- IDENTIFY (ID)
  - 2.4.1) 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-01: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione (continuazione)
      - 2_O. Tutti i sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete è consentito esclusivamente a quelli approvati.
    - ID.AM-02: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione
      - 1_O. Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto.
      - 2_O. L'installazione delle piattaforme e delle applicazioni software è consentita esclusivamente per quelle approvate.
      - 3_O. Esistono politiche che limitino l'aggiunta, rimozione o aggiornamento, nonché la gestione non autorizzata degli asset dell'organizzazione.
    - ID.AM-03: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati
      - 1_O. Tutti i flussi di dati e di informazioni, inclusi quelli verso l'esterno e relativi al servizio cloud, sono identificati, censiti e approvati da attori interni al soggetto.
    - ID.AM-06: 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_O. 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.
      - 2_O. È nominato, nell'ambito dell'articolazione di cui al punto 1_O., 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.
      - 3_O. Sono nominati, nell'ambito dell'articolazione di cui al punto 1_O., 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.
      - 4_O. L'incaricato di cui al punto 2_O. e il referente tecnico di cui al punto 3_O. operano in stretto raccordo.
  - 2.4.2) 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-01: È identificata e resa nota una policy di cybersecurity
      - 1_O. Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di cybersecurity.
      - 2_O. Il Documento di cui al punto 1_O. deve essere approvato dal soggetto e aggiornato almeno su base annuale o in corrispondenza di sostanziali variazioni all'interno dell'organizzazione.
    - ID.GV-04: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity
      - 1_O. I documento aggiornato che descrive i processi di gestione del rischio include la parte relativa ai rischi legati alla cybersecurity.
      - 2_O. 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 del cloud.
  - 2.4.3) 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-01: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate
      - 1_O. 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.
      - 2_O. 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).
    - ID.RA-05: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio
      - 1_O. 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.
      - 2_O. L'analisi del rischio tiene conto delle dipendenze interne ed esterne del servizio cloud.
      - 3_O. Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.
  - 2.4.4) 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-01: 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_O. Sono definiti i processi di gestione del rischio inerente la catena di approvvigionamento cyber.
      - 2_O. Tali processi sono validati e approvati da parte dei vertici del soggetto.

- 2.4.5) 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-01: Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza
    - 1_O. Le credenziali di accesso sono individuali per il personale del soggetto o comunque coinvolto nell'amministrazione del servizio e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.
    - 2_O. Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1_O., le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione.
    - 3_O. Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso.
    - 4_O. Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es., trasferimento di personale).
    - 5_O. Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza.
    - 6_O. Esiste una pianificazione aggiornata degli audit di sicurezza per verificare il rispetto di quanto previsto nei punti 1_O., 2_O., 3_O., 4_O. e 5_O. ed esiste un registro degli audit effettuati con la relativa documentazione.
  - PR.AC-03: L'accesso remoto alle risorse è amministrato
    - 1_O. Gli accessi da remoto effettuati sono monitorati da parte dell'organizzazione di cybersecurity.
    - 2_O. 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.
    - 3_O. 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.
    - 4_O. Esiste un log degli accessi eseguiti da remoto.
    - 5_O. Per gli accessi da remoto, sono impiegati modalità di autenticazione a fattore multiplo.
  - PR.AC-04: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni
    - 1_O. 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.
    - 2_O. 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.
    - 3_O. 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.
  - PR.AC-05: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)
    - 1_O. Sono presenti politiche e procedure per la sicurezza dell'infrastruttura di rete, le quali dovranno essere aggiornate almeno su base annuale.
    - 2_O. 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.

- PROTECT (PR)
  - PR.AC-07: Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti del soggetto, 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_O. 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.
    - 2_O. 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 all'Agenzia per la Cybersicurezza Nazionale (ACN) e all'Amministrazione informazioni trasparenti in merito alle funzionalità di autenticazione a più fattori disponibili, con specifiche sui meccanismi adoperati per l'autenticazione (es. e-mail, sms o check biometrico).
  - 2.4.6) 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-01: Il personale del soggetto è informato e addestrato
      - 1_O. 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.
      - 2_O. L'addestramento e la formazione di cui al punto 1_O. 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;
        c. la definizione di ruoli e delle responsabilità;
        d. politiche di accesso a sistemi, asset e risorse;
        e. politiche di gestione delle informazioni e della sicurezza;
        f. processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi;
        g. requisiti per la non divulgazione/confidenzialità di informazioni.
    - PR.AT-02: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità
      - 1_O. Sono definiti i contenuti dell'istruzione fornita al personale del soggetto con privilegi e le modalità di verifica dell'acquisizione dei contenuti.
      - 2_O. Sono definiti, per ogni membro del personale del soggetto, i privilegi e le istruzioni ricevute.
  - 2.4.7) 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-01: I dati memorizzati sono protetti (continuazione)
      - 2_O. Diversamente dal caso dei Metadata relativi al funzionamento del Servizio, che possono essere trattati mediante infrastrutture localizzate anche al di fuori del territorio dell'Unione europea, i Metadata relativi all'amministrazione sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea, salvo motivate e documentate ragioni di natura normativa o tecnica. In tal caso, l'applicazione della misura ID.RA-05 deve tenere opportunamente conto della localizzazione al di fuori del territorio europeo, verificando altresì la compliance rispetto alla normativa in tema di protezione dei dati personali. In caso di trasferimento di Metadata verso infrastrutture extra-UE, l'interruzione di tale flusso di comunicazione non deve comportare comunque il mancato rispetto dei livelli minimi di servizio previsti per il servizio cloud.
      - 3_O. Con riferimento al punto 2_O., nel caso in cui i Metadata relativi all'amministrazione siano finalizzati all'erogazione di servizi per la sicurezza informatica ovvero per la resilienza dell'infrastruttura digitale, essi possono essere trattati, in presenza di motivate ragioni tecniche e relative evidenze di una loro gestione conforme all'univocità delle finalità del trattamento, anche fuori del territorio europeo. In tal caso, l'applicazione della misura ID.RA-05 deve tenere opportunamente conto della localizzazione al di fuori del territorio europeo, verificando altresì la compliance rispetto alla normativa in tema di protezione dei dati personali. In caso di trasferimento di metadata verso infrastrutture extra-UE, l'interruzione di tale flusso di comunicazione non deve comportare comunque il mancato rispetto dei livelli minimi di servizio previsti per il servizio cloud.
      - 4_O. 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.
      - 5_O. Con riferimento alle chiavi crittografiche:
        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. 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.
      - 6_O. Con riferimento alle chiavi crittografiche, su richiesta dell'amministrazione, il soggetto garantisce:
        a. la gestione autonoma da parte dell'amministrazione;
        b. la generazione di chiavi crittografiche segrete e private per uno scopo unico.
      - 7_O. 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, coerentemente con quanto previsto nei punti 5_O. e 6_O..
      - 8_O. 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 crittografiche, coerentemente con quanto previsto nei punti 5_O. e 6_O..
    - PR.DS-02: I dati sono protetti durante la trasmissione
      - 1_O. 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.
    - PR.DS-03: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale
      - 1_O. Sono definite in relazione alla categoria ID.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.
    - PR.DS-05: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)
      - 1_O. 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.
      - 2_O. Sono adottate politiche di Data Loss Prevention coerentemente con la valutazione dei rischi.
    - PR.DS-06: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni
      - 1_O. Sono definiti 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.
    - PR.DS-07: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione
      - 1_O. Sono definite in relazione alla categoria ID.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;
        c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
  - PR.IP-01: 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_O. 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].

- **2.1 Interoperabilità e portabilità**
  - 2.1.1) Interoperabilità
    - IP.IN-01: Sono disponibili API per funzionalità applicative
      - 1_O. Il 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].
  - 2.1.2) Gestione remota
    - IP.GR-01: Sono disponibili API per la gestione remota del ciclo di vita del servizio
      - 1_O. Coerentemente con la tipologia di servizio cloud erogato, l'ambiente dello stesso 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.
      - 2_O. È disponibile una documentazione tecnica, fruibile dall'Amministrazione, in merito alle API esposte e gli endpoint SOAP e/o REST.
      - 3_O. Con riferimento ai punti 1_O. e 2_O., deve essere prevista la retrocompatibilità delle diverse versioni delle API con quella disponibile al momento della formalizzazione del contratto con l'Amministrazione acquirente.
  - 2.1.3) Portabilità
    - IP.PO-01: Sono disponibili funzionalità/API per import/export dei dati
      - 1_O. Sono disponibili funzionalità e/o API per consentire l'esportazione ed importazione massiva dei dati, garantendo l'utilizzo di formati aperti non proprietari.
    - IP.PO-02: 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_O. 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].
      - 2_O. Sono implementati protocolli di rete cifrati e standardizzati per la gestione, l'importazione e l'esportazione dei dati. [PaaS, SaaS].
      - 3_O. 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].

- **2.2 Performance e scalabilità**
  - 2.2.1) Caratteristiche del servizio
    - PS.CA-01: Il servizio cloud presenta le caratteristiche tipiche ed è conforme agli standard di settore
      - 1_O. 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.
  - 2.2.2) Scalabilità del servizio
    - PS.SC-01: Trasparenza sulle modalità e meccanismi di scalabilità
      - 1_O. Il 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).
      - 2_O. Il fornitore rende disponibili all'Amministrazione informazioni trasparenti in merito ad eventuali ulteriori funzionalità accessorie disponibili per il servizio e configurabili dall'Amministrazione acquirente per gestire la scalabilità ed ottenere parametri migliori.
      - 3_O. Per tutte le API esposte dal servizio cloud deve essere dichiarata la conformità al Modello di interoperabilità, definito da AgID con le linee guida adottate ai sensi della normativa vigente. Qualora le API esposte siano conformi, devono essere condivise le specifiche dell'API in formato machine readable compatibile con le indicazioni del modello d'interoperabilità (e.g. OpenAPI3 per le API REST, WSDL per le API SOAP).

Caratteristiche di base previste nel caso di dati e servizi ordinari

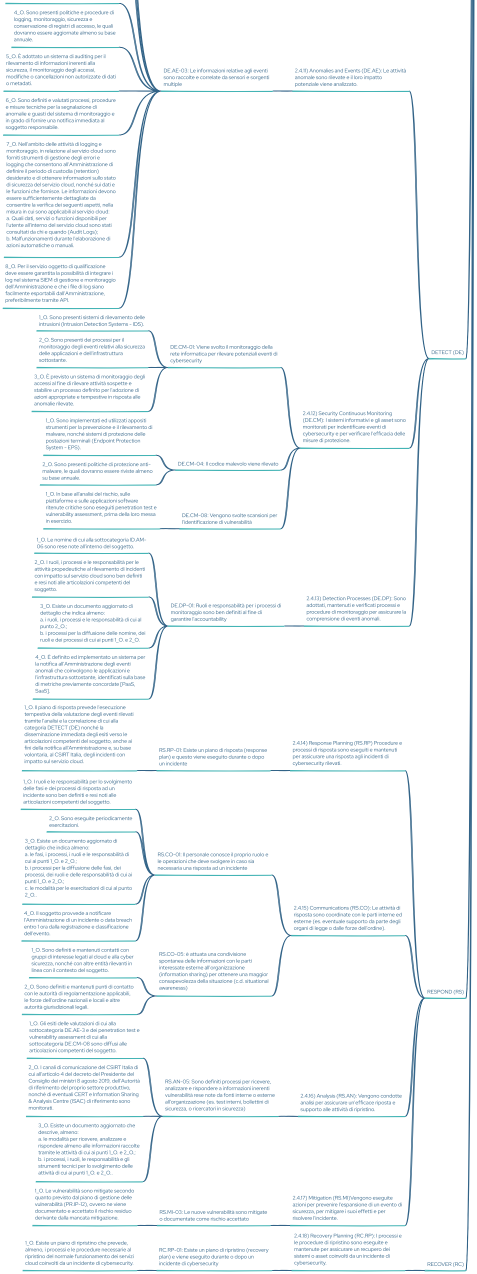
2.4 Sicurezza

- 2.4.8) 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 asset.
  - PR.IP-03: Sono attivi processi di controllo della modifica delle configurazioni
    - 1_O. 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.
    - 2_O. È implementata una procedura per la gestione delle eccezioni, incluse emergenze, nel processo di modifica e configurazione.
    - 3_O. Sono definiti e implementati piani di ripristino allo stato precedente (cd. rollback) in caso di errori o problemi di sicurezza.
  - PR.IP-04: I backup delle informazioni sono eseguiti, amministrati e verificati
    - 1_O. 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.
    - 2_Oa. Viene effettuato periodicamente un backup dei dati memorizzati nel cloud. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup.
    - 2_Ob. Viene effettuato periodicamente un backup delle informazioni memorizzate nel cloud necessarie per il completo ripristino del sistema, ivi incluso i dati dell'Amministrazione e i dati necessari per il ripristino del servizio. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup. A tal fine, viene anche assicurato che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.
    - 3_O. Le copie di backup di informazioni, software e immagini di sistema del servizio cloud sono protette adottando standard crittografici allo stato dell'arte e migliori pratiche di settore, 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 adottando standard crittografici allo stato dell'arte e migliori pratiche di settore.
    - 4_O. Viene verificato periodicamente il ripristino (test di restore) delle copie di backup come obiettivo (SLO) almeno 1 volta all'anno.
  - PR.IP-09: 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_O. 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.
    - 2_O. 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.
    - 3_O. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.
    - 4_O. I piani di business continuity sono collaudati e comunicati alle parti interessate.
    - 5_O. La documentazione di cui al punto 2_O. è resa disponibile, ove richiesto, all'Amministrazione e rivista periodicamente.
  - PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità
    - 1_O. 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.
    - 2_O. 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].
- 2.4.9) 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-01: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati
    - 1_O. 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.
  - PR.MA-02: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati
    - 1_O. 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-03 e dei seguenti punti.
    - 2_O. Tutti gli accessi eseguiti da remoto da personale di terze parti sono autorizzati dall'organizzazione di cybersecurity e limitati ai soli casi essenziali.
    - 3_O. Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi.
    - 4_O. Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili.
    - 5_O. 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.
- 2.4.10) 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-01: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi
    - 1_O. I log son conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi.
    - 2_O. 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.
  - PR.PT-04: Le reti di comunicazione e controllo sono protette
    - 1_O. I sistemi perimetrali, quali firewall, anche a livello applicativo (ivi inclusi Web Application Firewall), sono presenti, aggiornati, manutenuti e ben configurati.
  - PR.PT-05: 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_O. In relazione ai piani previsti dalla sottocategoria PR.IP-09:
      a. sono adottate architettura ridondate di rete, di connettività, nonché applicative.
    - 2_O. Esistono meccanismi per garantire la continuità di servizio, nel rispetto delle misure di sicurezza previste.
    - 3_O. Sono definite:
      a. le politiche di sicurezza adottate in relazione ai punti 1_O. e 2_O;
      b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

- 1_O. 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 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. e b., per rilevare tempestivamente eventi di interesse.
- 2_O. Le attività di analisi e correlazione di cui al punto precedente sono monitorate e registrate. La documentazione relativa alle attività di analisi e investigazione dell'evento, anche elettronica, e conservata per almeno 24 mesi.
- 3_O. Sono definite:
  a. le politiche applicate per individuare i sensori e le sorgenti di cui al punto 1_O., lettera a.;
  b. le procedure e gli strumenti tecnici per ottenere le informazioni di cui al punto 1_O., lettere a. e b.;
  c. le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui al punto 1_O., lettera c-;
  d. i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al punto 2_O.

2.3 Qualità

- 2.3.1) Livello del servizio (SLA)
  - QU.LS-01: 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_O. Il soggetto garantisce l'aderenza agli obiettivi (Minimum Service Level Objective - SLO) corrispondenti ai seguenti indicatori di servizio (Service Level Indicator - SLI) e ne garantisce il rispetto nei rapporti contrattuali nella forma di accordi relativi ai livelli di servizio (SLA):
      a. disponibilità pari al 99%, dove la disponibilità è intesa come la percentuale di tempo in un mese in cui il servizio cloud risulta essere accessibile e usabile, specificando che il tempo totale del periodo di riferimento, che funge da base di calcolo del dato percentuale, non tiene conto degli eventi catastrofici (per eventi catastrofici si intendono eventi che rendono indisponibili per un periodo di tempo prolungato le infrastrutture impiegate per l'erogazione del servizio e al verificarsi dei quali è attivata la soluzione di Disaster Recovery);
      b. "supporto tecnico per emergenze", relativo all'orario in cui il servizio di supporto tecnico è operativo per emergenze: 24 ore al giorno, 7 giorni a settimana per tutto l'anno;
      c. un tempo massimo di risposta agli incidenti (inteso come tempo massimo che intercorre tra la segnalazione di un evento con impatto critico sull'operatività dell'Amministrazione e la risposta da parte del soggetto) pari a 1 ora;
      d. "minor release", inteso come l'intervallo di tempo minimo di preavviso previsto per dare comunicazione, accompagnata da release note, alla Amministrazione di Minor Release (per Minor Release si intendono modifiche al servizio che riguardano principalmente correzioni di malfunzionamenti del software - bug - o comunque aggiunta di nuove funzionalità retro compatibili): 3 giorni;
      e. "major release", inteso come l'intervallo di tempo minimo di preavviso previsto per dare comunicazione, accompagnata da release note, alla Amministrazione di Major Release (per Major Release si intendono modifiche al servizio che riguardano una sostanziale evoluzione delle funzionalità del servizio rispetto alla versione precedente): 1 mese.
    - 2_O. Rispetto a quelli riportati al punto 1_O., il soggetto può comunicarne all'amministrazione eventuali ulteriori, o indicarne di nuovi, che potranno essere inseriti come impegni contrattuali con specifici Minimum Service Level Objective (SLO) nei rapporti contrattuali.
    - 3_O. 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.
  - QU.LS-02: Esistono limitazioni per i Service Level Agreement (SLA) per prevenire impatti sugli ambienti dell'Amministrazione
    - 1_O. 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.
  - QU.LS-03: Esistono contenuti e caratteristiche minimi per i Service Level Agreement
    - 1_O. 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 Model, se applicabile);
      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. Modalità di cessazione del servizio;
      h. Requisiti di interoperabilità e portabilità;
      i. Riservatezza dei dati.
  - QU.LS-04: È disponibile un servizio di monitoraggio (allarmi e parametri) e sono rese note eventuali integrazioni native con soluzioni leader di mercato
    - 1_O. 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.
- 2.3.2) Qualità del servizio (SE)
  - QU.SE-01: Sono adottati sistemi per la gestione del servizio IT e della qualità conformemente agli standard di settore
    - 1_O. Il sistema di gestione della qualità del servizio cloud è adottato formalmente dal soggetto in conformità allo standard UNI EN ISO 9001:2015-Sistemi di Gestione per la Qualità.
    - 2_O. 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 IT.
  - QU.SE-02: Viene fornito un adeguato servizio di assistenza e supporto
    - 1_O. È garantito il servizio di supporto e assistenza tecnica all'amministrazione per il servizio cloud.
    - 2_O. Il servizio di supporto e assistenza di cui al punto 1_O. è fornito almeno in lingua inglese dalle 08.00 alle 18.00 (ora italiana) nei giorni lavorativi. Su richiesta dell'Amministrazione, il servizio di supporto e assistenza di cui al punto 1_O. è fornito almeno in lingua italiana e/o per un orario più esteso fino a coprire tutti giorni dell'anno a qualsiasi orario (24 ore al giorno, 7 giorni alla settimana per tutto l'anno).
    - 3_O. Il servizio di supporto e assistenza di cui al punto 1_O. è accessibile almeno tramite recapito telefonico e posta elettronica.
    - 4_O. Il servizio di supporto e assistenza di cui al punto 1_O. prevede, inoltre, un sistema di supporto alla risoluzione dei problemi (detto anche "troubleshooting") a disposizione dell'Amministrazione, rendendolo disponibile, su richiesta dell'amministrazione, tramite API al fine di permettere l'interazione programmatica con i sistemi di gestione dei problemi (Case Management System).
  - QU.SE-03: Il soggetto dichiara la frequenza di aggiornamento del servizio
    - 1_O. Il soggetto deve dichiarare la frequenza attesa di aggiornamento del servizio cloud qualificato (es. periodicità rilasci pianificati).
  - QU.SE-04: Linee guida e raccomandazioni sull'uso sicuro di soluzioni cloud
    - 1_O. 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.



- DETECT (DE)
  - 2.4.11) Anomalies and Events (DE.AE): Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.
    - DE.AE-03: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple
      - 4_O. Sono presenti politiche e procedure di logging, monitoraggio, sicurezza e conservazione di registri di accesso, le quali dovranno essere aggiornate almeno su base annuale.
      - 5_O. 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.
      - 6_O. 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.
      - 7_O. 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.
      - 8_O. 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.
  - 2.4.12) 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-01: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity
      - 1_O. Sono presenti sistemi di rilevamento delle intrusioni (Intrusion Detection Systems - IDS).
      - 2_O. Sono presenti dei processi per il monitoraggio degli eventi relativi alla sicurezza delle applicazioni e dell'infrastruttura sottostante.
      - 3_O. È previsto un sistema di monitoraggio 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.
    - DE.CM-04: Il codice malevolo viene rilevato
      - 1_O. Sono implementati ed utilizzati appositi strumenti per la prevenzione e il rilevamento di malware, nonché sistemi di protezione delle postazioni terminali (Endpoint Protection System - EPS).
      - 2_O. Sono presenti politiche di protezione anti-malware, le quali dovranno essere riviste almeno su base annuale.
    - DE.CM-08: Vengono svolte scansioni per l'identificazione di vulnerabilità
      - 1_O. 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.
  - 2.4.13) Detection Processes (DE.DP): Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.
    - DE.DP-01: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability
      - 1_O. Le nomine di cui alla sottocategoria ID.AM-06 sono rese note all'interno del soggetto.
      - 2_O. I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sul servizio cloud sono ben definiti e resi noti alle articolazioni competenti del soggetto.
      - 3_O. Esiste un documento aggiornato di dettaglio che indica almeno:
        a. i ruoli, i processi e le responsabilità di cui al punto 2_O.;
        b. i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti 1_O. e 2_O.
      - 4_O. 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 [PaaS, SaaS].
- RESPOND (RS)
  - 2.4.14) Response Planning (RS.RP) Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.
    - RS.RP-01: Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente
      - 1_O. Il piano di risposta prevede l'esecuzione tempestiva della valutazione degli eventi rilevati tramite l'analisi e la correlazione di cui alla categoria DETECT (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.
  - 2.4.15) 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-01: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente
      - 1_O. I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di risposta ad un incidente sono ben definiti e resi noti alle articolazioni competenti del soggetto.
      - 2_O. Sono eseguite periodicamente esercitazioni.
      - 3_O. Esiste un documento aggiornato di dettaglio che indica almeno:
        a. le fasi, i processi, i ruoli e le responsabilità di cui ai punti 1_O. e 2_O.;
        b. i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilità di cui ai punti 1_O. e 2_O.;
        c. le modalità per le esercitazioni di cui al punto 2_O..
      - 4_O. Il soggetto provvede a notificare l'Amministrazione di un incidente o data breach entro 1 ora dalla registrazione e classificazione dell'evento.
    - RS.CO-05: 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 awarenesss)
      - 1_O. Sono definiti e mantenuti contatti con gruppi di interesse legati al cloud e alla cyber sicurezza, nonché con altre entità rilevanti in linea con il contesto del soggetto.
      - 2_O. 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.
  - 2.4.16) Analysis (RS.AN): Vengono condotte analisi per assicurare un'efficace riposta e supporto alle attività di ripristino.
    - RS.AN-05: 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_O. Gli esiti delle valutazioni di cui alla sottocategoria DE.AE-3 e dei penetration test e vulnerability assessment di cui alla sottocategoria DE.CM-08 sono diffusi alle articolazioni competenti del soggetto.
      - 2_O. 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 Sharing & Analysis Centre (ISAC) di riferimento sono monitorati.
      - 3_O. 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_O. e 2_O.;
        b. i processi, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1_O. e 2_O..
  - 2.4.17) Mitigation (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-03: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato
      - 1_O. 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.
- RECOVER (RC)
  - 2.4.18) 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-01: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity
      - 1_O. 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.