivi incluse applicazioni, sistemi, infrastrutture, configurazioni, ecc., indipendentemente dal fatto che gli asset siano gestiti internamente o esternamente (cioè in outsourcing).			
Ordinari	**IDENTIFY (ID)**	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-5:** Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	1. L'analisi del rischio è svolta in funzione delle minacce, delle vulnerabilità, delle relative probabilità di accadimento e dei conseguenti impatti derivanti dal loro sfruttamento alla luce delle minacce considerate.			
Ordinari	**IDENTIFY (ID)**	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-5:** Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	2. L'analisi del rischio tiene conto delle dipendenze interne ed esterne dell'Infrastruttura digitale.			
Ordinari	**IDENTIFY (ID)**	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-5:** Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	3. Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	2. Tutti i sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete è consentito esclusivamente a quelli approvati.			

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-2:** Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	1. Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-2:** Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	2. L'installazione delle piattaforme e delle applicazioni software è consentito esclusivamente per quelle approvate.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-2:** Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	3. Esistono politiche che limitino l'aggiunta, rimozione o aggiornamento, nonché la gestione non autorizzata degli asset dell'organizzazione.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-3:** I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	1. Tutti i flussi informativi, inclusi quelli verso l'esterno e relativi al servizio cloud, sono identificati e approvati da attori interni al soggetto.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	1. È definita e resa nota alle articolazioni competenti del soggetto l'organizzazione di cybersecurity, anche con riferimento at ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	2. È nominato, nell'ambito dell'articolazione di cui al punto 1, un incaricato, e un eventuale sostituto, con il compito di gestire l'attuazione delle disposizioni del Regolamento in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico del soggetto ed assicura l'efficace implementazione delle misure di sicurezza di cui al presente Allegato.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	3. Sono nominati, nell'ambito dell'articolazione di cui al punto 1, un referente tecnico, e almeno un suo sostituto, in possesso di competenze tecnico. specialistiche nella materia della sicurezza cibernetica, per lo svolgimento delle funzioni di interlocuzione con il CSIRT Italia ai fini della gestione degli incidenti aventi impatto sul servizio cloud.			
Ordinari	**IDENTIFY (ID)**	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	4. L'incaricato di cui al punto 2 e il referente tecnico di cui al punto 3 operano in stretto raccordo.			
Ordinari	**IDENTIFY (ID)**	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È indetificata e resa nota una policy di cybersecurity	1. Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di cybersecurity.			
Ordinari	**IDENTIFY (ID)**	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È indetificata e resa nota una policy di cybersecurity	2. il Documento di cui al punto 1 deve essere approvato dal soggetto e aggiornato almeno su base annuale o in corrispondenza di sostanziali variazioni all'interno dell'organizzazione.			
Ordinari	**IDENTIFY (ID)**	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-4:** La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity	1. Il documento aggiornato che descrive i processi di gestione del rischio include la parte relativa ai rischi legati alla cybersecurity.			
Ordinari	**IDENTIFY (ID)**	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-4:** La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity	2. Esiste un programma forniate di Enterprise Risk Management (ERM) che include politiche e procedure per l'identificazione, la valutazione, la proprietà, il trattamento e l'accettazione dei rischi di sicurezza e privacy del cloud.			
Ordinari	**IDENTIFY (ID)**	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-1:** Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	1. Esiste un piano aggiornato di verifica e test di sicurezza che descrive l'insieme delle attività finalizzate alla valutazione del livello di sicurezza cibernetica del servizio cloud e dell'efficacia delle misure di sicurezza tecniche e procedurali e che contiene, inoltre, la periodicità e le modalità di esecuzione.			
Ordinari	**IDENTIFY (ID)**	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-1:** Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	2. Esistono procedure, da aggiornare almeno su base annuale, per la gestione dei rischi associati a variazioni nell'ambito di asset organizzativi, ivi incluse applicazioni, sistemi, infrastrutture, configurazioni, ecc., indipendentemente dal fatto che gli asset siano gestiti internamente o esternamente (cioè in outsourcing).			
Ordinari	**IDENTIFY (ID)**	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-5:** Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	1. L'analisi del rischio è svolta in funzione delle minacce, delle vulnerabilità, delle relative probabilità di accadimento e dei conseguenti impatti derivanti dal loro sfruttamento alla luce delle minacce considerate.			
Ordinari	**IDENTIFY (ID)**	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-5:** Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	2. L'analisi del rischio tiene conto delle dipendenze interne ed esterne del servizio cloud.			
Ordinari	**IDENTIFY (ID)**	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-5:** Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	3. Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.			
Ordinari	**IDENTIFY (ID)**	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	1. Sono definiti i processi di gestione del rischio inerente la catena di approvvigionamento cyber.			
Ordinari	**IDENTIFY (ID)**	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	2. Tali processi sono validati e approvati da parte dei vertici del soggetto.			
Ordinari	**INTEROPERABILITA' E PORTATILITA'**	GESTIONE REMOTA	**IP.GR-1:** Sono disponibili API per la gestione remota del ciclo di vita del servizio	1. L'ambiente del servizio cloud deve essere accessibile tramite delle interfacce API per la gestione remota dei servizi, assicurando che le API esposte consentano l'implementazione di strumenti per la gestione automatica e remota del ciclo di vita del servizio cloud.			
Ordinari	**INTEROPERABILITA' E PORTATILITA'**	GESTIONE REMOTA	**IP.GR-1:** Sono disponibili API per la gestione remota del ciclo di vita del servizio	2. È disponibile una documentazione tecnica, fruibile dall'Amministrazione, in merito alle API esposte e gli endpoint SOAP e/o REST.			
Ordinari	**INTEROPERABILITA' E PORTATILITA'**	INTEROPERABILITA'	**IP.IN-1:** Sono disponibili API per funzionalità applicative	1.11 servizio SaaS espone opportune API di tipo SOAP e/o REST verso l'Amministrazione associate alle funzionalità applicative, prevedendo in particolare la tracciabilità delle versioni disponibili e la tracciabilità delle richieste ricevute ed evase. Inoltre, è disponibile documentazione tecnica, fruibile dall'Amministrazione, in merito alle API esposte e gli endpoint. [SaaS]			
Ordinari	**INTEROPERABILITA' E PORTATILITA'**	PORTABILITA'	**IP.PO-1:** Sono disponibili funzionalità/API per import/export dei dati	1. Sono disponibili funzionalità e/o API per consentire l'esportazione ed importazione massiva dei dati, garantendo l'utilizzo di formati aperti non proprietari.			
Ordinari	**INTEROPERABILITA' E PORTATILITA'**	PORTABILITA'	**IP.PO-2:** L'interoperabilità e la portabilità dei dati sono gestite mediante procedure e politiche regolarmente aggiornate. La portabilità dei dati prevede l'applicazione di protocolli di rete sicuri e l'accesso ai dati al termine dei rapporti contrattuali è gestito mediante accordi specifici.	1. Sono definite politiche e procedure per l'interoperabilità e la portabilità, le quali vengono riviste e aggiornate almeno su base annuale, compresi requisiti per: a. Comunicazioni tra le interfacce delle applicazioni; b. Interoperabilità del trattamento delle informazioni; c. Portabilità dello sviluppo di applicazioni; d. Scambio, uso, portabilità, integrità e persistenza delle informazioni/dati. [PaaS, SaaS]			
Ordinari	**INTEROPERABILITA' E PORTATILITA'**	PORTABILITA'	**IP.PO-2:** L'interoperabilità e la portabilità dei dati sono gestite mediante procedure e politiche regolarmente aggiornate. La portabilità dei dati prevede l'applicazione di protocolli di rete sicuri e l'accesso ai dati al termine dei rapporti contrattuali è gestito mediante accordi specifici.	2. Sono implementati protocolli di rete cifrati e standardizzati per la gestione, l'importazione e l'esportazione dei dati. [PaaS, SaaS]			
Ordinari	**INTEROPERABILITA' E PORTATILITA'**	PORTABILITA'	**IP.PO-2:** L'interoperabilità e la portabilità dei dati sono gestite mediante procedure e politiche regolarmente aggiornate. La portabilità dei dati prevede l'applicazione di protocolli di rete sicuri e l'accesso ai dati al termine dei rapporti contrattuali è gestito mediante accordi specifici.	3. Sono incluse, all'interno degli accordi disposizioni che specifichino l'accesso dell'Amministrazione ai dati al termine del contratto, inclusi: a. Formato dei dati; b. Durata del tempo in cui i dati saranno conservati; c. Portata dei dati conservati e messi a disposizione dell'Amministrazione; d. Politica di cancellazione dei dati. [PaaS, SaaS]			
Ordinari	**PERFORMANCE E SCALABILITA'**		**PS.CA-1:** Il servizio cloud presenta le caratteristiche tipiche ed è conforme agli standard di settore	1. Il servizio cloud garantisce almeno le seguenti caratteristiche, come da indicazioni NIST SP 800-145: a. self-service provisioning: il servizio cloud provvede unilateralmente alla fornitura delle risorse informatiche (ad esempio,. server e storage in cloud), secondo necessità e in modo automatico, senza ricorrere ad interazione umana. il servizio cloud soddisfa unilateralmente le richieste dell'Amministrazione di risorse computazionali (o informatiche), senza esplicita verifica o approvazione. b. accesso alla rete: il servizio cloud offre opzioni multiple di connettività alla rete; di cui almeno una basata su rete pubblica (es., Internet). c. elasticità: il soggetto implementa meccanismi automatici di provisioning e de-provisioning del servizio,. salvo documentate limitazioni tecniche, offrendo opportuni strumenti all'Amministrazione.			
Ordinari	**PERFORMANCE E SCALABILITA'**		**PS.SC.1:** Trasparenza sulle modalità e meccanismi di scalabilità	1.11 soggetto comunica all'Amministrazione: a. il meccanismo di scalabilità offerto (es. automatico e configurabile, nativo, manuale); b. la tipologia (orizzontale e/o verticale); c. le condizioni massime di carico sopportabili dal servizio (es. numero di utenti concorrenti e/o volume di richieste processabili); d. le modalità di configurazione (es. sulla base di metriche di monitoraggio, pianificato nel tempo); e. i tempi minimi di reazione del servizio alla richiesta di nuove risorse (es, attivazione di nuove risorse).			
Ordinari	**PROTECT (PR)**	**Awareness and Training (PR.AT):** Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti	**PR.AT-1:** Tutti gli utenti sono informati e addestrati	1.Esiste un documento aggiornato di dettaglio che indica i contenuti dell'addestramento e della formazione fornita al personal del soggetto e le modalità di verifica dell'acquisizione dei contenuti.			
Ordinari	**PROTECT (PR)**	**Awareness and Training (PR.AT):** Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti	**PR.AT-1:** Tutti gli utenti sono informati e addestrati	2.L'addestramento e la formazione di cui al punto 1 fornita agli utenti del soggetto, in relazione ai ruoli, prevede, almeno, le seguenti tematiche: a.la tutela della confidenzialità di dati in chiaro o cifrati; b.la restituzione dei beni di natura aziendale al termine del rapporto di lavoro; d.la definizione di ruoli e delle responsabilità; e.politiche di accesso a sistemi, asset e risorse; f.politiche di gestione delle informazioni e della sicurezza; g.processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi; h.requisiti per la non divulgazione/confidenzialità di informazioni.			
Ordinari	**PROTECT (PR)**	**Awareness and Training (PR.AT):** Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le	**PR.AT-2:** Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità	1. Sono definiti i contenuti dell'istruzione fornita al personale del soggetto con privilegi e le modalità di verifica dell'acquisizione dei contenuti.			
Ordinari	**PROTECT (PR)**	**Awareness and Training (PR.AT):** Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le	**PR.AT-2:** Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità	2. Sono definiti, per ogni membro del personale del soggetto, i privilegi e le istruzioni ricevute.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	1.Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno: a.le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati; b.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	2. Con riferimento alle infrastrutture, al trattamento dei dati e dei servizi dell'Amministrazione, resta fermo quanto previsto dall'allegato A al Regolamento, requisito IN-SA-PR.DS-1-01.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	3. Con riferimento all'accesso ai dati da parte di entità extra-UE, il soggetto: a.segnala all'Agenzia per la Cybersicurezza Nazionale (ACN) e all'Amministrazione ogni richiesta di accesso a dati o metadati da parte di entità extra-UE; b.fornisce accesso a dati dell'Amministrazione o metadati ad entità extra-UE solo a valle di un'autorizzazione esplicita da parte dell'Amministrazione.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-5:** Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	1. Sono definite in relazione alla categoria ID.AM, almeno: a.le politiche di sicurezza adottate per l'accesso ai dati; b.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza			

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-6:** Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni	1. Sono definite in relazione alla categoria ID.AM, almeno: a.l'elenco dei meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni; b.le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi è applicato a quale risorsa; c.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.		2. Sono adottate politiche di Data Loss Prevention coerentemente con la valutazione dei rischi			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	1. Le credenziali di accesso sono individuali per il personale del soggetto e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	2. Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1, le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	3. Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	4. Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es., trasferimento di personale).			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	5. Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	6. Esiste una pianificazione aggiornata degli audit di sicurezza delle identità digitali previsti e un registro degli audit effettuati con la relativa documentazione.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	6.Esiste una pianificazione aggiornata degli audit di sicurezza delle identità digitali previsti e un registro degli audit effettuati con la relativa documentazione.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-2:** L'accesso fisico alle risorse è protetto e amministrato	1. Con riferimento ai censimenti della sottocategoria ID.AM-1, esiste un documento aggiornato di dettaglio contenente almeno: a.le politiche di sicurezza adottate per la protezione e l'amministrazione degli accessi fisici; b.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-2:** L'accesso fisico alle risorse è protetto e amministrato	2. È definito un perimetro di sicurezza fisico al fine di salvaguardare il personale, i dati e i sistemi informativi.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-3:** L'accesso remoto alle risorse è amministrato	1.Gli accessi da remoto effettuati sono monitorati da parte dell'organizzazione di cybersecurity.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate		2.Fatti salvi documentati limiti tecnici, sono implementate adeguate misure di controllo dell'accesso, adottando sistemi di autenticazione, autorizzazione e registrazione/contabilizzazione centralizzati degli accessi, coadiuvati da sistemi di autenticazione, la cui sicurezza è proporzionale al rischio.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-3:** L'accesso remoto alle risorse è amministrato	3.È definito e implementato un modello di gestione degli accessi centralizzato volto ai processi di autorizzazione, logging e comunicazione degli accessi alle risorse e ai dati dell'Amministrazione.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-3:** L'accesso remoto alle risorse è amministrato	4.Esiste un log degli accessi eseguiti da remoto.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-4:** I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	1. Sono definite, con riferimento ai censimenti di cui alla categoria ID.AM, almeno: a.le risorse censite a cui è necessario accedere, per quali funzioni e con quali autorizzazioni; b.i gruppi di utenti e i loro privilegi in relazione alle risorse a cui possono accedere e con quali autorizzazioni; c.l'assegnazione degli utenti censiti a gruppi di utenti.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-4:** I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	2. Nell'ambito di implementazione dell'accesso al sistema informativo, vengono osservati principi di separazione delle funzioni e del privilegio minimo in relazione al rischio organizzativo			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-4:** I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	3. Sono definite e implementate politiche e procedure, misure tecniche per la segregazione dei ruoli di accesso privilegiato in modo che l'accesso amministrativo ai dati, le capacità di crittografia e gestione delle chiavi e le capacità di registrazione siano distinte e separate.			
Ordinari	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	1. Sono definite politiche e procedure con riferimento alla sicurezza delle applicazioni per fornire un adeguato supporto alla pianificazione, realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni, le quali dovranno essere riviste e aggiornate almeno su base annuale			
Ordinari	**PROTECT (PR)**	**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-12:** Viene sviluppato e implementato un piano di gestione delle vulnerabilità	1. Esiste un documento aggiornato di dettaglio che indica almeno: a.le politiche di sicurezza adottate per gestire le vulnerabilità; b.i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Ordinari	**PROTECT (PR)**	**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-12:** Viene sviluppato e implementato un piano di gestione delle vulnerabilità	2. Sono definite ed implementate procedure e misure tecniche volte all'aggiornamento degli strumenti di rilevamento, delle threat signatures e degli indicatori di compromissione, le quali dovranno essere riviste e aggiornate frequentemente o su base settimanale			
Ordinari	**PROTECT (PR)**	**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-4:** I backup delle informazioni sono eseguiti, amministrati e verificati	1.Viene effettuato periodicamente un backup dei dati memorizzati. Viene assicurata la riservatezza, l'integrità e ia disponibilità dei dati dei backup.			
Ordinari	**PROTECT (PR)**	**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-4:** I backup delle informazioni sono eseguiti, amministrati e verificati	2.Viene verificato periodicamente il ripristino (test di restare) delle copie di backup come da obiettivo (SLO) identificato per il corrispondente indicatore di servizio (SLI) riportato alla Tabella 1 "Indicatori minimi della qualità del Servizio"			
Ordinari	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti	**PR.MA-2:** La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	1.La manutenzione delle risorse e dei sistemi (ivi incluse le attività relative alle funzioni di sicurezza) svolta da remoto è eseguita nel rispetto delle misure di cui alla sottocategoria PR.AC-3 e dei seguenti punti.			
Ordinari	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti	**PR.MA-2:** La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	2.Tutti gli accessi eseguiti da remoto da personale di terze parti sono autorizzati dall'organizzazione di cybersecurity e limitati ai soli casi essenziali			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	1. Le credenziali di accesso sono individuali per il personale del soggetto e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	2. Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1, le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	3. Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	4. Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es., trasferimento di personale).			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	5. Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-1:** Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	6. Esiste una pianificazione aggiornata degli audit di sicurezza delle identità digitali previsti e un registro degli audit effettuati con la relativa documentazione.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-3:** L'accesso remoto alle risorse è amministrato	1. Gli accessi da remoto effettuati sono monitorati da parte dell'organizzazione di cybersecurity.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-3:** L'accesso remoto alle risorse è amministrato	2. Fatti salvi documentati limiti tecnici, sono implementate adeguate misure di controllo dell'accesso, adottando sistemi di autenticazione, autorizzazione e registrazione/contabilizzazione centralizzata degli accessi, coadiuvati da sistemi di autenticazione, la cui sicurezza è proporzionale al rischio.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-3:** L'accesso remoto alle risorse è amministrato	3. È definito e implementato un modello di gestione degli accessi centralizzato volto ai processi di autorizzazione, logging e comunicazione degli accessi alle risorse e ai dati dell'Amministrazione.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-3:** L'accesso remoto alle risorse è amministrato	4. Esiste un log degli accessi eseguiti da remoto.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-4:** I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	1. Sono definite, con riferimento ai censimenti di cui alla categoria ID.AM, almeno: a. le risorse censite a cui è necessario accedere, con riferimento alla categoria ID.AM, per quali funzioni e con quali autorizzazioni; b. i gruppi di utenti e i loro privilegi in relazione alle risorse a cui possono accedere e con quali autorizzazioni; c. l'assegnazione degli utenti censiti a gruppi di utenti.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-4:** I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	2. Nell'ambito di implementazione dell'accesso al sistema informativo, vengono osservati principi di separazione delle funzioni e del privilegio minimo in relazione al rischio organizzativo.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-4:** I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	3. Sono definite e implementate politiche, procedure e misure tecniche per la segregazione dei ruoli di accesso privilegiato in modo che l'accesso amministrativo ai dati, le capacità di crittografia e gestione delle chiavi e le capacità di registrazione siano distinte e separate.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-5:** L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	1. Sono presenti politiche e procedure per la sicurezza dell'infrastruttura di rete, le quali dovranno essere aggiornate almeno su base annuale.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-5:** L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	2. È presente una pianificazione per il monitoraggio della disponibilità, qualità e l'adeguata capacità delle risorse al fine di fornire le prestazioni di sistema richieste			

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-7:** Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)	1. Sono definite e implementate politiche e procedure per l'accesso ai sistemi, alle applicazioni e ai dati, compresa l'autenticazione multifattoriale almeno per gli utenti privilegiati e l'accesso a dati.			
Ordinari	**PROTECT (PR)**	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-7:** Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)	2. In relazione al servizio cloud, deve essere garantita all'Amministrazione la funzionalità di autenticazione a più fattori o l'uso di soluzioni di autenticazione a più fattori di terze parti. Devono essere rese disponibili informazioni trasparenti in merito alle funzionalità di autenticazione a più fattori accessibili all'Agenzia per la Cybersicurezza Nazionale (ACN) e all'Amministrazione, con specifiche sui meccanismi adoperati per l'autenticazione (es. e-mail, sms o check biometrico).			
Ordinari	**PROTECT (PR)**	**Awareness and Training (PR.AT):** Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti	**PR.AT-1:** Tutti gli utenti sono informati e addestrati	1. Esiste un documento aggiornato di dettaglio che indica i contenuti dell'addestramento e della formazione fornita al personale del soggetto e le modalità di verifica dell'acquisizione dei contenuti.			
Ordinari	**PROTECT (PR)**	**Awareness and Training (PR.AT):** Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti	**PR.AT-1:** Tutti gli utenti sono informati e addestrati	2. L'addestramento e la formazione di cui al punto 1 fornita agli utenti del soggetto, in relazione ai ruoli, prevede, almeno, le seguenti tematiche: a. la tutela della confidenzialità di dati in chiaro o cifrati. b. la restituzione dei beni di natura aziendale al termine del rapporto di lavoro d. la definizione di ruoli e delle responsabilità e. politiche di accesso a sistemi, asset e risorse E politiche di gestione delle informazioni e della sicurezza g. processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi h. requisiti per la non divulgazione/confidenzialità di informazioni			
Ordinari	**PROTECT (PR)**	**Awareness and Training (PR.AT):** Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti	**PR.AT-2:** Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità	1. Sono definiti i contenuti dell'istruzione fornita al personale del soggetto con privilegi e le modalità di verifica dell'acquisizione dei contenuti.			
Ordinari	**PROTECT (PR)**	**Awareness and Training (PR.AT):** Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti	**PR.AT-2:** Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità	2. Sono definiti, per ogni membro del personale del soggetto, i privilegi e le istruzioni ricevute.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	1.Sono definite, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	2. Con riferimento alle infrastrutture impiegate per l'erogazione dei servizio cloud al trattamento dei dati e dei servizi dell'Amministrazione, fermo restando quanto previsto dall'allegato B al Regolamento, requisito SC-SI-PR.DS-1-01, qualora sussistano motivate e documentate limitazioni di carattere tecnico, eventuali metadati necessari per l'erogazione del servizio cloud possono essere trattati mediante l'impiego di infrastrutture fisiche e tecnologiche localizzate al di fuori del territorio dell'Unione europea. In tal caso, i citati metadati non possono contenere, anche in parte, i dati dell'Amministrazione.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	3. Con riferimento all'accesso ai dati da parte di entità extra-UE, il soggetto: a. segnala all'Agenzia per la Cybersicurezza Nazionale (ACN) e all'Amministrazione ogni richiesta di accesso a dati o metadati da parte di entità extra-UE; b. fornisce accesso a dati dell'Amministrazione o metadati ad entità extra-UE solo a valle di un'autorizzazione esplicita da parte dell'Amministrazione.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	4. Il soggetto garantisce autonomia all'Amministrazione nella gestione delle proprie chiavi crittografiche e, in particolare: a. Esiste un documento aggiornato di dettaglio inerente alle procedure di crittografia, alla cifratura e alla gestione delle chiavi, le quali dovranno essere aggiornate almeno su base annuale, e recante un'indicazione puntuale di ruoli e responsabilità: b. È prevista una verifica periodica di sistemi, politiche e processi di crittografia e gestione delle chiavi in risposta all'aumento dell'esposizione al rischio, valutato mediante audit da eseguire con cadenza almeno annuale o dopo qualsiasi evento di sicurezza. c. È prevista la generazione di chiavi crittografiche mediante l'utilizzo di librerie crittografiche, con un'indicazione in merito all'algoritmo e al generatore di numeri casuali utilizzati. d. è prevista la generazione di chiavi crittografiche segrete e private per uno scopo unico. e. Sono previsti meccanismi di rotazione delle chiavi crittografiche secondo il periodo di validità delle stesse, tenendo conto di possibili rischi e requisiti normativi e legali.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	5. Sono presenti processi, procedure e misure tecniche per revocare e rimuovere le chiavi crittografiche prima della fine del loro periodo di validità, quando una chiave è compromessa, o un'entità non fa più parte dell'organizzazione, conformemente a requisiti legali e normativi.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	6. Sono definiti e implementati processi, procedure e misure per la creazione, disattivazione di chiavi al momento della scadenza, eventuali sospensioni e meccanismi di gestione per le chiavi d'accesso a repository			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-2:** I dati sono protetti durante la trasmissione	1. Sono utilizzati canali di comunicazione sicuri e criptati durante la migrazione di server, servizi, applicazioni o dati in ambienti cloud. Tali canali devono includere solo protocolli aggiornati e approvati.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-3:** Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	1. Sono definite in relazione alla categoria 1D.AM: a. le politiche di sicurezza adottate per il trasferimento fisico, la rimozione e la distruzione di dispositivi atti alla memorizzazione di dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-5:** Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	1. Sono definite in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per l'accesso ai dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-5:** Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	2. Sono adottate politiche di Data Loss Prevention coerentemente con la valutazione dei rischi.			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-6:** Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni	1. Sono definiti in relazione alla categoria 1D.AM, almeno: a. l'elenco dei meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni; b. le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi è applicato a quale risorsa;			
Ordinari	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-7:** Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	1. Sono definite in relazione alla categoria 1D.AM: a. l'architettura di massima per cui gli ambienti sono separati e, negli eventuali punti di contatto, come la separazione è realizzata; b. le politiche di sicurezza adottate per garantire la separazione dell'ambiente di sviluppo e test da quello di produzione;			
Ordinari	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	1. Sono definite politiche e procedure con riferimento alla sicurezza delle applicazioni per fornire un adeguato supporto alla pianificazione, realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni, le quali dovranno essere riviste e aggiornate almeno su base annuale. [IaaS, SaaS]			
Ordinari	**PROTECT (PR)**	**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-3:** Sono attivi processi di controllo della modifica delle configurazioni	1. Sono definite: a. le politiche di sicurezza adottate per l'aggiornamento delle configurazioni dei sistemi IT e di controllo industriale e per il controllo della modifica delle configurazioni in uso rispetto a quelle previste; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Ordinari	**PROTECT (PR)**	**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-3:** Sono attivi processi di controllo della modifica delle configurazioni	2. È implementata una procedura per la gestione delle eccezioni, incluse emergenze, nel processo di modifica e configurazione.			
Ordinari	**PROTECT (PR)**	**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-3:** Sono attivi processi di controllo della modifica delle configurazioni	3. Sono definiti e implementati piani di ripristino allo stato precedente (cd. rollback) in caso di errori o problemi di sicurezza.			
Ordinari	**PROTECT (PR)**	**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-4:** I backup delle informazioni sono eseguiti, amministrati e verificati	1. Sono definite, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per il backup delle informazioni; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Ordinari	**PROTECT (PR)**	**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-4:** I backup delle informazioni sono eseguiti, amministrati e verificati	2. Viene effettuato periodicamente un backup dei dati memorizzati nel cloud. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup			
Ordinari	**PROTECT (PR)**	**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-4:** I backup delle informazioni sono eseguiti, amministrati e verificati	3. Le copie di backup di informazioni, software e immagini di sistema del servizio cloud sono protette con crittografia forte ed archiviate regolarmente in siti remoti (nel rispetto di quanto previsto dalla categoria PR.DS). Qualora i backup siano trasmessi ad un sito remoto tramite rete, la trasmissione deve essere protetta con crittografia forte.			
Ordinari	**PROTECT (PR)**	**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-4:** I backup delle informazioni sono eseguiti, amministrati e verificati	4. Viene verificato periodicamente il ripristino (test di restore) delle copie di backup come da obiettivo (SLO) identificato per il corrispondente indicatore di servizio (SII) riportato alla Tabella 1 "Indicatori minimi della qualità del Servizio"			
Ordinari	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	1. L'impatto derivante da interruzioni di business ed eventuali rischi è determinato al fine di stabilire i criteri per sviluppare strategie e capacità di business continuity.			
Ordinari	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	2. Esiste un documento aggiornato di dettaglio contenente i piani di continuità operativa, nonché quelli di risposta in caso di incidenti, che comprende almeno: a. le politiche e i processi impiegati per identificare le priorità degli eventi; b. le fasi di attuazione dei piani; c. i ruoli e le responsabilità del personale; d. i flussi di comunicazione e reportistica; e. il raccordo con il CS1RT Italia.			
Ordinari	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	3. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.			
Ordinari	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	4. I piani di business continuity sono collaudati e comunicati alle parti interessate.			
Ordinari	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	5. La documentazione di cui al punto 2 è resa disponibile, ove richiesto, all'Amministrazione e rivista periodicamente.			
Ordinari	**PROTECT (PR)**	**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-12:** Viene sviluppato e implementato un piano di gestione delle vulnerabilità	1. Esiste un documento aggiornato di dettaglio che indica almeno: a. le politiche di sicurezza adottate per gestire le vulnerabilità; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Ordinari	**PROTECT (PR)**	**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-12:** Viene sviluppato e implementato un piano di gestione delle vulnerabilità	2. Sono definite ed implementate procedure e misure tecniche volte all'aggiornamento degli strumenti di rilevamento, delle threat signatures e degli indicatori di compromissione, le quali dovranno essere riviste e aggiornate frequentemente o su base settimanale. (SaaS)			
Ordinari	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	1. Sono definite anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per la registrazione della manutenzione e riparazione delle risorse e dei sistemi; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Ordinari	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-2:** La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	1. La manutenzione delle risorse e dei sistemi (ivi incluse le attività relative alle funzioni di sicurezza) svolta da remoto è eseguita nel rispetto delle misure di cui alla sottocategoria PR.AC-3 e dei seguenti punti.			

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Ordinari	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-2:** La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	2. Tutti gli accessi eseguiti da remoto da personale di terze parti sono autorizzati dall'organizzazione di cybersecurity e limitati ai soli casi essenziali.			
Ordinari	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-2:** La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	3. Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi.			
Ordinari	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-2:** La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	4. Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili.			
Ordinari	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-2:** La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	5. Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.			
Ordinari	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1:** Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi	1, I log sono conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi.			
Ordinari	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1:** Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi	a. le politiche di sicurezza adottate per la gestione dei log dei sistemi; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza con particolare riguardo all'integrità e alla disponibilità dei log.			
Ordinari	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-5:** Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	1. In relazione ai piani previsti dalla sottocategoria PR.IP 9: a. sono adottate architetture ridondate di rete, di connettività, nonché applicative;			
Ordinari	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-5:** Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	2. Esistono meccanismi per garantire la continuità di servizio, nel rispetto delle misure di sicurezza qui elencate. 3. Sono definite:			
Ordinari	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-5:** Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	a. le politiche di sicurezza adottate in relazione ai punti 1 e 2; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Ordinari	**QUALITA'**	**Qualità del servizio**	**QU.SE-1:** Sono adottati sistemi per la gestione del servizio IT e della qualità conformemente agli standard di settore	1.11 sistema di gestione della qualità del servizio cloud è adottato formalmente dal soggetto in conformità allo standard UNI EN 150 9001:2015-Sistemi di Gestione per la Qualità.			
Ordinari	**QUALITA'**	**Qualità del servizio**	**QU.SE-1:** Sono adottati sistemi per la gestione del servizio IT e della qualità conformemente agli standard di settore	2. Il sistema di gestione dei servizi IT del servizio cloud è adottato formalmente dal soggetto in conformità allo standard ISO/IEC 20000-1:2018-Sistema di gestione dei servizi 1T.			
Ordinari	**QUALITA'**	**Qualità del servizio**	**QU.SE-2:** Viene fornito un adeguato servizio di assistenza e supporto	1. è garantito il servizio di supporto e assistenza all'Amministrazione per il servizio cloud.			
Ordinari	**QUALITA'**	**Qualità del servizio**	**QU.SE-2:** Viene fornito un adeguato servizio di assistenza e supporto	2.Il servizio di supporto e assistenza di cui al punto 1 è fornito almeno in lingua italiana tutti i giorni dell'anno a qualsiasi orario (24/7/365).			
Ordinari	**QUALITA'**	**Qualità del servizio**	**QU.SE-2:** Viene fornito un adeguato servizio di assistenza e supporto	3.11 servizio di supporto e assistenza di cui al punto 1 è accessibile almeno tramite recapito telefonico e posta elettronica.			
Ordinari	**QUALITA'**	**Qualità del servizio**	**QU.SE-2:** Viene fornito un adeguato servizio di assistenza e supporto	4. Il servizio di supporto e assistenza di cui al punto 1 prevede, inoltre, un sistema di risoluzione dei problemi (troubleshooting) a disposizione dell'Amministrazione, garantendone anche l'esposizione tramite API per permettere l'interazione programmatica con i sistemi di gestione dei problemi (Case Management System).			
Ordinari	**QUALITA'**	**Qualità del servizio**	**QU.SE-3:** Il soggetto dichiara la frequenza di aggiornamento del servizio	1. Il soggetto deve dichiarare la frequenza attesa di aggiornamento del servizio cloud qualificato (es. periodicità rilasci pianificati).			
Ordinari	**QUALITA'**	**Qualità del servizio**	**QU.SE-4:** Linee guida e raccomandazioni sull'uso sicuro di soluzioni cloud	1. Devono essere rese disponibili all'Amministrazione le linee guida per una gestione sicura del servizio cloud oggetto di qualificazione, indirizzando, ove applicabile, i seguenti aspetti: a. Istruzioni per una configurazione sicura; b. Informazione su vulnerabilità note e meccanismi di aggiornamento; c. Gestione degli errori e meccanismi di logging; d. Meccanismi di autenticazione; e. Ruoli e diritti, comprese le combinazioni che risultano in un rischio elevato; f. Servizi e funzioni per l'amministrazione del servizio da parte di utenti privilegiati; g. Le linee guida vengono fornite e mantenute nelle modalità e tempistiche di cui alla misura IP.GR-01.			
Ordinari	**QUALITA'**	**Pricing**	**QU.PR-1:** Tracciamento, reportistica e trasparenza dei costi e della loro elaborazione	1. Il soggetto rende disponibile all'Amministrazione strumenti (es una dashboard) ed API che permettono di acquisire informazioni di dettaglio sulle metriche per il calcolo dei costi del servizio cloud (cd. di "billing") per rendere il calcolo trasparente all'Amministrazione. Le metriche per il calcolo dei costi del servizio cloud devono essere espresse a livello sintetico o dettagliate per indirizzo di costo (es. risorsa cloud).			
Ordinari	**QUALITA'**	**Pricing**	**QU.PR-1:** Tracciamento, reportistica e trasparenza dei costi e della loro elaborazione	2. Gli strumenti e le API di cui al punto 1 permettono di filtrare e creare report di fatturazione con il dettaglio dei costi per ora, giorno o mese, per ogni account o prodotto in uso del servizio cloud. Il tracciamento e l'aggiornamento delle informazioni sul costo deve essere aggiornato almeno una volta ogni ora.			
Ordinari	**QUALITA'**	**Pricing**	**QU.PR-2:** Notifica e monitoraggio dei costi	1. Il soggetto offre all'Amministrazione un sistema di monitoraggio dei costi che permetta di impostare allarmi con notifiche per avvisare l'Amministrazione nel caso in cui l'utilizzo del servizio cloud si avvicina o supera il budget/le soglie impostate.			
Ordinari	**QUALITA'**	**Pricing**	**QU.PR-3:** Requisiti minimi per il capitolato dei prezzi	1. Il soggetto specifica all'Amministrazione il proprio metodo e modello di determinazione dei prezzi per la fornitura del servizio cloud, che deve assicurare la massima flessibilità commerciale e supportare scalabilità e crescita.			
Ordinari	**QUALITA'**	**Pricing**		2.Il soggetto fornisce all'Amministrazione: a. un documento contenente i termini e le condizioni, specificando in particolare qualora i prezzi siano forniti per un servizio al consumo e se sono in atto politiche di adeguamento dinamico dei prezzi al mercato; b. un documento contenente i prezzi (i riferimenti ai prezzi al pubblico sono ammessi a condizione che, su richiesta, sia disponibile un documento completo di listino/prezzi).			
Ordinari	**QUALITA'**	**Pricing**	**QUIS-1:** È garantito il rispetto degli indicatori di servizio obbligatori, sono rese note le modalità di condivisione dei livelli di disponibilità dei servizi e le eventuali penali compensative	1. Il soggetto garantisce aderenza agli obiettivi (SLO) corrispondenti agli indicatori di servizio (SU) riportati in Tabella 1 "Indicatori della Qualità del Servizio" e ne garantisce il rispetto nei rapporti contrattuali nella forma di accordi relativi ai livelli di servizio (SLA). 11 soggetto può comunicare all'Amministrazione eventuali ulteriori indicatori della medesima tabella, o indicarne di nuovi, che potranno essere inseriti come impegni contrattuali con specifici SLO nei rapporti contrattuali.			
Ordinari	**QUALITA'**	**Pricing**	**QUIS-1:** È garantito il rispetto degli indicatori di servizio obbligatori, sono rese note le modalità di condivisione dei livelli di disponibilità dei servizi e le eventuali penali compensative	2.Il soggetto garantisce che venga definita la modalità di condivisione delle informazioni dei livelli di servizio atteso garantiti (SLA) del servizio cloud con l'Amministrazione (es. report periodico) e che, qualora successivamente all'avvio della fornitura si dovesse rendere necessaria una qualsiasi modifica ai livelli di servizio garantiti, questa dovrà essere preventivamente notificata all'Amministrazione per ottenerne la sua approvazione.			
Ordinari	**QUALITA'**	**Pricing**	**QUIS-1:** È garantito il rispetto degli indicatori di servizio obbligatori, sono rese note le modalità di condivisione dei livelli di disponibilità dei servizi e le eventuali penali compensative	3. Il soggetto garantisce l'applicazione di penali compensative da corrispondere all'Amministrazione in caso di violazione dei livelli di servizio garantiti dal contratto di fornitura del servizio qualificato. I metodi di quantificazione e le condizioni di riconoscimento delle penali compensative sono inclusi nel contratto e sono allineati ai valori e alle condizioni di mercato riscontrabili per servizi analoghi o appartenenti alla medesima categoria.			
Ordinari	**QUALITA'**	**Pricing**	**QU.LS-2:** Esistono limitazioni per i Service Leve! Agreement (SLA) per prevenire impatti sugli ambienti dell'Amministrazione	1. All'interno dei Service Level Agreement (SLA) tra il soggetto e l'Amministrazione sono presenti limitazioni con riferimento a modifiche che abbiano impatto direttamente sugli ambienti e/o tenant di proprietà dell'Amministrazione.			
Ordinari	**QUALITA'**	**Pricing**	**QULS-3:** Esistono contenuti e caratteristiche minimi per i Service Level Agreement	1. Ogni SLA tra il soggetto e l'Amministrazione tiene conto di quanto segue: a. Ambito, caratteristiche e ubicazione della relazione commerciale e dei servizi offerti; b. Requisiti di sicurezza delle informazioni (incluso il SSRM - Shared Security Responsibility Mode!); c. Processo di Change Management; d. Logging e Monitoring; e. Gestione degli incidenti e procedure di comunicazione; f. Diritto di audit e valutazione da parte di terzi; g. Terminazione del servizio; h. Requisiti di interoperabilità e portabilità; i. Riservatezza dei dati.			
Ordinari	**QUALITA'**	**Pricing**	**QULS-4:** È disponibile un servizio di monitoraggio (allarmi e parametri) e sono rese note eventuali integrazioni native con soluzioni leader di mercato.	1. Il soggetto rende disponibile all'Amministrazione l'accesso ad uno o più strumenti di monitoraggio per il servizio cloud. Essi devono consentire attività di raccolta, monitoraggio, filtraggio, creazione di report attraverso parametri predefiniti o parametrizzabili e consentire all'Amministrazione di impostare allarmi personalizzati. La granularità massima delle operazioni non deve essere superiore al minuto (ad es., deve essere possibile filtrare o raccogliere gli eventi ogni minuto). In aggiunta, il soggetto specifica l'eventuale disponibilità di API e strumenti di monitoraggio di terze parti integrate nativamente con il servizio qualificato.			
Ordinari	**RECOVER (RC)**	**Recovery Planning (RC.RP):** I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.	**RC.RP-1:** Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity	1. Esiste un piano di ripristino che prevede, almeno, i processi e le procedure necessarie al ripristino del normale funzionamento della porzione dell'infrastruttura coinvolta da un incidente di cybersecurity			
Ordinari	**RECOVER (RC)**	**Recovery Planning (RC.RP):** I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.	**RC.RP-1:** Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity	1. Esiste un piano di ripristino che prevede, almeno, i processi e le procedure necessarie al ripristino del normale funzionamento dei servizi cloud coinvolti da un incidente di cybersecurity.			
Ordinari	**RESPOND (RS)**	**Improvements (RS.MI):** Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i suoi effetti e per risolvere l'incidente	**RS.MI-3:** Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	1.Le vulnerabilità sono mitigate secondo quanto previsto dal piano di gestione delle vulnerabilità (PR.113-12), ovvero ne viene documentato e accettato il rischio residuo derivante dalla mancata mitigazione			
Ordinari	**RESPOND (RS)**	**Improvements (RS.MI):** Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i suoi effetti e per risolvere l'incidente	**RS.MI-3:** Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	2.Sono definite ed implementate procedure e misure tecniche per consentire azioni di risposta (programmate o al sopraggiungere di emergenze) in caso di vulnerabilità identificate, in base a! rischio.			
Ordinari	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	1. Il piano di risposta prevede l'esecuzione tempestiva della valutazione degli eventi rilevati tramite l'analisi e la correlazione di cui alla categoria DE nonché la disseminazione immediata degli esiti verso le articolazioni competenti del soggetto, anche ai fini della notifica all'Amministrazione e, su base volontaria, al CSIRT Italia, degli incidenti con impatto sul servizio cloud.			
Ordinari	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	1. I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di cui al punto 1 sono ben definiti e resi noti alle articolazioni competenti del soggetto.			
Ordinari	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	2. Sono eseguite periodicamente esercitazioni.			
Ordinari	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	3. Esiste un documento aggiornato di dettaglio che indica almeno: a. le fasi, i processi, i ruoli e le responsabilità di cui ai punti 1 e 2; b. i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilità di cui ai punti 1 e 4 c. le modalità per le esercitazioni di cui al punto 3.			
Ordinari	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-5:** È attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)	1. Sono definiti e mantenuti contatti con gruppi di interesse legati al cloud e altre entità rilevanti e in linea con il contesto del soggetto.			
Ordinari	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-5:** È attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)	2. Sono definiti e mantenuti punti di contatto con le autorità di regolamentazione applicabili, le forze dell'ordine nazionali e locali e altre autorità giurisdizionali legali.			
Ordinari	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.AN-5:** Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)	1. Gli esiti delle valutazioni di cui alla sottocategoria DE.AE-3 e dei penetration test e vulnerability assessment di cui alla sottocategoria DE.CM-8, qualora disponibili, sono diffusi alle articolazioni competenti del soggetto			
Ordinari	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.AN-5:** Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)	2. I canali di comunicazione del CSIRT Italia di cui all'articolo 4 del decreto del Presidente del Consiglio dei ministri 8 agosto 2019, dell'Autorità di riferimento del proprio settore produttivo, nonché di eventuali CERT e Information Shartng & Analysis Centre (ISAC) di riferimento sono monitorati.			
Ordinari	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.AN-5:** Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)	3. Esiste un documento aggiornato che descrive, almeno: a, le modalità per ricevere, analizzare e rispondere almeno alle informazioni raccolte tramite le attività di cui ai punti i e 2; b. i processi, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2.			
Ordinari	RISPARMIO ENERGETICO	**Risparmio energetico**	**RE.GE-01:** Gestione energetica condotta in aderenza agli standard di settore	1. Il soggetto ha formalmente adottato procedure per la gestione delle emissioni dei gas prodotti dai suoi Data Center (es. ISO 14064), o per la gestione dell'energia dei propri Data Center (es. ISO 50001), o per la gestione ambientale dei propri Data Center (es. 150 14001).			
Ordinari	RISPARMIO ENERGETICO	**Risparmio energetico**	**RE-GE-02:** Valutazione annuale dell'efficienza energetica del Data Center	1.Il soggetto determina con frequenza annuale l'efficienza energetica del proprio Data Center, ricorrendo al calcolo dell'indicatore Power Usage Effectiveness (PUE), che deve assumere valore massimo pari a 1,5. Il PUE mette in relazione la spesa energetica dell'infrastruttura, compresa di apparati IT, impianto di climatizzazione e impianti ausiliari, con la spesa esclusivamente riferita agli apparati IT. Nello specifico, è calcolato come il rapporto tra la spesa energetica sostenuta per tutta l'infrastruttura del DC e quella sostenuta per gli apparati.			
Strategici	**AFFIDABILITA'**		**A.8C-4: Sono disponibili soluzioni di Disaster Recovery con tempi di ripristino garantiti**	1. Provider di infrastruttura: L'infrastruttura digitale deve essere dotata di soluzioni di DR e deve garantire tempi di ripristino (RTO e RPO) variabili in funzione della criticità dell'applicazione ospitata conformemente con quanto definito nella BIA. Devono comunque essere garantiti almeno i seguenti parametri di ripristino in caso di disastro: RTO 8 ore e RPO 8 ore;			
Strategici	**AFFIDABILITA'**		**A.8C-4: Sono disponibili soluzioni di Disaster Recovery con tempi di ripristino garantiti**	2. Public Cloud provider: devono essere presenti servizi di Disaster Recovery.			
Strategici	**DETECT (DE)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**DE.AE-3:** Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	10. Esiste una repository centralizzata che contiene i log di accesso degli utenti del soggetto, gestito direttamente dal soggetto e segregato a livello logico rispetto ai sistemi a cui terze parti hanno accesso diretto.			

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Strategici	**DETECT (DE)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**DE.AE-3:** Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	11. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3 lett. a, b, c, d.			
Strategici	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	3. Il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali sono monitorati e correlati al fine di identificare eventi di cybersecurity.			
Strategici	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	4. Gli strumenti tecnici di cui al punto 1 sono aggiornati, manutenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PRA) e PR.MA e concorrono al rispetto delle politiche di cui alla categoria ID.AM,1D.GV,ID.SC, PR.AC e PR.DS.			
Strategici	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	5. Gli strumenti tecnici di cui al punto i sono impiegati anche per i fini di cui alla categoria DE.AE			
Strategici	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	6. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione al punto 2; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza			
Strategici	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	4. Sono configurati appositi software firewall su tutti i dispositivi.			
Strategici	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	5.I file in ingresso (tramite posta elettronica, download, dispositivi removibili, etc.) sono analizzati, anche tramite sandbox.			
Strategici	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	6. Gli strumenti tecnici di cui ai punti 4 e 5 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorieID.AM,ID.GV,ID.SC, PR.AC e PR.DS.			
Strategici	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	7. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 1, 2 e 3; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Strategici	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	5. Con riferimento alla sottocategoria ID.AM-2, fatti salvi documentati limiti tecnici, sono presenti sistemi di controllo per il rilevamento dei software non approvati.			
Strategici	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	6. Con riferimento alla sottocategoria ID.AM-3, sono presenti sistemi di controllo per il rilevamento delle connessioni non autorizzate.			
Strategici	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	7. Gli strumenti tecnici di cui ai punti 5 e 6 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM,1D.GV, I D.SC, PR.AC e PR.DS.			
Strategici	**DETECT (DE)**	**Security Continuous Monitoring (DE.CM):** I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	8. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 5 e 6; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.			
Strategici	DETECT (DE)		**DE.AE-3:** Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	9. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3 lett. a, b, c, d.			
Strategici	DETECT (DE)		**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	5. Con riferimento alla sottocategoria ID.AM-2, fatti salvi documentati limiti tecnici, sono presenti sistemi di controllo per il rilevamento dei software non approvati.			
Strategici	DETECT (DE)		**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	6. Con riferimento alla sottocategoria 1D.AM 3, sono presenti sistemi di controllo per il rilevamento delle connessioni non autorizzate.			
Strategici	DETECT (DE)		**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	7. Gli strumenti tecnici di cui ai punti 5 e 6 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.1P e PR.MA e concorrono a! rispetto delle politiche di cui alle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.			
Strategici	DETECT (DE)		**DE.CM-7:** Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	8. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 5 e 6; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza			
Strategici	**IDENTIFY (ID)**	**Asset Management (ID.AM)**: I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-6:** Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	13. I nominativi e gli estremi di contatto dell'incaricato di cui al punto 2 e del referente tecnico di cui al punto 4 sono comunicati dal soggetto all'Agenzia per la Cybersicurezza Nazionale (ACN).			
Strategici	IDENTIFY (ID)	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È indetificata e resa nota una policy di cybersecurity	3. Ogni scostamento dai livelli minimi di sicurezza definito internamente nel documento di cui al punto 1 deve essere identificato, gestito ed eventualmente autorizzato dal soggetto attraverso un processo di governance strutturato.			
Strategici	IDENTIFY (ID)	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È indetificata e resa nota una policy di cybersecurity	4.Esiste un documento aggiornato recante indicazioni in merito alla pianificazione, ai ruoli, all'implementazione, operazione, valutazione, e miglioramento di programmi di cybersecurity sia in relazione al personale interno che per eventuali terze parti			
Strategici	IDENTIFY (ID)	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-1:** Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	3. Le relazioni periodiche devono contenere almeno: a.la descrizione generale delle tipologie di verifiche effettuate e gli esiti delle stesse; b.la descrizione dettagliata delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza; c.il livello di esposizione delle risorse del sistema cui è possibile accedere a seguito dello sfruttamento delle vulnerabilità.			
Strategici	IDENTIFY (ID)	**Risk Assessment (ID.RA):** L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-1:** Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	4. Esiste un documento per la correzione delle vulnerabilità che prevede anche la notifica alle parti interessate.			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	3.Sono presenti politiche e procedure per la definizione, implementazione e applicazione del modello di responsabilità della sicurezza condivisa (Shared Security Responsibility Model-SSRM) all'interno dell'organizzazione, le quali dovranno essere riviste e aggiornate almeno su base annuale.			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	4.Il modello SSRM è applicato a tutta la catena di approvvigionamento cyber, ivi incluse le Infrastrutture digitali.			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-2:** I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber	1. In merito all'affidamento di forniture sono adottate misure in materia di sicurezza della catena di approvvigionamento attraverso: a.il coinvolgimento dell'organizzazione di cybersecurity, tra cui l'incaricato di cui alla sottocategoria ID.AM-6, punto 2, nel processo di fornitura, già a partire dalla fase di progettazione;b.fatti salvi documentati limiti tecnici, il rispetto del requisito di fungibilità, con la possibilità di ricorrere alla scadenza ad altro fornitore; c.fatti salvi documentati limiti tecnici, la diversificazione dei fornitori e la conseguente resilienza dell'Infrastruttura digitale; d.la valutazione dell'affidabilità tecnica dei fornitori e dei partner terzi, con riferimento alle migliori pratiche in materia e tenendo conto almeno: i.della qualità dei prodotti e delle pratiche di sicurezza cibernetica del fornitore e dei partner terzi, anche considerando il contrailo degli stessi sulla propria catena di approvvigionamento e la priorità data agli aspetti di sicurezza; ii.della capacità del fornitore e dei partner terzi di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo.			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-2:** I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber	2.Esiste un elenco aggiornato dei fornitori e partner terzi affidatari per il funzionamento dell'infrastruttura, nonché di dipendenze esterne, corredato dalla relativa documentazione dei processo di valutazione di cui al punto 1 lettera d			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-2:** I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber	3.Si raccomanda, ove possibile e in relazione alla criticità di: a. valutare l'affidabilità tecnica di cui al punto 1, lettera d, anche tenendo conto: i.della disponibilità del fornitore a condividere il codice sorgente; ii.di certificazioni o evidenze utili alla valutazione della qualità del processo di sviluppo del software del produttore; iii.dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire l'autenticità e l'integrità del software o firmware installato all'interno dei beni e dei sistemi di Information and Communication Technology; iv.dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire una corrispondenza univoca tra il codice sorgente e il codice oggetto installato e eseguito. b. adottare processi e strumenti tecnici per: i.valutare la qualità e la sicurezza del codice sorgente, qualora reso disponibile dal produttore; ii.acquisire il codice oggetto dai beni e sistemi di Information and Communication Technology; iii.confermare la corrispondenza univoca tra il codice sorgente e il codice oggetto installato ed eseguito			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-3:** I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber	1. Le misure di sicurezza implementate dal soggetto in relazione a dipendenze interne sono coerenti, anche in relazione agli esiti dell'analisi del rischio, con le misure di sicurezza applicate all'Infrastruttura digitale. A tal fine, i contratti, gli accordi o le convenzioni sono aggiornati di conseguenza.			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-4:** Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	1.Esiste un documento aggiornato che descrive il processo, le modalità, la cadenza delle valutazioni per i fornitori e partner terzi, proporzionate agli esiti dell'analisi del rischio effettuata.			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-4:** Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	2.Esiste una pianificazione aggiornata degli audit, delle verifiche o di altre forme di valutazione previste, nonché un registro di quelli effettuati e la relativa documentazione.			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-4:** Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	3.È definito ed implementato un processo di Audit Management al fine di consentire lo svolgimento di valutazioni indipendenti e di garanzia, nel rispetto dei principali standard di settore, almeno su base annuale e secondo una pianificazione che tenga conto del rischio			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-4:** Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	4.Le politiche e procedure di audit e garanzia degli standard, devono essere stabilite, documentate, approvate, mantenute e riviste almeno annualmente.			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-4:** Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	5.è definito, documentato, approvato, comunicato, applicato e mantenuto un piano di Remediation.			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	6. Esiste un documento recante i processi di cui ai punti 1 e 2.			

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-2:** I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber	3. Si raccomanda, ove possibile e in relazione alla criticità di: a. valutare l'affidabilità tecnica di cui al punto 1, lettera d, anche tenendo conto: i. della disponibilità del fornitore a condividere il codice sorgente; ii. di certificazioni o evidenze utili alla valutazione della qualità del processo di sviluppo del software del produttore; iii. dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire l'autenticità e l'integrità del software o firmware installato all'interno dei beni e dei sistemi di information and communication technology; iv. dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire una corrispondenza univoca tra il codice sorgente e il codice oggetto installato ed eseguito, b. adottare processi e strumenti tecnici per: i. valutare la qualità e la sicurezza del codice sorgente, qualora reso disponibile dal produttore; ii. acquisire il codice oggetto dai beni e sistemi di information and communication technology; iii. confermare la corrispondenza univoca tra il codice sorgente e il codice oggetto installato ed eseguito.			
Strategici	IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-3:** I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber	2. Le misure di sicurezza implementate dai terzi affidatari di servizi esterni sono coerenti, anche in relazione agli esiti dell'analisi del rischio, con le misure di sicurezza applicate al servizio cloud. A tal fine, contratti, accordi ❑ convenzioni sono aggiornati di conseguenza.			
Strategici	**PROTECT (PR)**	**Awareness and Training (PR.AT):** Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti	**PR.AT-1:** Tutti gli utenti sono informati e addestrati	3. Per ogni membro del personale del soggetto, esiste un registro aggiornato, comprensivo delle istruzioni ricevute.			
Strategici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	4. Sono definite ed implementate procedure e misure tecniche per la distruzione delle chiavi memorizzate al di fuori di un ambiente sicuro e revocare le chiavi memorizzate nei moduli di sicurezza hardware (HSM) quando non sono più necessari, in conformità con requisiti legali e normativi.			
Strategici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-3:** Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	2. Sono abilitate capacità di geo-localizzazione remota per tutti i dispositivi mobili gestiti.			
Strategici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-3:** Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	3. Sono definite ed implementate adeguate tecniche di cancellazione dei dati dell'Amministrazione da remoto.			
Strategici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-3:** Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.			
Strategici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-5:** Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.			
Strategici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-6:** Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni	Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui ai punto 1.			
Strategici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-7:** Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.			
Strategici	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	2. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria 1D.AM, almeno: a. le politiche di sicurezza adottate per lo sviluppo di configurazioni di sistemi 1T e il dispiegamento delle sole configurazioni adottate; b. l'elenco delle configurazioni dei sistemi IT e impiegate e il riferimento alle relative pratiche di riferimento; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza			
Strategici	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	3. Sono definiti e documentati requisiti di base per la sicurezza delle diverse applicazioni.			
Strategici	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	4. Sono definite ed implementate metriche tecniche e operative in linea con i requisiti di sicurezza e gli obblighi di conformità			
Strategici	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	5. Esiste un processo di mitigazione e ripristino per la sicurezza delle applicazioni vulnerabilità delle applicazioni, automatizzando la riparazione quando possibile.			
Strategici	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	6. E presente un processo per la convalida della compatibilità del dispositivo con sistemi operativi e applicazioni.			
Strategici	**PROTECT (PR)**	**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-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	7. È presente un sistema di gestione delle variazioni in termini di sistema operativo, patching e/o applicazioni			
Strategici	**PROTECT (PR)**	**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-11:** Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, deprovisioning)	1. Il soggetto rende disponibile all'Amministrazione la metodologia utilizzata per la verifica del personale (vetting process methodology) con accesso privilegiato all'infrastruttura o ai dati dell'Amministrazione.			
Strategici	**PROTECT (PR)**	**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-11:** Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, deprovisioning)	2. Il soggetto rende disponibile all'Amministrazione l'elenco dei dipendenti con accesso privilegiato all'infrastruttura o ai dati dell'Amministrazione. L'Amministrazione può richiedere unilateralmente la rimozione di uno o più dipendenti dal citato elenco e il soggetto provvede nel senso tempestivamente.			
Strategici	**PROTECT (PR)**	**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-12:** Viene sviluppato e implementato un piano di gestione delle vulnerabilità	2. Il documento di cui al punto 1 della misura PR.1P-12 dovrà essere aggiornato su base semestrale.			
Strategici	**PROTECT (PR)**	**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-12:** Viene sviluppato e implementato un piano di gestione delle vulnerabilità	3. Sono definite ed implementate misure tecniche per l'identificazione degli aggiornamenti per le applicazioni che usano librerie di terze parti o open, nel rispetto delle politiche interne di vulnerability management.			
Strategici	**PROTECT (PR)**	**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-3:** Sono attivi processi di controllo della modifica delle configurazioni	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.			
Strategici	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	7. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi dall'Infrastruttura digitale e, se previsti, dalle hot-replica e/o cold-replica nonché dal sito(i) di disaster recovery.			
Strategici	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	8. Esiste un documento aggiornato di dettaglio contenente i piani di disaster recovery, nonché quelli di risposta e di recupero in caso di incidenti, che comprende almeno: a. le politiche e i processi impiegati per identificare le priorità degli eventi; b. le fasi di attuazione dei piani; c. i ruoli e le responsabilità del personale; d. i flussi di comunicazione e reportistica; e. il raccordo con il CSIRT Italia			
Strategici	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	9. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.			
Strategici	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	10. Le strategie di disaster recovery sono collaudate e comunicate alle parti interessate.			
Strategici	**PROTECT (PR)**	**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-9:** Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	11. I dispositivi critici per il funzionamento dell'Infrastruttura sono ridondati e, se situati in località diverse, ad una distanza in linea con le migliori pratiche del settore.			
Strategici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	2. Esiste un registro aggiornato delle manutenzioni e riparazioni eseguite.			
Strategici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.			
Strategici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	4. In base all'analisi del rischio, ogni aggiornamento dei software ritenuti critici, fatte salve motivate esigenze di tempestività relative alla sicurezza, dovrà essere verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo e il relativo codice oggetto dovrà essere custodito per almeno 24 mesi.			
Strategici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	5. In base all'analisi del rischio di cui alla misura 1D.RA-5, ogni aggiornamento hardware o software di componenti ritenuti critici, fatte salve motivate esigenze di tempestività relative alla sicurezza, dovrà essere verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo e, se del caso, il relativo codice oggetto dovrà essere custodito per almeno 24 mesi. Le attività in ambiente di test sono volte a verificare anche aspetti di sicurezza			
Strategici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	6. Gli aggiornamenti software devono essere consentiti solo da fonti pre-autorizzate.			
Strategici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	7. Tutti i log relativi alle attività di manutenzione e aggiornamento dovranno essere prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze che svolgono tali attività.			
Strategici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	8. Esiste un documento aggiornato che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 5, 6 e 7.			
Strategici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-2:** La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	6. Esiste un documento aggiornato di dettaglio che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 2, 3, 4 e 5.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1:** Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-4:** Le reti di comunicazione e controllo sono protette	1. I sistemi perimetrali, quali firewall, anche a livello applicativo, sono presenti, aggiornati, manutenuti e ben configurati.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-4:** Le reti di comunicazione e controllo sono protette	2. Sistemi di prevenzione delle intrusioni (intrusion prevention systems - IPS) sono presenti, aggiornati, manutenuti e ben configurati.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-4:** Le reti di comunicazione e controllo sono protette	3. Gli strumenti tecnici di cui ai punti 1 e 2 concorrono al rispetto delle politiche di cui alla categoria ID.AM, I D.GV, ID.SC, PR.AC e PR.DS.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-4:** Le reti di comunicazione e controllo sono protette	4. L'aggiornamento, manutenzione e configurazione degli strumenti tecnici di cui ai punti 1 e 2 sono effettuati nel rispetto delle politiche di cui alla categoria PR.AC, PR.DS, PR.1P e PR.MA.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-4:** Le reti di comunicazione e controllo sono protette	5. Gli strumenti tecnici di cui ai punti 1 e 2 sono impiegati anche per i fini di cui alla funzione DE.			

Classificazione	Function	Category	Subcategory	Controlli	Valori attuali	Stato di realizzazione	Note
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-4:** Le reti di comunicazione e controllo sono protette	6. Esiste un documento aggiornato che descrive almeno i processi e gli strumenti tecnici impiegati per realizzare i punti 1, 2, 3 e 4.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-5:** Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	1-bis. In relazione ai piani previsti dalla sottocategoria PR.1P-9: a. sono adottate architettura ridondate di rete, di connettività, nonché applicative, b. esiste un sito di disaster recovery.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-5:** Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3.			
Strategici	**PROTECT (PR)**		**PR.AC-3:** L'accesso remoto alle risorse è amministrato	6.Le politiche e procedure aggiornate almeno su base annuale e rese disponibili per la consultazione. dietro specifica richiesta. del soggetto.			
Strategici	**PROTECT (PR)**		**PR.AC-3:** L'accesso remoto alle risorse è amministrato	7.è definito ed implementato un processo di autorizzazione congiunta con l'Amministrazione nel caso in cui vengano effettuati accessi ai dati della stessa. Nel caso in cui ciò non fosse possibile, il soggetto contatta l'Amministrazione nel minor tempo possibile informandolo degli accessi effettuati. Tutte le operazioni che prevedono l'accesso ai dati dell'Amministrazione devono essere gestite in linea con i criteri di user management e logging delle utenze privilegiate			
Strategici	**PROTECT (PR)**		**PR.AC-4:** I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	5. Il soggetto è autonomo nella gestione dell'infrastruttura, disponendo di proprie capacità per operare l'infrastruttura fisica e logica sottostante. Per casi eccezionali e sulla base di documentate limitazioni di carattere tecnico, il soggetto può avvalersi di competenze di terze parti, assicurandone, ove possibile, la fungibilità.			
Strategici	**PROTECT (PR)**		**PR.AC-5:** L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	3. Con riferimento ai censimenti di cui alla categoria 1D.AM, esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per la segmentazione/segregazione delle reti; b. la descrizione delle reti segregate/segmentate; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza; d. le modalità con cui porte di rete, protocolli e servizi in uso sono limitati e/o monitorati.			
Strategici	**PROTECT (PR)**		**PR.AC-7:** Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)	2. Esiste un documento aggiornato di dettaglio che, con riferimento ai censimenti di cui alla categoria 1D.AM e alla valutazione del rischio di cui alla categoria 1D.RA, contiene almeno: a. le modalità di autenticazione disponibili; b. la loro assegnazione alle categorie di transazioni.			
Strategici	**PROTECT (PR)**		**PR.AT-2:** Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità	3. Esiste un documento aggiornato di dettaglio recante i processi di cui ai punti 1 e 2			
Strategici	**PROTECT (PR)**		**PR.AC-3:** L'accesso remoto alle risorse è amministrato	6. Le politiche e procedure sono aggiornate almeno su base annuale e rese disponibili per la consultazione, dietro specifica richiesta, dell'Amministrazione.			
Strategici	**PROTECT (PR)**		**PR.AC-3:** L'accesso remoto alle risorse è amministrato	7. E definito ed implementato un processo di autorizzazione congiunta con l'Amministrazione nel caso in cui vengano effettuati accessi ai dati dello stesso. Nel caso in cui ciò non fosse possibile, il soggetto contatta l'Amministrazione nel minor tempo possibile informandolo degli accessi effettuati.			
Strategici	**PROTECT (PR)**		**PR.AC-3:** L'accesso remoto alle risorse è amministrato	8. Tutte le operazioni che prevedono l'accesso ai dati dell'Amministrazione devono essere gestite in linea con i criteri di user management e logging delle utenze privilegiate			
Strategici	**PROTECT (PR)**		**PR.AC-4:** I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	4. Tutte le attività privilegiate {es. installazione di aggiornamenti) e di accesso ai dati dell'Amministrazione da parte del personale del soggetto e di terze parti dovranno essere autorizzati dall'organizzazione di cybersecurity e limitate ai soli casi essenziali.			
Strategici	**PROTECT (PR)**		**PR.AC-5:** L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	3. Con riferimento ai censimenti di cui alla categoria ID.AM, esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per la segmentazione/segregazione delle reti; b. la descrizione delle reti segregate/segmentate; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza; d. le modalità con cui porte di rete, protocolli e servizi in uso sono limitati e/o monitorati.			
Strategici	**PROTECT (PR)**		**PR.AC-7:** Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)	3. Esiste un documento aggiornato di dettaglio che, con riferimento ai censimenti di cui alla categoria ID.AM e alla valutazione del rischio di cui alla categoria ID.RA, contiene almeno: a. le modalità di autenticazione disponibili; b. la loro assegnazione alle categorie di transazioni.			
Strategici	**PROTECT (PR)**		**PR.AT-2:** Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità	3. Esiste un documento aggiornato di dettaglio recante i processi di cui ai punti 1 e 2			
Strategici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	13. Esiste un documento aggiornato che descrive da quali sedi e infrastrutture è erogato i! servizio cloud. Il soggetto rende disponibile l'elenco all'Amministrazione.			
Strategici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-3:** Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.			
Strategici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-5:** Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.			
Strategici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-6:** Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.			
Strategici	**PROTECT (PR)**	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-7:** Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.			
Strategici	**PROTECT (PR)**		**PR.IP-3:** Sono attivi processi di controllo della modifica delle configurazioni	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.			
Strategici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	7. Esiste un registro aggiornato delle manutenzioni e riparazioni eseguite.			
Strategici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	8. In base all'analisi del rischio, ogni aggiornamento dei software ritenuti critici, fatte salve motivate esigenze di tempestività relative alla sicurezza, è verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo.			
Strategici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	9. Il codice oggetto relativo agli aggiornamenti di cui al punto 3 viene custodito per almeno 24 mesi.			
Strategici	**PROTECT (PR)**	**Maintenance (PR.MA):** La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-2:** La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	6. Esiste un documento aggiornato di dettaglio che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 2, 3, 4 e 5.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1:** Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 2 lett. a e b.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-4:** Le reti di comunicazione e controllo sono protette	1. I sistemi perimetrali, quali firewall, anche a livello applicativo, sono presenti, aggiornati, manutenuti e ben configurati.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-4:** Le reti di comunicazione e controllo sono protette	2. Sistemi di prevenzione delle intrusioni (intrusion prevention systems - IPS) sono presenti, aggiornati, manutenuti e ben configurati.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-4:** Le reti di comunicazione e controllo sono protette	3. Gli strumenti tecnici di cui ai punti 1 e 2 concorrono al rispetto delle politiche di cui alla categoria 1D.AM, ID.GV, 1D.SC, PR.AC e PR.DS.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-4:** Le reti di comunicazione e controllo sono protette	4. L'aggiornamento, manutenzione e configurazione degli strumenti tecnici di cui ai punti 1 e 2 sono effettuati nel rispetto delle politiche di cui alla categoria PR.AC, PR.DS, PR.IP e PR.MA.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-4:** Le reti di comunicazione e controllo sono protette	5. Gli strumenti tecnici di cui ai punti 1 e 2 sono impiegati anche per i fini di cui alla funzione DE.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-4:** Le reti di comunicazione e controllo sono protette	6. Esiste un documento aggiornato che descrive almeno i processi e gli strumenti tecnici impiegati per realizzare i punti 1, 2, 3 e 4.			
Strategici	**PROTECT (PR)**	**Protective Technology (PR.PT):** Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-5:** Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui ai punto 2 lett_ a e h_			
Strategici	RECOVER (RC)		**RC.IM-2:** Le strategie di recupero sono aggiornate	1. 11 piano di cui alla sottocategoria RC.RP-l è mantenuto aggiornato tenendo anche conto delle lezioni apprese nel corso delle attività di ripristino occorse.			
Strategici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	4. Esiste un registro aggiornato delle esercitazioni effettuate e dei partecipanti, con le relative lezioni apprese (lessons learned).			
Strategici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	5. Sono presenti politiche e procedure per la gestione degli incidenti di sicurezza, E-Discovery e Cloud Forensics, le quali dovranno essere riviste e aggiornate almeno su base annuale.			
Strategici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	6. Sono definiti ed implementati processi, procedure e misure tecniche per le notifiche di violazione della sicurezza.			
Strategici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	7. e previsto un meccanismo di segnalazione per ogni violazione della sicurezza, reale o presunta, comprese eventuali violazioni inerenti la supply chain, nel rispetto di SLA, leggi e regolamenti applicabili.			
Strategici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	8. Le attività di risposta condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione. In particolare, le attività di ripristino a seguito di un incidente sono comunicate alle parti interne ed esterne interessate (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT), ivi incluse le articolazioni competenti del soggetto, anche ai fini dell'eventuale interlocuzione con il CSIRT Italia.			
Strategici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	2. Le politiche e procedure per la gestione tempestiva degli incidenti di sicurezza sono riviste almeno su base annuale.			
Strategici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	3. Il piano di risposta e le politiche e procedure di cui ai punti 1 e 2 includono dipartimenti interni critici, l'Amministrazione (se impattata) e tutte le terze parti interessate.			
Strategici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	4. I piani di risposta agli incidenti sono collaudati e aggiornati ad intervalli pianificati o in caso di cambiamenti organizzativi o ambientali significativi.			
Strategici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	5. Sono definite e monitorate le metriche degli incidenti rilevanti in materia di cybersecurity.			
Strategici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	6. Sono definiti e implementati processi, procedure e misure di supporto ai processi aziendali per il triage degli eventi legati alla sicurezza.			
Strategici	**RESPOND (RS)**	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	7. Deve essere implementato un Computer Emergency Response Team (CERT), a coordinamento della fase di risoluzione degli incidenti e in aderenza a quanto definito dalle linee guida 1SO/IEC 27035-2. Inoltre, deve essere previsto il coinvolgimento periodico dell'Amministrazione in momenti di condivisione e revisione dello stato degli incidenti di interesse e, ove opportuno, nella risoluzione di tali incidenti, anche secondo gli accordi contrattuali in materia.			
Strategici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RC.CO-3:** Le attività di ripristino condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione	1. Le attività di ripristino a seguito di un incidente sono comunicate alle parti interne ed esterne interessate (es. le vittime, gli 1SP, i proprietari dei sistemi attaccati, i vendor, i CERT /CSIRT).			
Strategici	**RESPOND (RS)**	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RC.IM-2:** Le strategie di recupero sono aggiornate	Il piano di cui alla sottocategoria RC.RP-1 è mantenuto aggiornato tenendo anche conto delle lezioni apprese nel corso delle attività di ripristino occorse.			

REQUISITI PER LA QUALIFICAZIONE DEI SERVIZI CLOUD		
LIVELLO	CARATTERISTICHE	CERTIFICAZIONI RICHIESTE
QC1	è richiesto il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità di cui all'Allegato B2 dell'Atto per i servizi cloud per la pubblica amministrazione che possono trattare dati e servizi classificati quali ordinari, ai sensi dell'articolo 3 del Regolamento	**certificazione ISO 9001 - Sistemi di Gestione per la Qualità (SGQ) per il servizio cloud oggetto di qualifica** **una certificazione ISO/IEC 27001:2013 - Sistema di gestione per la sicurezza delle Informazioni (SGSI) con estensioni ISO/IEC 27017:2015 e ISO/IEC 27018:2019 per il servizio cloud oggetto di qualifica. In alternativa al suddetto requisito è possibile presentare certificazione Cloud Security Alliance - Star Leve12**
QC2	è richiesto, inoltre, il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità di cui all'Allegato B2 dell'Atto per i servizi cloud per ia pubblica amministrazione che possono trattare dati e servizi classificati quali critici, ai sensi dell'articolo 3 del Regolamento	**un'autocertificazione che attesti la conformità allo standard ISO 22301- Business Continuity-Management System (Gestione della continuità operativa) per il servizio cloud oggetto di qualifica** **un'autocertificazione che attesti la conformità allo standard ISO 20000- Service Management System per il servizio cloud oggetto di qualifica**
QC3	è richiesto, inoltre, il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità di cui all'Allegato B2 dell'Atto per i servizi cloud per la pubblica amministrazione che possono trattare dati e servizi classificati quali strategici, ai sensi dell'articolo 3 del Regolamento	**una certificazione ISO 22301- Business Continuity - Management System (Gestione della continuità operativa) per il servizio cloud oggetto di qualifica** **una certificazione ISO/IEC 20000 (Service Management) per il servizio cloud oggetto di qualifica;** **una certificazione Cloud Security Alliance - Star Level 2**
QC4	Ai fini della qualificazione di livello QC4 è richiesto il rispetto dei requisiti per il livello di qualificazione QC3 più ulteriori requisiti Requisiti in tema di controllo dei flussi ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati 2. Tutti i flussi per l'erogazione del servizio cloud sono soggetti a procedure di approvazione, di monitoraggio e di controllo concordati con l'Amministrazione. Requisiti in tema di cifratura e gestione chiavi e autonomia operativa PR.DS-1: i dati memorizzati sono protetti 14. Il servizio cloud supporta un meccanismo di cifratura di tipo Hold Your Own Key (HYOK), che consente all'Amministrazione la generazione e la gestione autonoma di tutte le chiavi di cifratura attraverso un HSM ospitato, alternativamente, presso: a. la propria infrastruttura b. un'infrastruttura messa a disposizione dal fornitore all'Amministrazione in modalità dedicata presso una terza parte scelta dall'Amministrazione 15. E' garantito l'accesso esclusivo da parte dell'Amministrazione alle chiavi di cui al punto 1 e ai dati in chiaro dell'Amministrazione. 16. 11 fornitore del servizio cloud mette a disposizione dell'Amministrazione un servizio di HSM in modalità dedicata. 17. li soggetto è autonomo nella fornitura del servizio cloud, disponendo di proprie capacità per operare l'infrastruttura fisica e logica sottostante. Per casi eccezionali e sulla base di documentate limitazioni di carattere tecnico, il soggetto può avvalersi di competenze di terze parti, assicurandone, ove possibile, la fungibilità. 5.1.3 Requisiti in tema di verifica e controllo del personale PR.IP-11: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, deprovisioning) 1. Il soggetto rende disponibile all'Amministrazione la metodologia utilizzata per la verifica del personale (vetting process methodology) con accesso privilegiato al servizio cloud o ai dati dell'Amministrazione. 2. Il soggetto rende disponibile all'Amministrazione l'elenco dei dipendenti con accesso privilegiato ai servizio cloud o ai dati dell'Amministrazione. L'Amministrazione può richiedere unilateralmente la rimozione di uno ❑ più dipendenti dal citato elenco e il soggetto provvede nel senso tempestivamente.	

REQUISITI PER LA QUALIFICAZIONE DI INFRASTRUTTURE		
LIVELLO	CARATTERISTICHE	CERTIFICAZIONI RICHIESTE
QI1	Ai fini della qualificazione di livello QI1 è richiesto il rispetto dei livelli minimi di cui all'Allegato A2 dell'Atto per le infrastrutture per la pubblica amministrazione che possono trattare dati e servizi classificati quali ordinari, ai sensi dell'articolo 3 del Regolamento	**una certificazione M 9001 Sistemi di Gestione per la Qualità (SGQ) per l'infrastruttura digitale oggetto di qualifica** **un'autocertificazione che attesti la conformità allo standard ISO/IEC 27001:2013 - Sistema di gestione per la sicurezza delle Informazioni, per l'infrastruttura digitale oggetto di qualifica**
QI2	Ai fini della qualificazione di livello QI2 è richiesto, inoltre, il rispetto dei livelli minimi di cui all'Allegato A2 dell'Atto per le infrastrutture per la pubblica amministrazione che possono trattare dati e servizi classificati quali critici, ai sensi dell'articolo 3 del Regolamento	**un'autocertificazione che attesti la conformità allo standard ISO 22301- Business Continuity-Management System (Gestione della continuità operativa) per l'infrastruttura digitale oggetto di qualifica;** **la certificazione ISO/IEC 27001:2013 - Sistema di gestione per la sicurezza delle Informazioni per l'infrastruttura digitale oggetto di qualifica**
QI3	Ai fini della qualificazione di livello QI3 è richiesto il rispetto dei requisiti per il livello di qualificazione Q12 è richiesto, inoltre, il rispetto dei livelli minimi di cui all'Allegato A2 dell'Atto per le infrastrutture per la pubblica amministrazione che possono trattare dati e servizi classificati quali strategici, ai sensi dell'articolo 3 del Regolamento	**una certificazione ISO 22301- Business Continuity-Management System (Gestione della continuità operativa) per l'infrastruttura digitale oggetto di qualifica**
QI4	Ai fini della qualificazione di livello QI4 è richiesto il rispetto dei requisiti per il livello di qualificazione QI3 9.1.2 Requisiti in tema di verifica e controllo del personale PR.IP-1 1: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, deprovisioning) 1. Il soggetto rende disponibile all'Amministrazione la metodologia utilizzata per la verifica del personale (vetting process methodology) con accesso privilegiato all'infrastruttura ❑ ai dati dell'Amministrazione. 2. Il soggetto rende disponibile all'Amministrazione l'elenco dei dipendenti con accesso privilegiato all'infrastruttura o ai dati dell'Amministrazione. L'Amministrazione può richiedere unilateralmente la rimozione di uno o più dipendenti dal citato elenco e il soggetto provvede nel senso tempestivamente.	

REGIONE BASILICATA
Ufficio Speciale per l'Amministrazione Digitale

Strategia regionale per il Cloud ed iniziative in linea con i requisiti AGID-ACN

Data Center Unico Regionale e cloud computing per la digital trasformation della Pubblica Amministrazione Locale della Basilicata, obiettivo per il periodo 2023-2026 100% dei servizi migrati in cloud in coerenza con la sostenibilità dei costi.

Posizionamento della strategia regionale rispetto alle iniziative dell'Agenzia per la Cybersicurezza Nazionale per la qualificazione dei Servizi Cloud e delle Infrastrutture dei Servizi Cloud.

18/01/2023

REGIONE BASILICATA
Ufficio Speciale per l'Amministrazione Digitale

Obiettivo generale:

2026 100% dei servizi della PAL Regionale verranno migrati in cloud realizzando un ecosistema che garantisce la sostenibilità dei costi di gestione.
In nostro patrimonio di conoscenze sviluppato dal 2000 ad oggi non può essere disperso, la Regione Basilicata ha svolto un ruolo di garanzia per l'innovazione nella PAL garantendo i servizi IT nei diversi settori di riferimento coinvolgendo tutti gli attori del territorio :

SETTORE	SERVIZI
SANITA'	SISTEMA INFORMATIVO SANITARIO UNICO REGIONALE; GigaRUPAR, strutture sanitarie connesse a 100 Gbps;
SERVIZI AL CITTADINO	HOSTING ED HOUSING DEI SISTEMI PER TUTTI GLI ENTI DEL TERRITORIO; PORTALE REGIONALE DEI SERVIZI, BANDI, AVVISI, GARE, FORMAZIONE, AGRICOLTURA ETC…
AMBIENTE e TERRITORIO	SISTEMA INFORMATIVO UNICO REGIONALE DEI DATI TERRITORIALI
ACQUA	HOUSING DEL SISTEMA INFORMATIVO UNICO DEI SERVIZI DI ACQUEDOTTO LUCANO

- ✓ LO STRUMENTO CARDINE E' STATO IL DATA CENTER GESTITO DIRETTAMENTE DALLA REGIONE
- ✓ IL MODELLO DI SOSTENIBILITA' E' BASATO SULL'UTILIZZO SAPIENTE DELLE RISORSE FINANZIARIE RINVENIENTI DAL **FESR, FSC** E **PNNR** A VANTAGGIO DI TUTTA LA COMUNITA' REGIONALE PER EVITARE SPRECHI E RIDONDANZE

REGIONE BASILICATA
Ufficio Speciale per l'Amministrazione Digitale

Contesto e stato dell'arte:

Il Programma Operativo FESR 2014-2020

Asse 2:	**Agenda Digitale**
Priorità d'investimento:	2C - Rafforzare le applicazioni delle TIC per l'e-government, l'e-learning, l'e-inclusione, l'e-culture e l'e-health
Obiettivo specifico 2C.2.2:	Digitalizzazione dei processi amministrativi e diffusione di servizi digitali pienamente interoperabili
Azione 2C.2.2.1:	Soluzioni tecnologiche per la digitalizzazione e l'innovazione dei processi interni dei vari ambiti della pubblica amministrazione nel quadro del sistema pubblico di connettività, quali ad esempio la giustizia (informatizzazione del processo civile), la sanità, il turismo, le attività e i beni culturali, i servizi alle imprese
Intervento	**DGR 1346 del 20 Dicembre 2018** che prevede, entro il 2023, la realizzazione dell'intervento per in importo complessivo di **€.11.071.200**
Tipologie indicative di beneficiari:	Regione Basilicata, PPP
Principi guida:	• superamento della frammentarietà nella raccolta, condivisione e ***conservazione in piena sicurezza*** dei dati; • realizzazione del paradigma del ***Cloud Computing*** per l'erogazione di servizi pubblici; • grado di razionalizzazione dei data center esistenti e di certificazione del ***Nuovo Data center***;
Indicatori:	• **SP05:** Numero di Data center realizzati: 1 • **SP10:** Numero di Amministrazioni collegate al Datacenter: 136 • **R14**: Percentuale di Amministrazioni pubbliche collegate al Datacenter: 80%

Questionario Agid del 2019, attraverso il quale è stata presa in esame dettagliatamente la situazione del data center regionale che, sulla base della precedente indagine fatta dalla stessa AGID nel 2017, era stato classificato in gruppo B. L'indagine è stata fatta in modo congiunto con il personale dell'Agid, e la stessa Agid, a mezzo di comunicazione del Direttore Generale, ha comunicato alla Regione l'esito positivo delle verifiche tecniche svolte dai competenti uffici AgID, confermando la coerenza della proposta del **NUOVO DATA CENTER REGIONALE** con la Strategia nazionale "Crescita digitale" e il Piano Triennale dell'Informatica nella PA ed **inserendolo tra i Poli Strategici Nazionali**.

REGIONE BASILICATA
Ufficio Speciale per l'Amministrazione Digitale

LA SFIDA CHE CI ATTENDE

COMPLETARE GLI INTERVENTI CHE A CAUSA DELL'EMERGENZA COVID HANNO SUBITO UN RALLENTAMENTO:

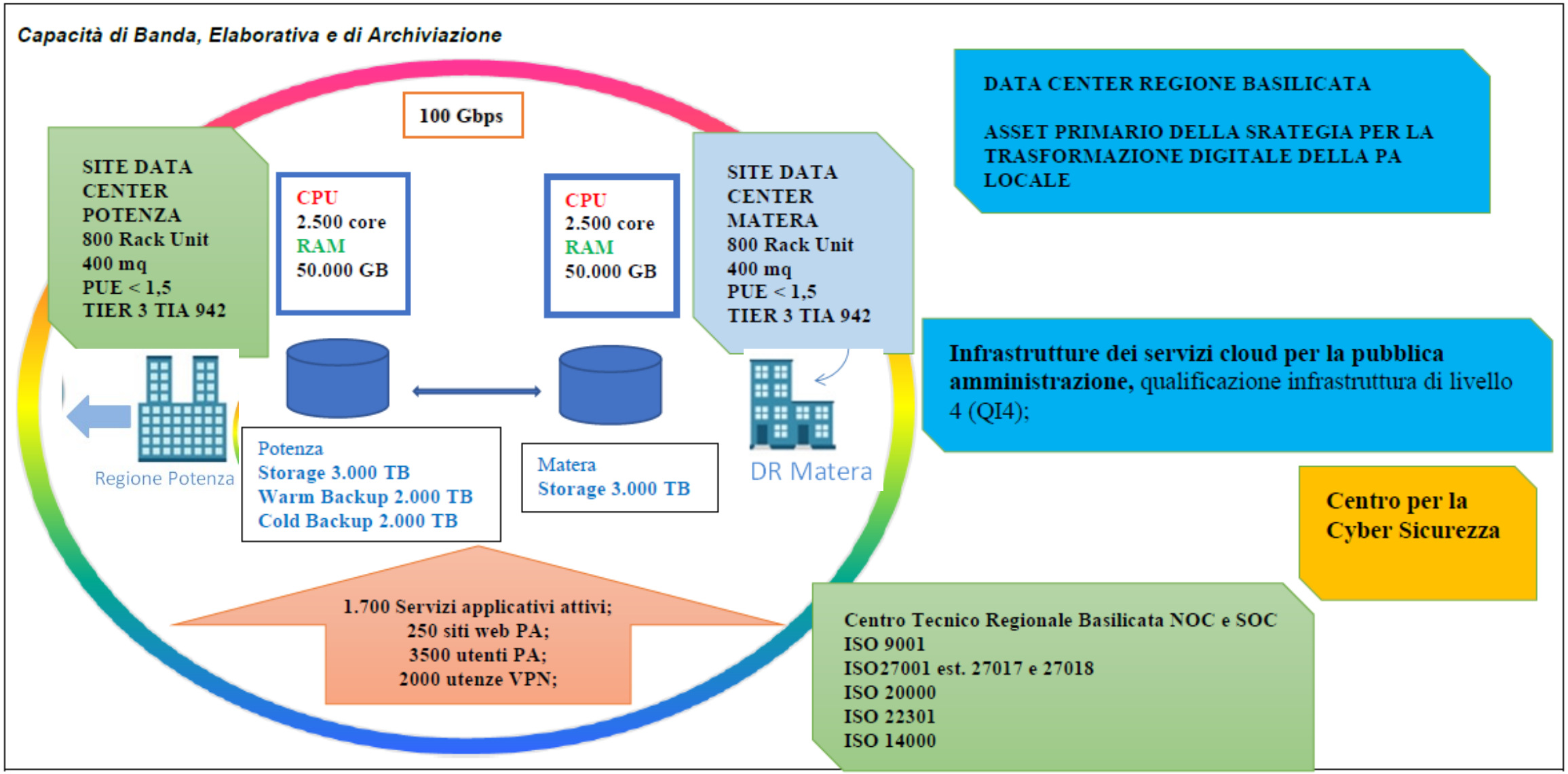
- entro la fine del 2023 **DATA CENTER DI CLASSE A++ E CONSEGUIMENTO DELLA QUALIFICAZIONE ACN DI LIVELLO QC4 E QI4** con oneri di investimento tutti a carico della Regione Basilicata (FSC, FESR, PNNR);

- entro la fine del 2024 migrare sul Cloud Regionale il 75% dei servizi della PAL Basilicata con oneri tutti in carico alla Regione Basilicata ovvero con l'utilizzo delle risorse assegnate ai Comuni e alla Aziende Sanitarie nell'ambito del PNNR;

- entro la fine del 2025 completare la migrazione al 100% ed avvio del modello di ripartizione degli oneri di gestione con le altre PAL Basilicata per garantire un adeguata sostenibilità.

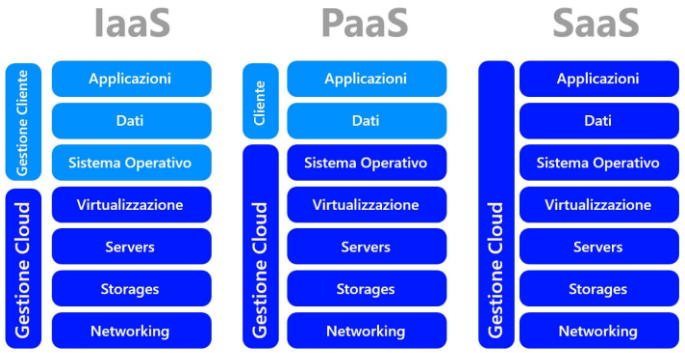
2021	2022	2023	2024	2025
• Progettazione del nuovo Data Center TIA 942 Certificazione	• Affidamento dei lavori nuovo Data Center Tier 3 • Potenziamento risorse di elaborazione e sicurezza • GigaRUPAR 100 Gbps	• Consegna dei lavori nuovo Data Center Tier 3 PZ+MT • Nuovo Centro di Gestione SOC e NOC, Qualificazione ACN GC4/QI4	• Migrazione Cloud 75% dei servizi • Centro per la Cyber Sicurezza	• Migrazione Cloud 100 % dei servizi PAL con partecipazione di tutti i beneficiari, partenariato con i privati per la sostenibilità

INFRASTRUTTURA CLOUD PER LA PAL DELLA REGIONE BASILICATA



REGIONE BASILICATA
Ufficio Speciale per l'Amministrazione Digitale

INFRASTRUTTURA CLOUD PER LA PAL DELLA REGIONE BASILICATA

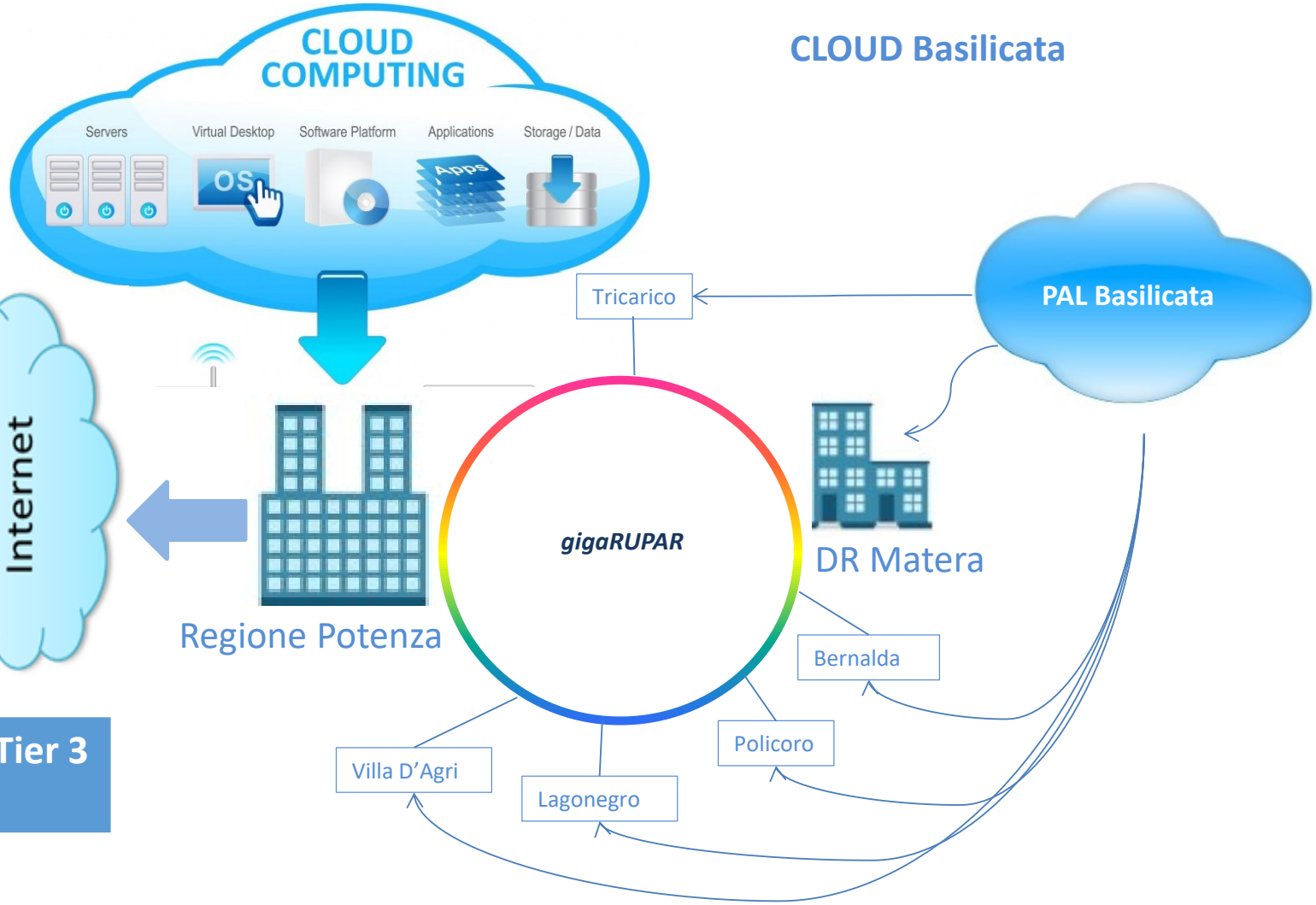


Capacità elaborativa
2.500 core CPU
50 TB RAM
3.000 TB HD

ACN qualificazione QC4 e QI4

Data Center Security ANSI/TIA 942 Tier 3
Sito Potenza e Sito Matera

CLOUD Basilicata



REGIONE BASILICATA
Ufficio Speciale per l'Amministrazione Digitale

DATA CENTER SITO PRIMARIO DI POTENZA

Figura 3 - foto aerea

REGIONE BASILICATA
Ufficio Speciale per l'Amministrazione Digitale

DATA CENTER SITO Disaster Recovery DI MATERA

1.000 Rack Unit

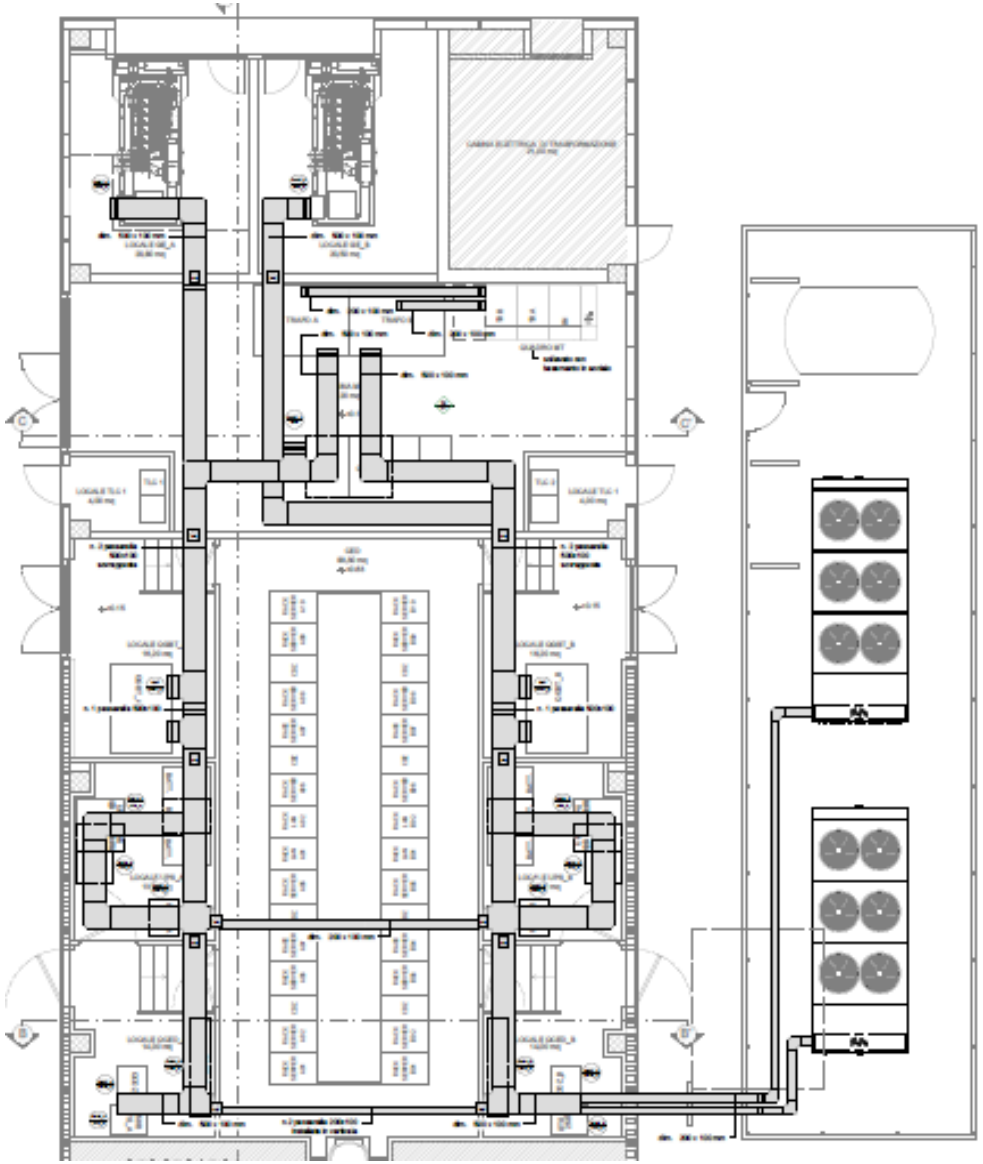


Figura 3 - foto aerea

I beneficiari diretti del progetto

SOGGETTI COINVOLTI NEL PROGETTO				
ENTE	**SPAZI DA CONSOLIDARE**	**SUPERFICE OCCUPATA**	**MQ**	**TOTALE MQ**
Regione Basilicata	**Data Center primario** presso il palazzo della Giunta regionale in Via Verrastro 4, Potenza	Sala A (piano -1)	132,47	**345,66**
		Sala B (piano 0)	41,25	
		Sala Centro stella	42,82	
		Sala CTR 1	85,26	
		Sala CTR 2	43,86	
Aziende sanitarie e ospedaliere	**Data Center secondario** presso Azienda Sanitaria di Matera, via Montescaglioso, Matera	Sala server	50,00	**50,00**
	Aziende Sanitaria Potenza	Sala Server sede Potenza	35	**50,00**
		Sala Server sede Venosa	15	
	Ospedale San Carlo	Sala Server SIO	63	**63,00**
	IRCCS (CROB)	Sala Server CROB	25	**25,00**
Comuni	Comuni (67) con meno di 2.000 abitanti *(comuni censiti: 50)*	Sala server	11	**737,00**
	Comuni (53) con più di 2.000 abitanti e <10.000 *(comuni censiti: 2)*	Sala server	11	**583,00**
	Comuni (9) con più di 10.000 ab. e <50.000 *(Comuni censiti: 1)*	Sala server	11	**99,00**
	Comuni (2) con più di 50.000 abitanti *(Comuni censiti: 1)*	Sala server	25	**50,00**
Enti Vigilati (10), Enti interregionali(1), Consorzi (6), Società Partecipate (6), Fondazioni (7)	Acquedotto Lucano	Sala Server sede Potenza	35	**65,00**
		Sala Server sede Matera	30	
	FARBAS	Sala Server sede Potenza	35	**35,00**
	ARLAB	Sala Server sede Potenza	30	**30,00**
	Gli altri (9+1+6+5+6)		15	**315,00**
			TOTALE	**2447,66**

REGIONE BASILICATA
Ufficio Speciale per l'Amministrazione Digitale

I beneficiari diretti del progetto

SOGGETTI COINVOLTI NEL PROGETTO DI RAZIONALIZZAZIONE	
ENTE	**Numero complessivo**
Regione	1
Comuni	131
Aziende sanitarie e ospedaliere	4
Enti Vigilati (10), Enti interregionali(1), Consorzi (6), Società Partecipate (6), Fondazioni (7)	30
TOTALE	**166**

Nel corso del 2019, sono stati effettuati una serie di questionari volti a verificare il grado di informatizzazione delle PA lucane. In prima battura sono state analizzate le amministrazioni che, più di tutte, hanno necessità di un sostegno da parte della Regione per sopperire a quelle lacune infrastrutturali difficilmente colmabili per via delle esigue disponibilità finanziarie.
A 67 comuni lucani, quelli con minor numero di abitanti, è stata proposta la compilazione di un **questionario** riguardante lo stato delle dotazioni tecnologiche, dei servizi telematici erogati ai propri cittadini, della connettività utilizzata, della spesa ICT sostenuta, dei sistemi e procedure di sicurezza adottati ecc.
Parallelamente è stata analizzata la situazione delle **4 aziende sanitarie/ospedaliere** che, insieme alla Regione Basilicata, presentano rispetto ai comuni condizioni di maggior complessità e carico di risorse elaborative.
L'indagine sui comuni è poi proseguita a 360 gradi, attraverso la compilazione di un'indagine **ISTAT** a cui hanno aderito, quasi la totalità dei comuni, in una percentuale pari al 93%.
A conclusione di queste attività di indagine vi è stato infine il **questionario Agid del 2019**, attraverso il quale è stata presa in esame dettagliatamente la situazione del data center regionale che, sulla base della precedente indagine fatta dalla stessa AGID nel 2017, era stato classificato in gruppo B. L'indagine è stata fatta in modo congiunto con il personale dell'Agid, e la stessa Agid, a mezzo di comunicazione del Direttore Generale, ha comunicato alla Regione l'esito positivo delle verifiche tecniche svolte dai competenti uffici AgID, confermando la coerenza della proposta del **nuovo data center regionale** con la Strategia nazionale "Crescita digitale" e il Piano Triennale dell'Informatica nella PA ed **inserendolo tra i Poli Strategici Nazionali**.