

ALLEGATO 2

Misure di sicurezza di base per i soggetti essenziali

1. GOVERNO (GOVERN)

- 1.1. **Contesto organizzativo (GV.OC):** Il contesto – missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali – che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso¹.
 - 1.1.1. **GV.OC-04:** Gli obiettivi, le capacità e i servizi critici dai quali gli stakeholder dipendono o che si aspettano dall'organizzazione sono compresi e comunicati.
 - 1. È mantenuto un elenco aggiornato dei sistemi informativi e di rete rilevanti.
- 1.2. **Strategia di gestione del rischio (GV.RM):** Le priorità, i vincoli, le dichiarazioni sulla tolleranza e la propensione al rischio, e le assunzioni dell'organizzazione sono stabilite, comunicate e utilizzate per supportare le decisioni sul rischio operativo.
 - 1.2.1. **GV.RM-03:** Le attività e gli esiti della gestione del rischio di cybersecurity sono parte integrante dei processi di gestione del rischio dell'organizzazione.
 - 1. Nell'ambito dei processi di gestione del rischio del soggetto NIS e nel rispetto delle politiche di cui alla misura GV.PO-01, è definito, attuato, aggiornato e documentato un piano di gestione dei rischi per la sicurezza informatica per identificare, analizzare, valutare, trattare e monitorare i rischi.
- 1.3. **Ruoli, responsabilità e correlati poteri (GV.RR):** Sono stabiliti e comunicati i ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo.
 - 1.3.1. **GV.RR-02:** I ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati.
 - 1. È definita, approvata dagli organi di amministrazione e direttivi, e resa nota alle articolazioni competenti del soggetto NIS, l'organizzazione per la sicurezza informatica e ne sono stabiliti ruoli e responsabilità.
 - 2. È mantenuto un elenco aggiornato del personale dell'organizzazione di cui al punto 1 avente specifici ruoli e responsabilità ed è reso noto alle articolazioni competenti del soggetto NIS.
 - 3. All'interno dell'organizzazione per la sicurezza informatica di cui al punto 1, sono inclusi il punto di contatto e il suo sostituto, il referente CSIRT e gli eventuali suoi sostituti, di cui alla determinazione adottata ai sensi dell'articolo 7, comma 6 del decreto NIS.
 - 4. I ruoli e le responsabilità di cui al punto 1 sono riesaminati e, se opportuno, aggiornati periodicamente e comunque almeno ogni due anni, nonché qualora si verificano incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

¹ Per ragioni di coerenza con i titoli delle categorie e sottocategorie del Framework nazionale sono stati mantenuti i termini "cybersecurity" ed "organizzazione" che, nell'ambito del presente allegato, sono da intendersi, ad eccezione dell'organizzazione di sicurezza informatica, rispettivamente equivalenti alle locuzioni "sicurezza informatica" e "soggetto NIS".

1.3.2. **GV.RR-04:** La cybersecurity è inclusa nelle pratiche delle risorse umane.

1. Per almeno i sistemi informativi e di rete rilevanti, il personale autorizzato ad accedervi è individuato previa valutazione dell'esperienza, capacità e affidabilità e deve fornire idonea garanzia del pieno rispetto della normativa in materia di sicurezza informatica.
2. Gli amministratori di sistema dei sistemi informativi e di rete sono individuati previa valutazione dell'esperienza, capacità e affidabilità e devono fornire idonea garanzia del pieno rispetto della normativa in materia di sicurezza informatica.
3. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.
4. In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono definiti a livello contrattuale gli eventuali obblighi, in materia di sicurezza informatica, che rimangono validi dopo la cessazione o la modifica del rapporto di lavoro dei dipendenti del soggetto NIS (ad esempio prevedendo clausole in materia di riservatezza).
5. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 4.

1.4. **Politica (GV.PO):** La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata.

1.4.1. **GV.PO-01:** La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata.

1. Sono adottate e documentate politiche di sicurezza informatica per almeno i seguenti ambiti:
 - a) gestione del rischio;
 - b) ruoli e responsabilità;
 - c) affidabilità delle risorse umane;
 - d) conformità e audit di sicurezza;
 - e) gestione dei rischi per la sicurezza informatica della catena di approvvigionamento;
 - f) gestione degli asset;
 - g) gestione delle vulnerabilità;
 - h) continuità operativa, ripristino in caso di disastro e gestione delle crisi informatiche;
 - i) gestione dell'autenticazione, delle identità digitali e del controllo accessi;
 - j) sicurezza fisica;
 - k) formazione del personale e consapevolezza;
 - l) sicurezza dei dati;
 - m) sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;
 - n) protezione delle reti e delle comunicazioni;
 - o) monitoraggio degli eventi di sicurezza;
 - p) risposta agli incidenti e ripristino.
2. Per gli ambiti di cui al punto 1 sono incluse almeno le politiche in relazione ai requisiti indicati nella tabella 1 in appendice al presente allegato.
3. Le politiche di cui al punto 1 sono approvate dagli organi di amministrazione e direttivi e rese note alle articolazioni competenti del soggetto NIS tenuto anche conto della necessità di conoscere (need to know).

1.4.2. **GV.PO-02:** La politica per la gestione del rischio di cybersecurity è revisionata, aggiornata, comunicata e applicata per riflettere i cambiamenti nei requisiti, nelle minacce, nella tecnologia e nella missione dell'organizzazione.

1. Le politiche di cui alla misura GV.PO-01 sono riesaminate e, se opportuno, aggiornate periodicamente e comunque almeno con cadenza annuale, nonché qualora si verifichino evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.
2. Ai fini del riesame di cui al punto 1, è verificata almeno la conformità delle politiche di cui alla misura GV.PO-01 alla normativa in materia di sicurezza informatica.
3. È mantenuto un registro aggiornato contenente gli esiti del riesame di cui al punto 1.

1.5. **Gestione del rischio di cybersecurity della catena di approvvigionamento (GV.SC):** I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.

1.5.1. **GV.SC-01:** Sono stabiliti e accettati dagli stakeholder dell'organizzazione il programma, la strategia, obiettivi, politiche e processi di gestione del rischio di cybersecurity della catena di approvvigionamento.

1. In merito all'affidamento di forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, anche mediante ricorso agli strumenti delle centrali di committenza di cui all'allegato I.1, articolo 1, comma 1, lettera i), del decreto legislativo 31 marzo 2023, n. 36, sono previsti:
 - a) il coinvolgimento dell'organizzazione per la sicurezza informatica di cui alla misura GV.RR-02 nella definizione ed esecuzione dei processi di approvvigionamento a partire dalla fase di identificazione e progettazione della fornitura;
 - b) in accordo agli esiti della valutazione del rischio associato alla fornitura di cui alla misura GV.SC-07, la definizione di requisiti di sicurezza sulla fornitura coerenti con le misure di sicurezza applicate dal soggetto NIS ai sistemi informativi e di rete.
2. Per i requisiti di sicurezza di cui al punto 1, lettera b), sono considerati, ove applicabile, almeno i seguenti ambiti:
 - a) affidabilità dei fornitori, tenendo conto almeno delle loro eventuali vulnerabilità specifiche, della qualità complessiva dei loro prodotti e delle pratiche di sicurezza informatica, specie con riguardo all'oggetto della fornitura, della capacità di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo, nonché, ove applicabile, dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS;
 - b) ruoli e responsabilità nell'ambito della fornitura;
 - c) affidabilità delle risorse umane;
 - d) conformità e audit di sicurezza;
 - e) gestione delle vulnerabilità;
 - f) continuità operativa e ripristino in caso di disastro;
 - g) gestione dell'autenticazione, delle identità digitali e del controllo accessi;
 - h) sicurezza fisica;
 - i) formazione del personale e consapevolezza;
 - j) sicurezza dei dati;

- k) protezione delle reti e delle comunicazioni;
- l) monitoraggio degli eventi di sicurezza ivi inclusi gli accessi e le attività effettuate;
- m) gestione e segnalazione degli incidenti;
- n) sviluppo sicuro del codice e sicurezza fin dalla progettazione e per impostazione predefinita;
- o) manutenzione ordinaria ed evolutiva ivi inclusi gli aggiornamenti di sicurezza;
- p) dismissione della fornitura ivi compresa la restituzione e la cancellazione dei dati;
- q) subappalto, subfornitura o relativi potenziali requisiti di sicurezza lungo la catena di fornitura.

1.5.2. **GV.SC-02:** I ruoli e le responsabilità in materia di cybersecurity per fornitori, clienti e partner sono stabiliti, comunicati e coordinati internamente ed esternamente.

1. Nell'ambito dell'organizzazione per la sicurezza informatica di cui alla misura GV.RR-02, sono definiti e resi noti alle articolazioni competenti del soggetto NIS gli eventuali ruoli e responsabilità in materia di sicurezza informatica assegnati al personale delle terze parti.
2. Il personale di cui al punto 1 avente specifici ruoli e responsabilità è incluso nell'elenco di cui al punto 2 della misura GV.RR-02.

1.5.3. **GV.SC-04:** I fornitori sono noti e prioritizzati in base alla criticità.

1. È mantenuto un inventario aggiornato dei fornitori delle forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, che comprende almeno:
 - a) gli estremi di contatto del referente della fornitura;
 - b) la tipologia di fornitura.

1.5.4. **GV.SC-05:** I requisiti per affrontare i rischi di cybersecurity nella catena di approvvigionamento sono stabiliti, prioritizzati e integrati nei contratti e in altri tipi di accordi con i fornitori e altre terze parti rilevanti.

1. Fatte salve motivate e documentate ragioni normative o tecniche, i requisiti di sicurezza di cui alla misura GV.SC-01, punto 1, lettera b) sono inseriti nelle richieste di offerta, bandi di gara, contratti, accordi e convenzioni relativi alle forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete.

1.5.5. **GV.SC-07:** I rischi posti da un fornitore, dai suoi prodotti e servizi e da altre terze parti sono compresi, registrati, prioritizzati, valutati, trattati e monitorati nel corso della relazione.

1. Nell'ambito della valutazione del rischio di cui alla misura ID.RA-05, è valutato e documentato il rischio associato alle forniture. A tal fine, sono valutati almeno:
 - a) il livello di accesso del fornitore ai sistemi informativi e di rete del soggetto NIS;
 - b) l'accesso del fornitore alla proprietà intellettuale e ai dati anche sulla base della loro criticità;
 - c) l'impatto di una grave interruzione della fornitura;
 - d) i tempi e i costi di ripristino in caso di indisponibilità dei servizi;
 - e) i ruoli e le responsabilità del fornitore nel governo dei sistemi informativi e di rete.
2. È verificata periodicamente e documentata la conformità delle forniture ai requisiti di cui alla misura GV.SC-05.

2. IDENTIFICAZIONE (IDENTIFY)

- 2.1. **Gestione degli asset (ID.AM):** Gli asset (ad esempio, dati, hardware, software, sistemi, infrastrutture, servizi, persone) che consentono all'organizzazione di raggiungere gli obiettivi di business sono identificati e gestiti in coerenza con la loro importanza rispetto agli obiettivi organizzativi e alla strategia sul rischio dell'organizzazione.
- 2.1.1. **ID.AM-01:** Sono mantenuti gli inventari dell'hardware gestito dall'organizzazione.
1. È mantenuto un inventario aggiornato degli apparati fisici (hardware) che compongono i sistemi informativi e di rete, ivi inclusi i dispositivi IT, IoT, OT e mobili, approvati da attori interni al soggetto NIS.
- 2.1.2. **ID.AM-02:** Sono mantenuti gli inventari del software, dei servizi e dei sistemi gestiti dall'organizzazione.
1. È mantenuto un inventario aggiornato dei servizi, dei sistemi e delle applicazioni software che compongono i sistemi informativi e di rete, ivi incluse le applicazioni commerciali, open-source e custom, anche accessibili tramite API, approvati da attori interni al soggetto NIS.
- 2.1.3. **ID.AM-03:** Sono mantenute le rappresentazioni delle comunicazioni di rete, dei flussi di dati di rete interni ed esterni, autorizzati dall'organizzazione.
1. È mantenuto un inventario aggiornato dei flussi di rete tra i sistemi informativi e di rete del soggetto NIS e l'esterno, approvati da attori interni al soggetto NIS.
- 2.1.4. **ID.AM-04:** Sono mantenuti gli inventari dei servizi erogati dai fornitori.
1. È mantenuto un inventario aggiornato dei servizi informatici erogati dai fornitori, ivi inclusi i servizi cloud.
- 2.2. **Valutazione del rischio (Risk Assessment) (ID.RA):** È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.
- 2.2.1. **ID.RA-01.** Le vulnerabilità negli asset sono identificate, confermate e registrate.
1. Le informazioni di cui al punto 1 della misura ID.RA-08 sono utilizzate per identificare eventuali vulnerabilità sui i sistemi informativi e di rete.
 2. Per almeno i sistemi informativi e di rete rilevanti, in accordo al piano di gestione delle vulnerabilità di cui alla misura ID.RA-08, fatte salve motivate e documentate ragioni normative o tecniche, sono eseguite periodicamente e comunque prima della loro messa in esercizio, attività per l'identificazione delle vulnerabilità che comprendano almeno vulnerability assessment e/o penetration test.
 3. Le attività di cui al punto 2 sono documentate tramite apposite relazioni che contengono almeno:
 - a) la descrizione generale delle attività effettuate e gli esiti delle stesse;
 - b) la descrizione delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza.
- 2.2.2. **ID.RA-05:** Minacce, vulnerabilità, probabilità e impatti sono utilizzati per comprendere il rischio inerente e per informare la prioritizzazione della risposta al rischio.
1. In accordo al piano di gestione dei rischi per la sicurezza informatica di cui alla misura GV.RM-03, è eseguita e documentata la valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete, anche con riferimento alle eventuali dipendenze da fornitori e partner terzi, che comprende almeno:
 - a) l'identificazione del rischio;

- b) l'analisi del rischio;
 - c) la ponderazione del rischio.
2. La valutazione del rischio di cui al punto 1 è eseguita a intervalli pianificati e comunque almeno ogni due anni, nonché qualora si verificano incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.
 3. La valutazione del rischio di cui al punto 1 è approvata dagli organi di amministrazione e direttivi.
 4. La valutazione del rischio di cui al punto 1 è effettuata considerando almeno le minacce interne ed esterne, le vulnerabilità non risolte e gli impatti conseguenti ad eventuali incidenti.

2.2.3. **ID.RA-06:** Le risposte al rischio sono scelte, priorizzate, pianificate, monitorate e comunicate.

1. È definito, documentato, eseguito e monitorato un piano di trattamento dei rischi per la sicurezza informatica che comprende almeno:
 - a) le opzioni di trattamento e le misure da attuare in merito al trattamento di ciascun rischio individuato e le relative priorità;
 - b) le articolazioni competenti per l'attuazione delle misure di trattamento dei rischi e le tempistiche per tale attuazione;
 - c) la descrizione e le ragioni che giustificano l'accettazione di eventuali rischi residui al trattamento.
2. Qualora per motivate e documentate ragioni normative o tecniche non siano attuati i requisiti di cui alla tabella 2 in appendice al presente allegato, sono adottate, ove applicabile, misure di mitigazione compensative e il piano di cui al punto 1 include la descrizione di tali misure e dell'eventuale rischio residuo.
3. Il piano di cui al punto 1, ivi compresa l'accettazione di eventuali rischi residui, è approvato dagli organi di amministrazione e direttivi.

2.2.4. **ID.RA-08:** Sono stabiliti processi per la ricezione, l'analisi e la risposta alle divulgazioni di vulnerabilità.

1. Sono monitorati almeno i canali di comunicazione del CSIRT Italia, nonché di eventuali CERT e Information Sharing & Analysis Centre (ISAC) settoriali, al fine di acquisire, analizzare e rispondere alle informazioni sulle vulnerabilità.
2. Le vulnerabilità, ivi comprese quelle identificate ai sensi della misura ID.RA-01, sono prontamente risolte attraverso aggiornamenti di sicurezza o misure di mitigazione, ove disponibili, ovvero accettando e documentando il rischio in accordo al piano di trattamento dei rischi di cui alla misura ID.RA-06.
3. È definito, attuato, aggiornato e documentato un piano di gestione delle vulnerabilità che comprende almeno:
 - a) le modalità per l'identificazione delle vulnerabilità di cui alla misura ID.RA-01 e la relativa pianificazione delle attività;
 - b) le modalità per monitorare, ricevere, analizzare e rispondere alle informazioni sulle vulnerabilità;
 - c) le procedure, i ruoli, le responsabilità per lo svolgimento delle attività di cui alle lettere a) e b).
4. Il piano di cui al punto 3 è approvato dagli organi di amministrazione e direttivi.

5. Ai fini di cui al punto 1, sono monitorati anche i canali dei fornitori del software ritenuto critico.

2.3. **Miglioramento (ID.IM):** I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.

2.3.1. **ID.IM-01:** Sono identificati miglioramenti in esito alle valutazioni.

1. In accordo agli esiti del riesame di cui al punto 1 della misura GV.PO-02, è definito, attuato, documentato e approvato dagli organi di amministrazioni e direttivi un piano di adeguamento che identifichi gli interventi necessari ad assicurare l'attuazione delle politiche di sicurezza.
2. Gli organi di amministrazione e direttivi sono informati mediante apposite relazioni periodiche sugli esiti dei piani di cui al punto 1.
3. È definito, attuato, aggiornato e documentato un piano per la valutazione dell'efficacia delle misure di gestione del rischio per la sicurezza informatica che comprenda l'indicazione delle misure da valutare e i relativi metodi di valutazione.
4. Gli organi di amministrazione e direttivi sono informati mediante apposite relazioni periodiche sul piano di valutazione dell'efficacia di cui al punto 3.

2.3.2. **ID.IM-04:** I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati.

1. Per almeno i sistemi informativi e di rete rilevanti è definito, attuato, aggiornato e documentato un piano di continuità operativa, che comprende almeno:
 - a) le finalità, ivi incluse le esigenze di continuità operativa, e l'ambito di applicazione;
 - b) i ruoli e le responsabilità;
 - c) i contatti principali e i canali di comunicazione (interni ed esterni);
 - d) le condizioni per l'attivazione e la disattivazione del piano;
 - e) le risorse necessarie, ivi compresi i backup e le ridondanze.
2. Per almeno i sistemi informativi e di rete rilevanti è definito, attuato, aggiornato e documentato un piano di ripristino in caso di disastro, che comprende almeno:
 - a) le finalità, ivi incluse le esigenze di ripristino in caso di disastro, e l'ambito di applicazione;
 - b) i ruoli e le responsabilità;
 - c) i contatti principali e i canali di comunicazione (interni ed esterni);
 - d) le condizioni per l'attivazione e la disattivazione del piano;
 - e) le risorse necessarie, ivi compresi i backup e le ridondanze;
 - f) l'ordine di ripristino delle operazioni;
 - g) le procedure di ripristino per operazioni specifiche, compresi gli obiettivi di ripristino.
3. Per almeno i sistemi informativi e di rete rilevanti è definito, attuato, aggiornato e documentato un piano per la gestione delle crisi informatiche che comprende almeno:
 - a) i ruoli e le responsabilità del personale e, se opportuno, dei fornitori, specificando l'assegnazione dei ruoli in situazioni di crisi, comprese le procedure specifiche da seguire;
 - b) le modalità di comunicazione tra i soggetti e le autorità competenti.
4. I piani di cui ai punti 1, 2 e 3 sono approvati dagli organi di amministrazione e direttivi.

5. I piani di cui ai punti 1, 2 e 3 sono riesaminati e, se opportuno, aggiornati periodicamente e comunque almeno ogni due anni, nonché qualora si verificano incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi.

3. PROTEZIONE (PROTECT)

- 3.1. **Gestione delle identità, autenticazione e controllo degli accessi (PR.AA):** L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.

- 3.1.1. **PR.AA-01:** Le identità e le credenziali degli utenti, dei servizi e dell'hardware autorizzati sono gestite dall'organizzazione.

1. Tutte le utenze, ivi incluse quelle con privilegi amministrativi e quelle utilizzate per l'accesso remoto, sono censite, approvate da attori interni al soggetto NIS e, fatte salve motivate e documentate ragioni tecniche, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono individuali per gli utenti.
2. Le credenziali (ad esempio nome utente e password) relative alle utenze sono robuste e aggiornate in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05.
3. Per almeno i sistemi informativi e di rete rilevanti, sono verificate periodicamente le utenze e le relative autorizzazioni, aggiornandole/revocandole in caso di variazioni (ad esempio trasferimento o cessazione di personale).
4. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1, 2 e 3.

- 3.1.2. **PR.AA-03:** Utenti, servizi e hardware sono autenticati.

1. Le modalità di autenticazione delle utenze per accedere ai sistemi informativi e di rete sono commisurate al rischio. A tal fine sono valutati almeno i rischi connessi:
 - a) ai privilegi delle utenze;
 - b) alla criticità dei sistemi informativi e di rete;
 - c) alla tipologia di operazioni che le utenze possono effettuare sui sistemi informativi e di rete.
2. Per almeno i sistemi informativi e di rete rilevanti, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono impiegate soluzioni di autenticazione multifattore.
3. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.

- 3.1.3. **PR.AA-05:** I permessi, i diritti e le autorizzazioni di accesso sono definiti in una politica, gestiti, applicati e rivisti e incorporano i principi del minimo privilegio e della separazione dei compiti.

1. I permessi sono assegnati alle utenze in accordo ai principi del minimo privilegio e della separazione delle funzioni, tenuto anche conto della necessità di conoscere (need to know).
2. È assicurata la completa distinzione tra utenze con e senza privilegi amministrativi degli amministratori di sistema alle quali debbono corrispondere credenziali diverse.
3. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.

- 3.1.4. **PR.AA-06:** L'accesso fisico agli asset è gestito, monitorato e applicato in misura appropriata al rischio.
1. Per almeno i sistemi informativi e di rete rilevanti, l'accesso fisico è protetto.
 2. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.
- 3.2. **Consapevolezza e formazione (PR.AT):** Il personale dell'organizzazione è sensibilizzato e formato sulla cybersecurity in modo da poter svolgere i propri compiti inerenti alla cybersecurity.
- 3.2.1. **PR.AT-01:** Il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.
1. È definito, attuato, aggiornato e documentato un piano di formazione in materia di sicurezza informatica del personale, ivi inclusi gli organi di amministrazione e direttivi, che comprende almeno:
 - a) la pianificazione delle attività di formazione previste con l'indicazione dei contenuti della formazione fornita;
 - b) le eventuali modalità di verifica dell'acquisizione dei contenuti.
 2. Il piano di formazione di cui al punto 1 è approvato dagli organi di amministrazione e direttivi.
 3. È mantenuto un registro aggiornato recante l'elenco dei dipendenti che hanno ricevuto la formazione di cui al punto 1, i relativi contenuti e l'elenco delle verifiche svolte laddove previste.
- 3.2.2. **PR.AT-02.** Gli individui che ricoprono ruoli specializzati sono sensibilizzati e formati in modo da possedere le conoscenze e le competenze per svolgere i pertinenti compiti tenendo conto dei rischi di cybersecurity.
1. Il piano di cui alla misura PR.AT-01 prevede una formazione dedicata al personale con ruoli specializzati, ossia che richiedono una serie di capacità e competenze attinenti alla sicurezza, ivi compresi gli amministratori di sistema, che comprende almeno:
 - a) le istruzioni relative alla configurazione e al funzionamento sicuri dei sistemi informativi e di rete;
 - b) le informazioni sulle minacce informatiche note;
 - c) le istruzioni sul comportamento da tenere in caso di eventi rilevanti per la sicurezza.
 2. È mantenuto un registro aggiornato recante l'elenco dei dipendenti che hanno ricevuto la formazione di cui al punto 1, i relativi contenuti e l'elenco delle verifiche svolte laddove previste.
- 3.3. **Sicurezza dei dati (PR.DS):** I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.
- 3.3.1. **PR.DS-01:** La riservatezza, l'integrità e la disponibilità dei dati a riposo (data-at-rest) sono protette.
1. Per almeno i sistemi informativi e di rete rilevanti, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, i dati memorizzati sui dispositivi portatili, ivi inclusi laptop,

smartphone e tablet, e sui supporti removibili, sono cifrati con protocolli e algoritmi allo stato dell'arte e considerati sicuri.

2. Fatte salve motivate e documentate ragioni normative o tecniche, è disabilitata l'auto esecuzione dei supporti removibili ed è effettuata la loro scansione al fine di rilevare codici malevoli prima che siano utilizzati nei sistemi informativi e di rete.
3. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.

3.3.2. **PR.DS-02:** La riservatezza, l'integrità e la disponibilità dei dati in transito (data-in-transit) sono protette.

1. Per almeno i sistemi informativi e di rete rilevanti, ivi inclusi quelli di comunicazione vocale, video e testuale, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, sono utilizzati, per la trasmissione dei dati da e verso l'esterno del soggetto NIS, protocolli e algoritmi di cifratura allo stato dell'arte e considerati sicuri.
2. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.

3.3.3. **PR.DS-11:** I backup dei dati sono creati, protetti, mantenuti e verificati.

1. In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04, sono effettuati periodicamente i backup dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate copie di backup offline.
2. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.
3. Per almeno i sistemi informativi e di rete rilevanti, è assicurata la riservatezza e l'integrità delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura.
4. Per almeno i sistemi informativi e di rete rilevanti, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.
5. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 3 e 4.

3.4. **Sicurezza delle piattaforme (PR.PS):** L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.

3.4.1. **PR.PS-01:** Sono stabilite e applicate pratiche di gestione della configurazione.

1. Per almeno i sistemi informativi e di rete rilevanti, sono definite, e documentate in un elenco aggiornato, le loro configurazioni di riferimento sicure (hardened).
2. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.

3.4.2. **PR.PS-02:** Il software è mantenuto, sostituito e rimosso in base al rischio.

1. Fatte salve motivate e documentate ragioni normative o tecniche, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, è installato esclusivamente software,

ivi compresi i sistemi operativi, per il quale è garantita la disponibilità di aggiornamenti di sicurezza.

2. Fatte salve motivate e documentate ragioni normative o tecniche, sono installati, senza ingiustificato ritardo, gli ultimi aggiornamenti di sicurezza rilasciati dal produttore in coerenza con il piano di gestione delle vulnerabilità di cui alla misura ID.RA-08.
3. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.
4. Fatte salve motivate e documentate ragioni normative o tecniche, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, l'aggiornamento del software ritenuto critico è verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo.
5. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 4.

3.4.3. **PR.PS-03:** L'hardware è mantenuto, sostituito e rimosso in base al rischio.

1. Per almeno i sistemi informativi e di rete rilevanti, sono adottate e documentate procedure per il trasferimento fisico e la dismissione di dispositivi atti alla memorizzazione di dati in modo sicuro.
2. Per almeno i sistemi informativi e di rete rilevanti, sono mantenuti uno o più registri delle manutenzioni effettuate sull'hardware.

3.4.4. **PR.PS-04:** I registri di log sono generati e resi disponibili per il monitoraggio continuo.

1. Tutti gli accessi eseguiti da remoto e quelli effettuati con utenze con privilegi amministrativi sono registrati.
2. Per almeno i sistemi informativi e di rete rilevanti, sono acquisiti e, in modo sicuro e possibilmente centralizzato, conservati almeno i log necessari ai fini del monitoraggio degli eventi di sicurezza, ivi compresi quelli relativi agli accessi di cui al punto 1.
3. In accordo agli esiti della valutazione rischio di cui alla misura ID.RA-05, sono definite e documentate le tempistiche di conservazione dei log di cui al punto 2.
4. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.

3.4.5. **PR.PS-06:** Le pratiche di sviluppo sicuro del software sono integrate e le loro prestazioni sono monitorate durante l'intero ciclo di vita del software.

1. Sono adottate e documentate pratiche di sviluppo sicuro del codice nello sviluppo del software.

3.5. **Resilienza dell'infrastruttura tecnologica (PR.IR):** Le architetture di sicurezza sono gestite in accordo con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità degli asset e la resilienza organizzativa.

3.5.1. **PR.IR-01:** Le reti e gli ambienti sono protetti dall'accesso logico e dall'uso non autorizzati.

1. Per almeno i sistemi informativi e di rete rilevanti, sono definite e documentate le eventuali attività consentite da remoto e implementate adeguate misure di sicurezza per l'accesso.
2. È mantenuto un elenco aggiornato dei sistemi informativi e di rete ai quali è possibile accedere da remoto con la descrizione delle relative modalità di accesso.
3. Sono presenti, aggiornati, mantenuti e configurati in modo adeguato i sistemi perimetrali, quali firewall.

4. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 2 e 3.

3.5.2. **PR.IR-03:** Sono implementati meccanismi per soddisfare i requisiti di resilienza in situazioni normali e avverse.

1. In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono utilizzati sistemi di comunicazione di emergenza protetti.
2. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.

4. RILEVAMENTO (DETECT)

4.1. **Monitoraggio continuo (DE.CM):** Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.

4.1.1. **DE.CM-01:** Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.

1. Per almeno i sistemi informativi e di rete rilevanti, sono presenti, aggiornati, mantenuti e configurati in modo adeguato strumenti tecnici per rilevare tempestivamente gli incidenti significativi.
2. Sono definiti e documentati i livelli di servizio attesi (SL) dei servizi e delle attività del soggetto NIS anche ai fini di rilevare tempestivamente gli incidenti significativi.
3. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.
4. Per almeno i sistemi informativi e di rete rilevanti, sono utilizzati strumenti di analisi e filtraggio sul flusso di traffico in ingresso (ivi inclusa la posta elettronica).
5. Per almeno i sistemi informativi e di rete rilevanti, ai fini di cui al punto 1, sono monitorati gli accessi da remoto, le attività dei sistemi perimetrali (ad esempio router e firewall), gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete, ai punti terminali (endpoint) e agli applicativi al fine di rilevare gli eventi di sicurezza informatica.
6. Per almeno i sistemi informativi e di rete rilevanti, ai fini di cui al punto 1, sono definiti, monitorati e documentati parametri quali-quantitativi per rilevare gli accessi non autorizzati o con abuso dei privilegi concessi.
7. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 4 e 5.

4.1.2. **DE.CM-09:** L'hardware e il software di elaborazione, gli ambienti di runtime e i loro dati sono monitorati per individuare eventi potenzialmente avversi.

1. Fatte salve motivate e documentate ragioni normative o tecniche, sono presenti, aggiornati, mantenuti e configurati in modo adeguato, sistemi di protezione dei punti terminali (endpoint) per il rilevamento del codice malevolo.
2. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.

5. RISPOSTA (RESPOND)

5.1. **Gestione degli incidenti (RS.MA):** Le risposte agli incidenti di cybersecurity rilevati sono gestite.

5.1.1. **RS.MA-01:** Il piano di risposta agli incidenti è eseguito in coordinamento con le terze parti interessate una volta dichiarato un incidente.

1. È definito, attuato, aggiornato e documentato un piano per la gestione degli incidenti di sicurezza informatica e la notifica al CSIRT Italia, in accordo a quanto previsto dall'articolo 25 del decreto NIS, che comprende almeno:
 - a) le fasi e le procedure di gestione e notifica degli incidenti con l'indicazione dei relativi ruoli e delle responsabilità;
 - b) le procedure per la predisposizione e la trasmissione delle relazioni di cui all'articolo 25, comma 5, lettere c), d) ed e) del decreto NIS;
 - c) le informazioni di contatto per la segnalazione degli incidenti;
 - d) le modalità di comunicazione interna, anche con riguardo al coinvolgimento degli organi di amministrazione e direttivi, ed esterna;
 - e) la reportistica da utilizzare per la documentazione dell'incidente.
2. Il piano di cui al punto 1 è approvato dagli organi di amministrazione e direttivi.
3. Il piano di cui al punto 1 è riesaminato e, se opportuno, aggiornato periodicamente e comunque almeno ogni due anni, nonché qualora si verificano incidenti significativi, integrando le relative lezioni apprese, o mutamenti dell'esposizione alle minacce e ai relativi rischi.

5.2. **Segnalazione e comunicazione della risposta agli incidenti (RS.CO):** Le attività di risposta sono coordinate con gli stakeholder interni ed esterni come richiesto da leggi, regolamenti o politiche.

5.2.1. **RS.CO-02:** Gli stakeholder interni ed esterni sono informati degli incidenti.

1. In accordo al piano per la gestione degli incidenti di cui alla misura RS.MA-01, sono documentate e adottate procedure per comunicare senza ingiustificato ritardo, se ritenuto opportuno e qualora possibile, sentito il CSIRT Italia, ovvero qualora intimato dall'Agenzia per la cybersicurezza nazionale ai sensi dell'articolo 37, comma 3, lettere g) e h), del decreto NIS:
 - a) ai destinatari dei propri servizi, gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi;
 - b) ai destinatari dei propri servizi che sono potenzialmente interessati da una minaccia informatica significativa, le misure o azioni correttive o di mitigazione che tali destinatari possono adottare in risposta a tale minaccia e la natura di tale minaccia.
2. Sono documentate e adottate procedure per informare il pubblico sugli incidenti occorsi, qualora intimato dall'Agenzia per la cybersicurezza nazionale ai sensi dell'art. 37, comma 3, lettera i) del decreto NIS.

6. **RIPRISTINO (RECOVER)**

6.1. **Esecuzione del piano di ripristino dagli incidenti (RC.RP):** Le attività di ripristino sono eseguite per garantire la disponibilità operativa dei sistemi e dei servizi interessati da incidenti di cybersecurity.

- 6.1.1. **RC.RP-01:** La parte del piano di risposta agli incidenti relativa al ripristino viene eseguita una volta avviata dal processo di risposta agli incidenti.
1. Nell'ambito del piano per la gestione degli incidenti di cui alla misura RS.MA-01, sono adottate e documentate procedure per il ripristino con riguardo almeno al ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da incidenti di sicurezza informatica, ivi compresi quelli di cui all'articolo 25 del decreto NIS.
- 6.2. **Comunicazione sul ripristino dagli incidenti (RC.CO):** Le attività di ripristino sono coordinate con le parti interne ed esterne.
- 6.2.1. **RC.CO-03:** Le attività di ripristino e i progressi nel ripristino delle capacità operative sono comunicati agli stakeholder interni ed esterni designati.
1. Sono adottate e documentate procedure per comunicare alle parti interne interessate, ivi incluse le articolazioni competenti del soggetto NIS, le attività di ripristino a seguito di un incidente.

Appendice

Tabella 1: Requisiti di cui al punto 2 della misura GV.PO-01.

Ambiti Politiche	Requisiti
a) Gestione del rischio.	GV.OC-04: punto 1. GV.RM-03: punto 1. ID.RA-05: punti 1, 2, 3 e 4. ID.RA-06: punti 1, 2 e 3.
b) Ruoli e responsabilità.	GV.RR-02: punti 1, 2, 3 e 4.
c) Affidabilità delle risorse umane.	GV.RR-04: punti 1, 2 e 4.
d) Conformità e audit di sicurezza.	GV.PO-01: punti 1, 2 e 3. GV.PO-02: punti 1, 2, 3. ID.IM-01: punti 1, 2, 3 e 4.
e) Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento.	GV.SC-01: punti 1 e 2. GV.SC-02: punto 1. GV.SC-04: punto 1. GV.SC-05: punto 1. GV.SC-07: punti 1 e 2.
f) Gestione degli asset.	ID.AM-01: punto 1. ID.AM-02: punto 1. ID.AM-03: punto 1. ID.AM-04: punto 1.
g) Gestione delle vulnerabilità.	ID.RA-01: punti 1, 2 e 3. ID.RA-08: punti 1, 2, 3, 4 e 5.
h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi informatiche.	ID.IM-04: punti 1, 2, 3, 4 e 5.
i) Gestione dell'autenticazione, delle identità digitali e del controllo accessi.	PR.AA-01: punti 1, 2 e 3. PR.AA-03: punti 1 e 2. PR.AA-05: punti 1 e 2. PR.IR-01: punti 1 e 2.
j) Sicurezza fisica.	PR.AA-06: punto 1.
k) Formazione del personale e consapevolezza.	PR.AT-01: punti 1, 2 e 3. PR.AT-02: punti 1 e 2.
l) Sicurezza dei dati.	PR.DS-01: punti 1 e 2. PR.DS-02: punto 1. PR.DS-11: punti 1, 3 e 4.
m) Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete.	PR.PS-01: punto 1. PR.PS-02: punti 1, 2 e 4. PR.PS-03: punti 1 e 2. PR.PS-04: punti 1, 2 e 3. PR.PS-06: punto 1.
n) Protezione delle reti e delle comunicazioni.	PR.IR-01: punto 3. PR.IR-03: punto 1.
o) Monitoraggio degli eventi di sicurezza.	DE.CM-01: punti 1, 2, 4, 5 e 6. DE.CM-09: punto 1.
p) Risposta agli incidenti e ripristino.	RS.MA-01: punti 1, 2 e 3. RS.CO-02: punti 1 e 2. RC.RP-01: punto 1. RC.CO-03: punto 1.

Tabella 2: Requisiti di cui al punto 2 della misura ID.RA-06.

Requisiti
GV.SC-05: punto 1.
ID.RA-01: punto 2.
PR.AA-01: punto 1.
PR.DS-01: punti 1 e 2.
PR.DS-02: punto 1.
PR.PS-02: punti 1, 2 e 4.
DE.CM-09: punto 1.