Roma, 18 aprile 2025

Al Comitato di Presidenza
Al Consiglio Direttivo
Alla Commissione Legale
Alla Commissione Sindacale
Alle Associazioni Territoriali

Circolare n. 20/2025

Oggetto: Varie - Ordine pubblico – Rafforzamento livello globale cybersicurezza – Attuazione della nuova disciplina – Adempimenti.

L'ACN – Agenzia per la cybersicurezza nazionale – ha pubblicato sul proprio sito (https://www.acn.gov.it/portale/w/nis-avviata-la-seconda-fase) alcuni provvedimenti che danno il via alla seconda fase attuativa della Direttiva NIS (Direttiva UE n.2555/2022 recepita, come è noto, dal decreto legislativo n.138/2024).

Si tratta del passaggio dalla fase di identificazione dei soggetti NIS a quella dell'attuazione tecnica e organizzativa degli obblighi previsti dalle nuove norme.

Come è noto, lo scorso 28 febbraio era scaduto per i soggetti interessati il termine dell'obbligo di registrazione sulla piattaforma digitale dedicata.

Si riepilogano di seguito gli aspetti principali delle determinazioni adottate dal direttore generale dell'ACN.

- Determina ACN n.136117 del 10.4.2025 – Sono stati disciplinati l'accesso al portale dei servizi, le modalità per la registrazione e l'aggiornamento delle informazioni nonché la designazione del punto di contatto e delle altre persone abilitate ad operare sul portale dei servizi dell'ACN per conto dei soggetti NIS che dovranno procedere all'aggiornamento annuale delle informazioni attraverso la piattaforma digitale, nel periodo compreso tra il 15 aprile e il 31 maggio; tale adempimento prevede la revisione e la conferma dei dati anagrafici, contabili e tecnici dell'organizzazione.

- Determina ACN n.136118 del 10.4.2025 – Sono state introdotte disposizioni specifiche in merito alla partecipazione ad accordi volontari di condivisione delle informazioni sulla sicurezza informatica (non più una pratica lasciata all'iniziativa dei singoli come in precedenza, bensì un adempimento formalizzato, con obbligo di notifica, aggiornamento e documentazione): pertanto, i soggetti NIS devono notificare, attraverso la piattaforma digitale, tutti gli accordi sottoscritti a partire dall'entrata in vigore del decreto (16 ottobre 2024); l'adempimento prevede la condivisione del testo dell'accordo, della sua denominazione e dell'elenco dei partecipanti. Entro il 31 maggio di ogni anno deve essere eseguito l'aggiornamento degli accordi in essere, e ogni variazione (la sottoscrizione alla risoluzione, la modifica dei partecipanti etc.) deve essere comunicata entro 14 giorni. Eventuali accordi precedenti all'entrata in vigore del decreto, se ancora attivi, dovranno essere notificati entro il 31 maggio 2026.

00198 ROMA
Via Panama, 62
tel. 06.86399800
www.fedit.it
segreteria@fedit.it
Cod. Fisc. 80159670159

• Determina ACN n.164179 del 14.4.2025 – Sono state stabilite le specifiche tecniche di base che i soggetti NIS dovranno adottare per adempiere agli obblighi della normativa. Sono indicate nello specifico i termini per l'adeguamento a tali obblighi: 18 mesi dal momento in cui si viene inseriti nell'elenco dei soggetti NIS per adottare tutte le misure di sicurezza richieste; 9 mesi per attivare i sistemi di notifica degli incidenti rilevanti. Il provvedimento si fonda su quattro allegati che definiscono le misure minime di sicurezza e le definizioni specifiche per gli incidenti significativi di base rispettivamente per i soggetti cd importanti e cd essenziali.

Con i migliori saluti.

Il Segretario Generale
Alfredo D'Ascoli

federazione italiana trasportatori

00198 ROMA
Via Panama, 62
tel. 06.86399800

www.fedit.it
segreteria@fedit.it

Cod. Fisc. 80159670159

confetra

Agenzia per la Cybersicurezza Nazionale

Determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale

di cui all'articolo 7, comma 6, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, recante termini, modalità e procedimenti di utilizzo e accesso alla piattaforma digitale nonché ulteriori informazioni che i soggetti devono fornire all'Autorità nazionale competente NIS e termini, modalità e procedimento di designazione dei rappresentanti NIS sul territorio nazionale.

IL DIRETTORE GENERALE

VISTO il decreto legislativo 12 gennaio 2019, n. 14, recante "*Codice della crisi d'impresa e dell'insolvenza in attuazione della legge 19 ottobre 2017, n. 155*";

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

VISTO il decreto legislativo 4 settembre 2024, n. 138, recante "*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148"* e, in particolare, l'articolo 7 e l'articolo 40, comma 5, lettera b);

VISTO il Regolamento (CEE) n. 2137/85 del Consiglio del 25 luglio 1985 relativo all'istituzione di un gruppo europeo di interesse economico (GEIE);

VISTO il decreto legislativo 23 luglio 1991, n. 240, recante "Norme per l'applicazione del regolamento n. 85/2137/CEE relativo all'istituzione di un Gruppo europeo di interesse economico - GEIE, ai sensi dell'art. 17 della legge 29 dicembre 1990, n. 428";

VISTA la raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese;

VISTA la legge 28 giugno 2024, n. 90, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici";

VISTO il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", e, in particolare, l'articolo 76;

CONSIDERATO che, ai sensi del richiamato articolo 7, comma 1, del decreto legislativo 4 settembre 2024, n. 138, i soggetti di cui all'articolo 3 del medesimo decreto si registrano o

aggiornano la propria registrazione sulla piattaforma digitale resa disponibile dall'Autorità nazionale competente NIS;

CONSIDERATO, altresì, che, ai sensi dell'articolo 7, comma 6, e dell'articolo 40, comma 5, lettera b), del decreto legislativo 4 settembre 2024, n. 138, con determinazione dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS, sono stabiliti i termini, le modalità nonché i procedimenti di utilizzo e accesso alla piattaforma digitale di cui all'articolo 7 e le eventuali ulteriori informazioni che i soggetti devono fornire ai sensi dello stesso articolo, nonché i termini, le modalità e i procedimenti di designazione dei rappresentanti di cui all'articolo 5, comma 3, del medesimo decreto legislativo;

RITENUTO di aggiornare e sostituire la determinazione ACN n. 38565 del 26 novembre 2024 al fine di integrare le previsioni relative alla piattaforma digitale in relazione agli adempimenti di cui all'articolo 7, commi 4 e 5, nonché alle previsioni di cui all'articolo 17, comma 4, del decreto legislativo 4 settembre 2024, n. 138;

SENTITO il Tavolo per l'attuazione della disciplina NIS di cui all'articolo 12 del decreto legislativo 4 settembre 2024, n. 138, nella riunione del 10 aprile novembre 2025;

ADOTTA LA PRESENTE DETERMINAZIONE

Capo I
Disposizioni di carattere generale

Articolo 1
(Definizioni)

1. Ai fini della presente determinazione si intende per:
   a) "decreto NIS", il decreto legislativo 4 settembre 2024, n. 138;
   b) "Agenzia per la cybersicurezza nazionale", l'Agenzia per la cybersicurezza nazionale di cui all'articolo 5, comma 1, del decreto-legge 14 giugno 2021, n. 82;
   c) "Autorità nazionale competente NIS", l'Autorità nazionale competente di cui all'articolo 10, comma 1, del decreto NIS;
   d) "Autorità di settore NIS", le Amministrazioni di cui all'articolo 11, commi 1 e 2, del decreto NIS;
   e) "organi di amministrazione e direttivi", gli organi di amministrazione e direttivi di cui all'articolo 23 del decreto NIS, ivi incluso, laddove presente, il consiglio di amministrazione dei soggetti NIS;
   f) "Portale ACN", il Portale dei servizi tramite il quale sono accessibili i servizi che l'Agenzia per la cybersicurezza nazionale mette a disposizione dei suoi interlocutori e dei soggetti, pubblici e privati, che rientrano nell'ambito di applicazione della disciplina cyber o con i quali l'Agenzia deve interagire ai sensi della stessa;

g) "Servizi NIS", i servizi, accessibili tramite il Portale ACN, necessari per supportare l'espletamento degli adempimenti previsti dal decreto NIS e le interlocuzioni tra l'Autorità nazionale compente NIS e i soggetti;
h) "Servizio NIS/Registrazione", il Servizio NIS reso disponibile dall'Autorità nazionale competente NIS ai fini della registrazione di cui all'articolo 7, comma 1, del decreto NIS;
i) "Servizio NIS/Aggiornamento annuale", il Servizio NIS reso disponibile dall'Autorità nazionale competente NIS per fornire e aggiornare le informazioni di cui all'articolo 7, commi 4 e 5, del decreto NIS;
j) "sito web", il sito web istituzionale dell'Agenzia per la cybersicurezza nazionale (acn.gov.it);
k) "piattaforma digitale", la piattaforma digitale di cui all'articolo 7, comma 1, del decreto NIS, accessibile tramite il Portale ACN per l'erogazione dei Servizi NIS;
l) "soggetto", un soggetto, di cui all'articolo 2, comma 1, lettera hhh), del decreto NIS, di natura giuridica pubblica o privata per conto della quale un utente accede al Portale ACN e, in particolare, ai Servizi NIS;
m) "soggetto NIS", un soggetto che rientra nell'ambito di applicazione del decreto NIS;
n) "punto di contatto", la persona fisica designata dal soggetto NIS ai sensi dell'articolo 7, comma 1, lettera c), del decreto NIS;
o) "sostituto punto di contatto", la persona fisica designata dal soggetto NIS ai sensi dell'articolo 7, comma 4, lettera d), del decreto NIS;
p) "segreteria", la persona fisica che svolge funzioni di supporto al punto di contatto e al sostituto punto di contatto per promuovere l'efficace interlocuzione con l'Autorità nazionale competente NIS;
q) "operatore", la persona fisica che svolge funzioni di supporto al punto di contatto e al sostituto punto di contatto operando sui servizi NIS;
r) "utente", il punto di contatto, il sostituto punto di contatto, la segreteria e gli operatori che accedono al Portale ACN e, in particolare, accedono ai Servizi NIS;
s) "rappresentante NIS", il rappresentante di cui all'articolo 5, comma 3, del decreto NIS;
t) "censimento", il processo di autenticazione, tracciamento e verifica di un utente finalizzato alla sua associazione a un soggetto per accedere al Portale ACN e, in particolare, ai Servizi NIS;
u) "associazione", il processo di tracciamento, verifica e convalida dell'associazione dell'utenza con un soggetto che consente all'utente stesso di accedere al Portale ACN e, in particolare, ai Servizi NIS;
v) "registrazione", il processo di cui all'articolo 7, comma 1, del decreto NIS;
w) "dichiarazione", la dichiarazione resa dal punto di contatto ai fini della registrazione;
x) "elenco dei soggetti NIS", l'elenco dei soggetti essenziali e dei soggetti importanti di cui all'articolo 7, comma 3, del decreto NIS;
y) "impresa collegata", un soggetto che soddisfa i criteri di cui all'articolo 3, paragrafi 2 e 3, dell'allegato alla raccomandazione 2003/361/CE, o che fa parte di un gruppo di imprese;
z) "impresa autonoma", una impresa non identificabile come impresa collegata;

aa) "gruppo di imprese", ai sensi dell'articolo 2, comma 1, lettera h), del decreto legislativo 12 gennaio 2019, n. 14, l'insieme delle società, delle imprese e degli enti, esclusi lo Stato e gli enti territoriali, che esercitano o sono sottoposti, ai sensi degli articoli 2497 e 2545-septies del codice civile, alla direzione e coordinamento di una società, di un ente o di una persona fisica; a tal fine si presume, salvo prova contraria, che l'attività di direzione e coordinamento delle società del gruppo sia esercitata dalla società o ente tenuto al consolidamento dei loro bilanci oppure dalla società o ente che le controlla, direttamente o indirettamente, anche nei casi di controllo congiunto;

bb) "gruppo europeo di interesse economico (GEIE)", un gruppo di imprese costituito sulla base delle condizioni, modalità ed effetti disciplinati dal Regolamento (CEE) n. 2137/85.

cc) "aggiornamento annuale delle informazioni", il processo tramite il quale i soggetti NIS forniscono e, ogni anno, aggiornano le informazioni di cui all'articolo 7, commi 4 e 5, del decreto NIS;

dd) "spazio di indirizzamento IP pubblico in uso o nella disponibilità del soggetto NIS", gli indirizzi IP pubblici e statici che un soggetto NIS utilizza o ha nella propria disponibilità in forza di contratti o accordi con fornitori di servizi Internet (ISP), Registri Internet Regionali o altre organizzazioni deputate alla fornitura di indirizzi IP sulla base delle normative e degli accordi nazionali, europei e internazionali vigenti;

ee) "nomi di dominio in uso o nella disponibilità del soggetto NIS", i nomi di dominio che un soggetto NIS utilizza o ha nella propria disponibilità in forza di contratti o accordi con fornitori di servizi di registrazione di nomi di dominio o altre organizzazioni deputate loro fornitura di nomi di dominio sulla base delle normative e degli accordi nazionali, europei e internazionali vigenti;

ff) "accordi di condivisione", gli accordi di condivisione delle informazioni sulla sicurezza informatica, di cui all'articolo 17, comma 2, del decreto NIS;

Articolo 2
(Oggetto, ambito di applicazione e finalità)

1. La presente determinazione stabilisce termini, modalità e procedimenti di utilizzo e accesso al Portale ACN e, in particolare, ai Servizi NIS nonché le ulteriori informazioni che i soggetti NIS devono fornire all'Autorità nazionale competente NIS ai fini dello svolgimento delle funzioni attribuite dal decreto NIS, i termini, le modalità e i procedimenti di designazione dei rappresentanti NIS nell'Unione.
2. Ai fini del comma 1, la presente determinazione definisce:
   a) le modalità di designazione del punto di contatto e del sostituto punto di contatto:
   b) il processo per il censimento degli utenti per accedere al Portale ACN;
   c) il procedimento per l'associazione degli utenti al soggetto per conto del quale accedono ai Servizi NIS;
   d) il procedimento per la registrazione, tramite il Servizio NIS/Registrazione;
   e) il processo per l'aggiornamento annuale delle informazioni, tramite il Servizio NIS/Aggiornamento annuale.
3. Ai sensi dell'articolo 23, comma 1, lettera b), del decreto NIS, gli organi di amministrazione e direttivi dei soggetti NIS sovrintendono alla registrazione, comunicazione o

aggiornamento delle informazioni di cui all'articolo 7 del medesimo decreto e sono responsabili delle eventuali violazioni.

4. La mancata registrazione, comunicazione o aggiornamento delle informazioni di cui all'articolo 7 del decreto NIS, con le modalità sopra indicate, è punita ai sensi dell'articolo 38 del medesimo decreto.
5. La presente determinazione è aggiornata entro il 30 giugno 2025.

Articolo 3
(Termini di uso del Portale ACN e dei Servizi NIS)

1. I soggetti comunicano con l'Autorità nazionale competente NIS, anche ai fini del censimento, dell'associazione e della registrazione, esclusivamente tramite i Servizi NIS o tramite la sezione dedicata nell'area NIS del sito web, salvo in caso di diversa espressa specifica indicazione dell'Autorità nazionale competente o per cause di forza maggiore, fermo restando quanto previsto dal decreto NIS.
2. Le istruttorie dell'Autorità nazionale competente NIS e delle Autorità di settore NIS ai fini della presente determinazione sono svolte prioritariamente sulla base delle informazioni trasmesse dai soggetti tramite i Servizi NIS.
3. Gli utenti aggiornano le informazioni trasmesse tramite il Portale ACN o tramite i Servizi NIS tempestivamente, secondo eventuale specifica indicazione dell'Autorità nazionale competente NIS, nel rispetto dei termini indicati dal decreto NIS.
4. Gli utenti sono tenuti a verificare la correttezza delle informazioni visualizzate o ricevute tramite il Portale ACN e i Servizi NIS, e in caso di incongruenze effettuano la segnalazione di cui al comma 6.
5. Resta ferma la responsabilità penale, ai sensi dell'articolo 76 del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445, in caso di rilascio di dichiarazioni mendaci, formazione di atti falsi o, comunque, contenenti dati non più rispondenti a verità.
6. Gli utenti segnalano, tramite gli appositi canali di comunicazione del Portale ACN o tramite la sezione dedicata nell'area NIS del sito web, malfunzionamenti o comportamenti inattesi del Portale ACN stesso e dei Servizi NIS.
7. Le informazioni visualizzate o ricevute tramite il Portale ACN e i Servizi NIS sono condivise nel rispetto della politica di condivisione delle informazioni. Salvo diversa specifica indicazione, le informazioni visualizzate o ricevute tramite il Portale ACN e i Servizi NIS sono a divulgazione limitata e sono ristrette all'originatore e ai destinatari dell'informazione, nonché alle loro organizzazioni, alle loro terze parti e ai propri clienti. I destinatari non possono condividere le informazioni ricevute al di fuori della propria organizzazione, delle loro terze parti e dei propri clienti. La condivisione delle informazioni ricevute nella propria organizzazione con le terze parti e con i clienti è limitata ai dati strettamente necessari per lo svolgimento delle attività (principio del need-to-know).

Articolo 4
(Punto di contatto)

1. Il punto di contatto è una persona fisica designata dal soggetto NIS con il compito di curare l'attuazione delle disposizioni del decreto NIS per conto del soggetto stesso. In particolare, il punto di contatto accede al Portale ACN e ai Servizi NIS, effettua, per conto del soggetto, la registrazione di cui all'articolo 7 del decreto NIS, e interloquisce, per conto del soggetto NIS, con l'Autorità nazionale competente NIS.
2. Le funzioni di punto di contatto possono essere svolte dal rappresentante legale del soggetto NIS, da uno dei procuratori generali del soggetto NIS, censiti sul registro delle imprese di cui all'articolo 8 della legge 29 dicembre 1993, n. 580, o da un dipendente del soggetto NIS delegato dal rappresentante legale del soggetto medesimo. Laddove il punto di contatto, nell'espletamento delle proprie funzioni, si avvalga di personale esterno, restano comunque ferme le disposizioni di cui al comma 1.
3. Qualora il soggetto sia parte di un gruppo di imprese, le funzioni di punto di contatto possono essere svolte da un dipendente di un'altra impresa del gruppo che rientra nell'ambito di applicazione del decreto NIS, delegato dal rappresentante legale del soggetto stesso.
4. Qualora il soggetto NIS sia una pubblica amministrazione, le funzioni di punto di contatto possono essere svolte da personale che presta servizio o dipendente di un'altra pubblica amministrazione che rientra nell'ambito di applicazione del decreto NIS, previa autorizzazione di quest'ultima ai sensi dell'articolo 53 del decreto legislativo 30 marzo 2001, n. 165, delegato dal rappresentante legale del soggetto stesso.
5. Il punto di contatto riferisce direttamente al vertice gerarchico del soggetto NIS nonché agli organi di amministrazione e direttivi del soggetto medesimo ai fini di quanto previsto dal decreto NIS.
6. Resta ferma, in ogni caso, la responsabilità degli organi di amministrazione e direttivi del soggetto NIS ai sensi dell'articolo 23 del decreto NIS e delle persone fisiche ai sensi dell'articolo 38 del medesimo decreto.
7. Nel caso di avvicendamento del punto di contatto, gli organi di amministrazione e direttivi provvedono senza ingiustificato ritardo alla designazione del nuovo punto di contatto e assicurano il suo censimento sul Portale ACN.
8. La designazione del punto di contatto da parte dei soggetti di cui all'articolo 1, comma 1, della legge 28 giugno 2024, n. 90, che rientrano nell'ambito di applicazione del decreto NIS, può soddisfare l'obbligo di nomina e comunicazione del referente per la cybersicurezza di cui all'articolo 8, comma 2, della medesima legge.

Articolo 5
(Sostituto punto di contatto)

1. Il sostituto punto di contatto è una persona fisica, distinta dal punto di contatto, designato con le medesime modalità di quest'ultimo ai sensi dell'articolo 4 a cui si applicano le previsioni del citato articolo.
2. Il sostituto punto di contatto supporta il punto di contatto nell'esercizio delle proprie funzioni, può interloquire direttamente con l'Autorità nazionale competente NIS e può

effettuare sulla piattaforma digitale le medesime azioni del punto di contatto, ad eccezione della registrazione di cui all'articolo 7 del decreto NIS.

3. Il sostituto punto di contatto è designato entro il 31 maggio dell'anno in cui il soggetto NIS ha ricevuto comunicazione di inserimento nell'elenco dei soggetti NIS.

Articolo 6
(Rappresentante nell'Unione)

1. Per designare il proprio rappresentante NIS in Italia, i soggetti NIS di cui all'articolo 5, comma 1, lettera b), del decreto NIS, trasmettono e aggiornano, dal primo settembre al trenta novembre di ogni anno, al domicilio digitale dell'Agenzia per la cybersicurezza nazionale la documentazione indicata nella sezione dedicata del sito web. Con le medesime modalità, tali soggetti comunicano il domicilio digitale per le conseguenti interlocuzioni con l'Autorità nazionale competente NIS.
2. L'Autorità nazionale competente NIS comunica al domicilio digitale del soggetto l'autorizzazione, o il diniego, a procedere al censimento e alla registrazione entro trenta giorni dalla ricezione della trasmissione di cui al comma 1.
3. Ove si renda necessario richiedere al soggetto integrazioni o informazioni, i termini di cui al comma 2 sono sospesi e ricominciano a decorrere dalla data di ricevimento delle integrazioni e delle informazioni che sono rese entro il termine di dieci giorni dalla richiesta. Il tardivo riscontro alle richieste di cui al presente comma può essere motivo di diniego di censimento e registrazione.
4. Fermo restando quanto previsto dall'articolo 4, comma 2, i soggetti di cui al comma 1 del presente articolo possono delegare le funzioni di punto di contatto:
   a) al rappresentante NIS stesso, qualora sia una persona fisica;
   b) al rappresentante legale, a uno dei procuratori generali o a un dipendente del rappresentante NIS stesso, qualora quest'ultimo sia una persona giuridica.

Capo II
Censimento e associazione delle utenze

Articolo 7
(Censimento degli utenti)

1. Gli utenti si autenticano sul Portale ACN tramite le proprie credenziali personali del Sistema Pubblico di Identità Digitale (SPID).
2. Gli utenti completano la propria anagrafica fornendo le informazioni seguenti, se non già condivise tramite SPID:
   a) nome e cognome;
   b) codice fiscale;
   c) luogo e data di nascita;
   d) cittadinanza;
   e) Paese di residenza e, ove richiesto, di domicilio;

f) indirizzo della sede prevalente di servizio, aziendale o professionale;
g) indirizzo di posta elettronica ordinaria, preferibilmente individuale, nonché di servizio, aziendale o professionale;
h) ove disponibile, un indirizzo di posta elettronica certificata, preferibilmente individuale, nonché di servizio, aziendale o professionale;
i) numero di telefono, preferibilmente individuale, nonché di servizio, aziendale o professionale;
j) ove disponibile, un numero alternativo di telefono, preferibilmente individuale di servizio, aziendale o professionale;
k) denominazione e codice fiscale dell'organizzazione di appartenenza prevalente.

3. Qualora, ai sensi della normativa vigente, un utente non possa disporre di credenziali SPID può autenticarsi con credenziali personali. La procedura per la richiesta delle credenziali personali è pubblicata nella sezione dedicata del sito web. Tali utenti forniscono un codice di identificazione nazionale in luogo del codice fiscale di cui al comma 2, lettera c).

Articolo 8
(Associazione dell'utenza del punto di contatto e del sostituto al soggetto NIS)

1. Il punto di contatto, censito sul Portale ACN, effettua l'associazione della sua utenza con il soggetto che lo ha designato attraverso la digitazione del suo codice fiscale o del codice dell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA).
2. L'utente:
   a) verifica la denominazione nonché l'indirizzo, il domicilio digitale e i recapiti della sede legale del soggetto visualizzati dal Portale ACN;
   b) indica se è:
      1) rappresentante legale del soggetto;
      2) procuratore generale del soggetto;
      3) delegato dal rappresentante legale del soggetto;
   c) indica il codice fiscale dell'organizzazione di cui è dipendente qualora diverso dal soggetto al quale si sta associando;
   d) indica il ruolo svolto presso il soggetto.
3. Nel caso di cui al comma 2, lettera b), numero 3, l'utente inserisce sul Portale ACN la delega rilasciata a suo nome dal soggetto NIS, dichiarando che la stessa lo autorizza ad accedere al Portale ACN stesso e ai Servizi NIS per conto del medesimo soggetto.
4. L'associazione dell'utenza del punto di contatto è sottoposta alla convalida del soggetto NIS, secondo la procedura telematica indicata nella richiesta inviata al domicilio digitale di quest'ultimo.
5. Al termine del processo di censimento e associazione, il soggetto riceve al suo domicilio digitale la comunicazione di conclusione del processo stesso.
6. La convalida dell'associazione dell'utenza del punto di contatto ad un soggetto NIS determina la dissociazione, se presente, dell'utenza del punto di contatto precedentemente associata.

7. Il sostituto punto di contatto effettua, su invito del punto di contatto, l'associazione con le medesime modalità del punto di contatto di cui al presente articolo.

Articolo 9
(Associazione dell'utenze al soggetto NIS)

1. Al punto di contatto è data facoltà di invitare ulteriori utenti con il ruolo di operatore e, al più, un utente con il ruolo di segreteria.
2. Gli utenti censiti sul Portale ACN che non sono stati designati e associati quali punti di contatto o sostituti punti di contatto:
    a) sono associati al soggetto NIS, per conto del quale operano, su indicazione e invito del punto di contatto;
    b) non possono effettuare azioni sul Portale ACN che determinano la trasmissione di comunicazioni, inerenti il perfezionamento degli adempimenti di cu al decreto NIS, al domicilio digitale del soggetto NIS o all'Autorità nazionale competente NIS.
3. Tutti gli utenti possono:
    a) annullare la propria associazione con il soggetto NIS;
    b) disabilitare la propria utenza.
4. Il punto di contatto, il sostituto punto di contatto e la segreteria possono ridurre il proprio ruolo ad operatore.

Capo III
Registrazione dei soggetti NIS e elaborazione dell'elenco dei soggetti NIS

Articolo 10
(Registrazione)

1. Dal 1° gennaio al 28 febbraio di ogni anno, gli utenti compilano, tramite il Servizio NIS/Registrazione, la dichiarazione per il soggetto per cui operano ai fini della sua registrazione, assicurandosi che le informazioni fornite siano corrette e aggiornate.
2. In particolare, l'utente:
    a) qualora il soggetto non sia un'impresa autonoma, indica se il soggetto è parte di un gruppo di imprese e, in tal caso, indica se il soggetto è la capo gruppo ovvero indica il codice fiscale della capo gruppo;
    b) qualora il soggetto non sia un'impresa autonoma, elenca i soggetti NIS di cui è a conoscenza che sono imprese collegate nei confronti delle quali soddisfi almeno uno dei criteri di cui all'articolo 3, comma 10, del decreto NIS, indicando il codice fiscale di tali imprese e quale dei criteri è soddisfatto;
    c) qualora il soggetto non sia un'impresa autonoma, elenca le imprese collegate che soddisfano nei suoi confronti almeno uno dei criteri di cui all'articolo 3, comma 10, del decreto NIS, indicando il codice fiscale di tali imprese e quale dei criteri è soddisfatto, ai fini della loro identificazione come soggetti NIS ai sensi del medesimo comma;

d) elenca i codici ATECO che descrivono l'attività del soggetto;
e) indica le normative settoriali dell'Unione europea citate negli allegati I e II del decreto NIS per definire le tipologie di soggetto che rientrano nell'ambito di applicazione del decreto NIS;
f) indica i valori del fatturato e del bilancio nonché del numero di dipendenti al fine di determinare l'appartenenza del soggetto NIS alla categoria delle medie o grandi imprese ai sensi della raccomandazione 2003/361/CE. Le pubbliche amministrazioni possono non indicare i valori del fatturato e del bilancio;
g) elenca le tipologie di soggetto di cui agli allegati I, II e III del decreto NIS a cui il soggetto è riconducibile nonché, per i soggetti identificati ai sensi dell'articolo 3, commi 8, 9 e 13 del medesimo decreto, di cui all'allegato IV del decreto NIS.

3. Fermo restando l'obbligo di registrazione per i soggetti di cui all'articolo 3, comma 10, del decreto NIS, l'Autorità nazionale competente NIS informa le imprese di cui al comma 2, lettera c), del presente articolo che nei loro confronti si sono verificati i presupposti di cui al citato articolo del decreto NIS.
4. Qualora il soggetto non sia una impresa autonoma, il calcolo del fatturato e del bilancio nonché del numero di dipendenti di cui al comma 2, lettera f), del presente articolo è effettuato ai sensi dell'articolo 6, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE.
5. Qualora in fase di compilazione della dichiarazione siano rilevate incongruenze, queste sono segnalate all'utente che deve procedere a:
   a) modificare la dichiarazione correggendo le informazioni errate o incomplete;
   b) fornire ulteriori elementi informativi per giustificare l'incongruenza rilevata.
5. Al termine della compilazione della dichiarazione, all'utente è rimessa la conferma della valutazione preliminare, svolta automaticamente sulla base delle informazioni fornite ai sensi del presente articolo.
6. Gli utenti designati quali punti di contatto confermano, ai sensi del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445, le informazioni fornite e le trasmettono telematicamente tramite il servizio NIS/Registrazione all'Autorità nazionale competente NIS. Copia di tali informazioni, per ricevuta, è inviata al domicilio digitale del soggetto con l'avvertenza che tale dichiarazione potrà essere sottoposta alle verifiche di coerenza di cui all'articolo 11.

Articolo 11
(Clausola di salvaguardia)

1. Nel caso in cui l'utente ritenga che il calcolo effettuato ai sensi dell'articolo 8, comma 4, non sia proporzionato tenuto conto dei criteri di cui al decreto del Presidente del Consiglio dei ministri di cui all'articolo 40, comma 1, lettera a), del decreto NIS, nel corso della registrazione può chiedere l'applicazione della clausola di salvaguardia di cui all'articolo 3, comma 12, del decreto NIS.
2. Ai fini della richiesta di cui al comma 1, tramite il Servizio NIS/Registrazione, l'utente fornisce gli elementi di valutazione corrispondenti ai criteri di cui al decreto del Presidente del Consiglio dei ministri di cui all'articolo 40, comma 1, lettera a), del decreto NIS

all'Autorità nazionale competente NIS, che li condivide con le Autorità di settore interessate ai fini delle valutazioni di cui all'articolo 11, comma 4, lettera c), del medesimo decreto.
3. Al soggetto NIS è fornito riscontro con la comunicazione dell'Autorità nazionale competente NIS ai sensi dell'articolo 7, comma 3, del decreto NIS.

Articolo 12
(Individuazione da parte dell'Autorità nazionale competente NIS)

1. I soggetti che ricevono una notifica di individuazione da parte dell'Autorità nazionale competente NIS, su proposta delle Autorità di settore, ai sensi dell'articolo 3, comma 13, del decreto NIS, procedono al censimento e alla registrazione alla stregua delle disposizioni del presente capo.
2. In fase di registrazione, tali soggetti prendono visione e confermano gli elementi presenti nella notifica di cui al comma 1.

Articolo 13
(Verifiche di coerenza)

1. Le verifiche di coerenza delle informazioni contenute nelle dichiarazioni sono svolte, a campione, dall'Autorità nazionale competente NIS d'intesa con le Autorità di settore e non sollevano il soggetto NIS dall'obbligo del rispetto dei termini d'uso di cui all'articolo 3 della presente determinazione e, in particolare, dalla responsabilità per le dichiarazioni mendaci di cui al comma 5 del medesimo articolo.
2. Nei casi di cui al comma 1, l'Autorità nazionale competente NIS fornisce riscontro al soggetto entro trenta giorni dalla presentazione della dichiarazione tramite il servizio NIS/Registrazione. Il predetto termine può essere prorogato dall'Autorità nazionale competente NIS, per una sola volta e fino ad un massimo di ulteriori venti giorni, qualora sia necessario svolgere approfondimenti complessi riguardanti la coerenza delle informazioni contenute nella dichiarazione.
3. Ove si renda necessario richiedere al soggetto integrazioni, informazioni aggiuntive o modifiche della dichiarazione, i termini di cui al comma 2 sono sospesi e ricominciano a decorrere dalla data di ricevimento delle integrazioni e delle informazioni che sono rese entro il termine di dieci giorni dalla richiesta. Il tardivo riscontro alle richieste di cui al presente comma può essere motivo di rigetto della dichiarazione.
4. Al termine delle verifiche di coerenza delle informazioni contenute nelle dichiarazioni, l'Autorità nazionale competente comunica, tramite i Servizi NIS al domicilio digitale del soggetto NIS:
   a) l'esito positivo della verifica;
   b) l'esito negativo della verifica.
5. La comunicazione di cui al comma 4, lettera b), non solleva il soggetto NIS dall'obbligo di registrazione di cui all'articolo 7, comma 1, del decreto NIS.

Articolo 14
(Elaborazione dell'elenco dei soggetti NIS e comunicazioni)

1. L'elenco dei soggetti NIS di cui all'articolo 7, comma 2, del decreto NIS è elaborato dall'Autorità nazionale competente NIS sulla base delle informazioni trasmesse dai soggetti NIS ai sensi del capo III della presente determinazione e delle verifiche svolte dalle Autorità di settore ai sensi dell'articolo 11, comma 4, lettera a), del medesimo decreto che, ove necessario, possono proseguire anche successivamente all'elaborazione dell'elenco dei soggetti NIS.
2. Ai sensi del comma 1, il processo di registrazione di cui alla presente determinazione costituisce la fase endoprocedimentale del procedimento di costituzione dell'elenco dei soggetti NIS.
3. Ai sensi dell'articolo 7, comma 3, l'Autorità nazionale competente NIS comunica ai soggetti registrati l'inserimento, o meno, nell'elenco dei soggetti NIS. Ai soggetti inseriti nell'elenco dei soggetti NIS e ai loro punti di contatto viene, altresì, comunicato un codice identificativo univoco, per il soggetto NIS, al fine di facilitare le interlocuzioni con l'Autorità nazionale competente NIS.

Capo IV
Aggiornamento annuale delle informazioni

Articolo 15
(Processo per l'aggiornamento delle informazioni)

1. Dal quindici aprile al 31 maggio 2025, gli utenti aggiornano, tramite il Servizio NIS/Aggiornamento annuale, le informazioni per conto del soggetto per cui operano, assicurandone la correttezza.
2. Per tutti i soggetti NIS:
   a) il punto di contatto si assicura che i propri dati anagrafici e di contatto siano corretti e aggiornati. Ove prevista dall'articolo 4, il punto di contatto si assicura che la delega conferitagli dal rappresentante legale del soggetto sia corretta, aggiornata e conforme a quanto previsto dall'articolo medesimo;
   b) il sostituto punto di contatto si assicura che i propri dati anagrafici e di contatto siano corretti e aggiornati. Ove prevista dall'articolo 5, il sostituto punto di contatto si assicura che la delega conferitagli dal rappresentante legale del soggetto sia corretta, aggiornata e conforme a quanto previsto dall'articolo medesimo;
   c) la segreteria, ove presente, si assicura che i propri dati anagrafici e di contatto siano corretti e aggiornati.
3. Per tutti i soggetti NIS, gli utenti verificano la correttezza e l'aggiornamento:
   a) dei dati anagrafici e di contatto del soggetto NIS. Tali informazioni includono almeno il codice fiscale, la denominazione, l'indirizzo della sede legale, l'indicazione del rappresentante legale, l'elenco dei procuratori generali, il numero di telefono, il domicilio digitale e un indirizzo di posta elettronica ordinaria funzionale;

b) dell'elenco dei componenti degli organi di amministrazione e direttivi, quali persone fisiche responsabili ai sensi dell'articolo 38, comma 5, del decreto NIS;
c) ove applicabile, dell'elenco dei servizi che rientrano nell'ambito di applicazione della direttiva 2022/2555 che il soggetto NIS offre nell'UE e indicando in quali Stati membri;
d) dello spazio di indirizzamento IP pubblico e dei nomi di dominio in uso o nella disponibilità del soggetto NIS, eventualmente distinto a livello di articolazioni di primo livello;
e) dell'elenco degli accordi di condivisione delle informazioni.

4. Per i soggetti NIS di cui all'articolo 7, comma 5, gli utenti verificano la correttezza e l'aggiornamento dell'elenco delle sedi del soggetto NIS nell'Unione, indicandone l'indirizzo.
5. Per i soggetti NIS di cui all'articolo 5, comma 1, lettera b), del decreto NIS, che hanno designato il proprio rappresentante NIS in Italia ai sensi dell'articolo 6 della presente determinazione, gli utenti verificano che dati anagrafici e di contatto del rappresentante NIS siano corretti e aggiornati.
6. Qualora ritenuto opportuno, è data la facoltà di descrivere la struttura organizzativa dell'organizzazione, indicandone la suddivisione in articolazioni di primo livello. Tale descrizione della struttura organizzativa potrà essere impiegata per l'eventuale conferimento di informazioni di dettaglio relative alle articolazioni di primo livello.
7. Gli utenti designati quali punti di contatto confermano, ai sensi del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445, le informazioni fornite e le trasmettono telematicamente tramite il servizio NIS/Aggiornamento annuale all'Autorità nazionale competente NIS. Copia di tali informazioni, per ricevuta, è inviata al domicilio digitale del soggetto.
8. La modifica, confermata da punto di contatto, dell'indicazione del rappresentante legale o dell'elenco dei procuratori generali del soggetto NIS è sottoposta alla convalida del soggetto medesimo, secondo la procedura telematica indicata nella richiesta inviata al domicilio digitale di quest'ultimo.
9. Le modifiche dei dati anagrafici e di contatto del soggetto NIS sono trasmesse, per ricevuta, al domicilio digitale di quest'ultimo.
10. Le modifiche dei dati anagrafici e di contatto degli utenti sono trasmesse, per ricevuta, all'indirizzo di posta elettronica certificata indicata dall'utente stesso o, in subordine, all'indirizzo di posta elettronica ordinaria indicata dall'utente stesso.

Articolo 16
(Elencazione degli organi di amministrazione e direttivi)

1. Ai fini dell'articolo 15, comma 3, lettera b), tramite il Servizio NIS/Aggiornamento annuale, gli utenti elencano i codici fiscali delle persone fisiche che compongono gli organi di amministrazione e direttivi, indicandone l'indirizzo di posta elettronica certificata.
2. Le informazioni di cui al comma 1 sono confermate dal punto di contatto.
3. Ai fini dell'articolo 7, comma 4, lettera c), del decreto NIS, le persone fisiche appartenenti agli organi di amministrazione e direttivi del soggetto NIS accettano tale indicazione

accedendo al Portale ACN, secondo la procedura telematica indicata nella richiesta inviata a loro indirizzo di posta elettronica certificata di cui al comma 1.

Capo V
Disposizioni finali

Articolo 13
(Disposizioni finanziarie)

11. Agli oneri derivanti dalla presente determinazione, a carico dell'Autorità nazionale competente NIS e delle Autorità di settore, si provvede, rispettivamente, con le risorse di cui agli articoli 10 e 11 del decreto NIS.

Articolo 14
(Pubblicità)

1. La presente determinazione è pubblicata sul sito web e sui siti web istituzionali delle Autorità di settore NIS e ne sarà data, altresì, comunicazione tramite pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Articolo 15
(Entrata in vigore)

1. La presente determinazione aggiorna e sostituisce la determinazione ACN n. 38565 del 26 novembre 2024.
2. Per quanto non previsto dalla presente determinazione, si applicano le disposizioni del decreto NIS. La presente determinazione si applica a decorrere dal 15 aprile 2025.

Roma, *data del protocollo*

IL DIRETTORE GENERALE

Bruno Frattasi

Agenzia per la Cybersicurezza Nazionale

Determinazione del Direttore Generale dell'Agenzia per la cybersicurezza nazionale

di cui all'articolo 31, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera l), che, ai sensi dell'articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo.

IL DIRETTORE GENERALE

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

VISTO il decreto legislativo 4 settembre 2024, n. 138, recante "*il recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148"*, c.d. decreto NIS, ed in particolare l'articolo 31, commi 1 e 2, che prevede che, ai fini di cui agli articoli 23, 24, 25, 27, 28 e 29, l'Autorità nazionale competente NIS stabilisce obblighi proporzionati tenuto debitamente conto del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico, nonché termini, modalità, specifiche e tempi graduali di implementazione di tali obblighi;

VISTO l'articolo 40, comma 5, lettera l), del decreto NIS che prevede che tali obblighi sono stabiliti con una o più Determinazioni dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS;

VISTO altresì l'articolo 42, comma 1, lettera c), del decreto NIS, che prevede, in fase di prima applicazione, che l'Autorità nazionale competente NIS stabilisce le modalità e le specifiche di base per l'adempimento ai predetti obblighi;

VISTO il decreto del Presidente del Consiglio dei ministri del 10 marzo 2023, recante la nomina del Prefetto Bruno Frattasi a Direttore generale dell'Agenzia per la cybersicurezza nazionale;

VISTO il "*Framework Nazionale per la Cybersecurity e la Data Protection*", edizione 2025 (Framework nazionale), realizzato dal Centro di ricerca di cyber intelligence and information security (CIS) della Sapienza Università di Roma e dal Cybersecurity national lab del Consorzio interuniversitario nazionale per l'informatica (CINI), in collaborazione con l'Agenzia per la cybersicurezza nazionale (ACN), quale strumento di supporto per le organizzazioni pubbliche e private in materia di strategie e processi volti alla sicurezza informatica;

CONSIDERATO che gli allegati tecnici recanti le predette specifiche di base, illustrate nella seconda riunione plenaria del Tavolo per l'attuazione della disciplina NIS, tenutasi il 28 gennaio

2025, sono stati condivisi con le Autorità di settore e con le associazioni di categoria anche per mezzo dei tavoli settoriali di cui all'articolo 11, comma 4, lettera f), del decreto NIS;

PRESSO ATTO dei riscontri pervenuti;

SENTITO il Tavolo per l'attuazione della disciplina NIS nella riunione del 10 aprile 2025;

RITENUTO di avviare la procedura di informazione ai sensi della Direttiva (UE) n. 2015/1535 del Parlamento europeo e del Consiglio del 9 settembre 2015;

CONSIDERATO il grado di esposizione dei soggetti ai rischi, le dimensioni dei soggetti e la probabilità che si verifichino incidenti, nonché la loro gravità, compreso il loro impatto sociale ed economico;

ADOTTA LA PRESENTE DETERMINAZIONE

Articolo 1
(Definizioni)

1. Ai fini della presente determinazione si intende per:
   a) "decreto NIS", il decreto legislativo 4 settembre 2024, n. 138;
   b) "Agenzia per la cybersicurezza nazionale", l'Agenzia per la cybersicurezza nazionale di cui all'articolo 5, comma 1, del decreto-legge 14 giugno 2021, n. 82;
   c) "Autorità nazionale competente NIS", l'Autorità nazionale competente di cui all'articolo 10, comma 1, del decreto NIS;
   d) "Autorità di settore NIS", le Amministrazioni di cui all'articolo 11, commi 1 e 2, del decreto NIS;
   e) "soggetto NIS", un soggetto, di cui all'articolo 2, comma 1, lettera hhh), del decreto NIS, di natura giuridica pubblica o privata che rientra nell'ambito di applicazione del decreto NIS;
   f) "soggetti essenziali", i soggetti NIS considerati essenziali ai sensi del decreto NIS;
   g) "soggetti importanti", i soggetti NIS considerati importanti ai sensi del decreto NIS;
   h) "comunicazione di inserimento nell'elenco dei soggetti NIS", la comunicazione di cui all'articolo 7, comma 3, lettera a), del decreto NIS;
   i) "organi di amministrazione e direttivi", gli organi di amministrazione e direttivi di cui all'articolo 23 del decreto NIS, ivi incluso, laddove presente, il consiglio di amministrazione dei soggetti NIS;
   j) "misure di sicurezza di base", specifiche di base per gli obblighi di cui agli articoli 23 e 24 del decreto NIS, sviluppate in accordo al Framework nazionale e organizzate in funzioni, categorie, sottocategorie e requisiti;
   k) "incidenti significativi di base", le specifiche di base che descrivono gli incidenti significativi di cui all'articolo 25 del decreto NIS;

l) “sistemi informativi e di rete rilevanti”, sistemi informativi e di rete la cui compromissione comporterebbe un impatto significativo sulla confidenzialità, integrità e disponibilità delle attività e servizi per i quali il soggetto NIS rientra nell’ambito di applicazione del decreto NIS;
m) “fornitori di servizi di registrazione dei nomi di dominio”, i fornitori di cui all’articolo 2, comma 1, lettera oo), del decreto NIS;
n) “gestori di registri dei nomi di dominio di primo livello”, i gestori di cui all’articolo 2, comma 1, lettera pp), del decreto NIS;
o) “soggetti PSNC-NIS”, i soggetti di cui all'articolo 1, comma 2-bis, del decreto-legge n. 105 del 2019 che sono soggetti NIS;
p) “sistemi informativi e di rete PSNC”, sistemi informativi e di rete che sono inseriti nell'elenco di cui all'articolo 1, comma 2, lettera b), del decreto-legge n. 105 del 2019
q) “operatori di servizi essenziali”, c.d. OSE, i soggetti NIS identificati prima della data di entrata in vigore del decreto NIS come operatori di servizi essenziali ai sensi del decreto legislativo 18 maggio 2018, n. 65;
r) “sistemi informativi e di rete OSE”, sistemi informativi e di rete dell’operatore di servizi essenziali che abilitano i servizi essenziali per i quali l’operatore stesso è stato identificato ai sensi del decreto legislativo 18 maggio 2018, n. 65;
s) “operatori telco”, i soggetti NIS che forniscono reti pubbliche di comunicazione elettronica o servizi di comunicazioni elettroniche accessibili al pubblico ai sensi del decreto legislativo 1° agosto 2003, n. 259, ad un numero di utenti pari o superiore, anche alternativamente:
    1) all’1% della base di utenti nazionale, calcolato sulla base dei dati pubblicati dall’Osservatorio trimestrale delle comunicazioni a cura dell’Autorità per le garanzie nelle comunicazioni;
    2) a un milione;
t) “sistemi informativi e di rete telco”, sistemi informativi e di rete per l’accesso alla rete fissa o mobile, da postazione o da terminale mobile, individuati come critici dall’operatore telco in quanto potenzialmente in grado di servire, per ciascun servizio indicato:
    1) una percentuale dell’utenza pari o superiore all’1% della base di utenti nazionale per quel servizio, sulla base dei dati pubblicati dall’Osservatorio trimestrale delle comunicazioni a cura dell’Autorità per le garanzie nelle comunicazioni;
    2) un’utenza pari o superiore a un milione.

Articolo 2
(Adozione delle specifiche di base)

1. In fase di prima applicazione del decreto NIS sono adottate le specifiche di base di cui agli allegati 1, 2, 3 e 4, facenti parte integrante della presente determinazione.

2. Le misure di sicurezza di base, a carico degli organi di amministrazione e direttivi e in materia di misure di gestione dei rischi per la sicurezza informatica, sono stabiliti:

    a) per i soggetti importanti, nell’allegato 1;
    b) per i soggetti essenziali, nell’allegato 2.

3. Gli incidenti significativi di base sono stabiliti:
   a) per i soggetti importanti, nell'allegato 3;
   b) per i soggetti essenziali, nell'allegato 4.

Articolo 3
(Termini per l'adozione delle specifiche di base)

1. Il termine per l'adozione delle misure di sicurezza di base di cui agli allegati 1 e 2 è fissato in diciotto mesi dalla ricezione, da parte del soggetto NIS della comunicazione di inserimento nell'elenco dei soggetti NIS.
2. Il termine per l'adempimento dell'obbligo di notifica degli incidenti significativi di base descritti negli allegati 3 e 4 è fissato in nove mesi dalla ricezione, da parte del soggetto NIS, della comunicazione di inserimento nell'elenco dei soggetti NIS.

Articolo 4
(Sicurezza, stabilità e resilienza dei sistemi di nomi di dominio)

1. Fermo restando quanto previsto dall'articolo 29 del decreto NIS, entro diciotto mesi dalla ricezione della comunicazione di inserimento nell'elenco dei soggetti NIS, i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio si adeguano alle previsioni di cui al predetto articolo, commi 1 e 2, nonché adottano e rendono pubbliche le politiche e le procedure di cui al comma 3 del medesimo articolo.
2. Le modalità di adeguamento alle previsioni di cui all'articolo 29, commi 1 e 2, nonché le politiche e le procedure di cui al comma 3 del medesimo articolo sono approvate dagli organi di amministrazione e direttivi.
3. Ai sensi dell'articolo 32, comma 3, i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio adottano politiche al fine di assicurare un livello di sicurezza informatica coerente con le specifiche di cui all'allegato 1.
4. Le politiche di sicurezza informatica di cui al comma 3 sono approvate dagli organi di amministrazione e direttivi.

Articolo 5
(Obblighi di notifica per i soggetti PSNC-NIS)

1. Fermo restando quanto previsto dall'articolo 33 del decreto NIS, i soggetti PSNC-NIS notificano gli incidenti significativi di base di cui all'allegato 4, ai sensi dell'articolo 25 del decreto NIS, limitatamente ai sistemi informativi e di rete diversi da quelli PSNC.
2. Il termine per l'obbligo di cui al comma 1 decorre dalla data di entrata in vigore della presente determinazione.

Articolo 6
(Regime transitorio per gli operatori di servizi essenziali)

1. Fermo restando quanto previsto dall'articolo 2, comma 2, e dall'articolo 3, comma 1, gli operatori di servizi essenziali, limitatamente ai sistemi informativi e di rete OSE, per quanto non in contrasto con la legge e il decreto NIS, assicurano il mantenimento delle misure tecniche e organizzative già adottate prima dell'entrata in vigore del decreto NIS ai sensi del decreto legislativo 18 maggio 2018, n. 65.
2. Al fine di assicurare la continuità dell'obbligo di notifica di incidente di cui all'articolo 12, comma 5, del decreto legislativo 18 maggio 2018, n. 65, dall'entrata in vigore della presente determinazione, ai sensi dell'articolo 25 del decreto NIS, gli operatori di servizi essenziali, limitatamente ai sistemi informativi e di rete OSE, notificano gli incidenti significativi di base di cui:
    a) all'allegato 3, qualora siano soggetti importanti;
    b) all'allegato 4, qualora siano soggetti essenziali.
3. Il termine per gli adempimenti di cui al presente articolo decorre dalla data di entrata in vigore della presente determinazione.

Articolo 7
(Regime transitorio per gli operatori telco)

1. Fermo restando quanto previsto dall'articolo 2, comma 2, e dall'articolo 3, comma 1, gli operatori telco, limitatamente ai sistemi informativi e di rete telco, per quanto non in contrasto con la legge e il decreto NIS, assicurano il mantenimento delle misure di sicurezza e di integrità delle reti e dei servizi già adottate prima dell'entrata in vigore del decreto NIS ai sensi del decreto del Ministro dello sviluppo economico del 12 dicembre 2018.
2. Al fine di assicurare la continuità dell'obbligo di notifica di incidente di cui all'articolo 40, comma 3, lettera b), del decreto legislativo 1° agosto 2003, n. 259, ai sensi dell'articolo 25 del decreto NIS, dall'entrata in vigore della presente determinazione, gli operatori telco, limitatamente ai sistemi informativi e di rete telco, notificano gli incidenti significativi di base:
    a) di cui all'allegato 3, qualora siano soggetti importanti;
    b) di cui all'allegato 4, qualora siano soggetti essenziali.
3. Ai fini del comma 2, nella definizione del livello di servizio atteso di cui agli allegati 3 e 4, gli operatori telco considerano come incidenti significativi di base i seguenti casi:
    a) durata superiore ad un'ora e percentuale degli utenti colpiti superiore al quindici per cento del totale degli utenti nazionali del servizio interessato;
    b) durata superiore a due ore e percentuale degli utenti colpiti superiore al dieci per cento del totale degli utenti nazionali del servizio interessato;
    c) durata superiore a quattro ore e percentuale degli utenti colpiti superiore al cinque per cento del totale degli utenti nazionali del servizio interessato;

d) durata superiore a sei ore e percentuale degli utenti colpiti superiore al due per cento del totale degli utenti nazionali del servizio interessato;
e) durata superiore ad otto ore e percentuale degli utenti colpiti superiore all'uno per cento del totale degli utenti nazionali del servizio interessato.

4. Il termine per gli adempimenti di cui al presente articolo decorre dalla data di entrata in vigore della presente determinazione.

Articolo 8
(Disposizioni finanziarie)

1. Dalla presente determinazione non derivano nuovi o maggiori oneri a carico della finanza pubblica, anche ai sensi dell'articolo 12, comma 6, del decreto NIS.

Articolo 9
(Pubblicità)

1. La presente determinazione è pubblicata sui siti web istituzionali dell'Agenzia per la cybersicurezza nazionale e delle Autorità di settore NIS. Ne sarà data, altresì, comunicazione tramite pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Articolo 10
(Entrata in vigore e disposizioni transitorie)

1. Per quanto non previsto dalla presente determinazione, si applicano le disposizioni del decreto NIS.
2. La presente determinazione entra in vigore a decorrere dal 30 aprile 2025.
3. L'articolo 2, commi 2 e 3, e l'articolo 3 entrano in vigore il giorno successivo all'esperimento della procedura di informazione ai sensi della Direttiva (UE) n. 2015/1535 del Parlamento europeo e del Consiglio del 9 settembre 2015.

Roma, *data del protocollo*

IL DIRETTORE GENERALE
Bruno Frattasi

Firmato digitalmente da: Bruno Frattasi
Data: 14/04/2025 10:52:39

ALLEGATO 1

Misure di sicurezza di base per i soggetti importanti

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 compreso[1].

1.1.1. **GV.OC-4**: 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)**: I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.

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 almeno un suo sostituto, di cui alla determina 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 verifichino incidenti

[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".

significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

1.3.2. **GV.RR-04**: La cybersecurity è incluso 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.

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;
   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.

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.

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.

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, le cui forniture hanno un potenziale impatto 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 impatto 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-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.

2.2.2. **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 verifichino incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.
3. La valutazione del rischio cui al punto 1 è approvata dagli organi di amministrazione e direttivi.

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

1. È definito, documentato, eseguito e monitorato un piano di trattamento del rischio 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 del rischio informatico 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.

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.

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 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 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 che comprende almeno:
   a) i ruoli e 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 verifichino 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 e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono impiegate modalità 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 1e 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.

3.3. **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 e 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 e documentate ragioni normative o tecniche, è disabilitata l'auto esecuzione dei supporti rimovibili 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, e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, ivi inclusi quelli di comunicazione vocale, video e testuale, 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.

3.4. **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-02**: Il software è mantenuto, sostituito e rimosso in base al rischio.

1. Fatte salve motivate e documentate ragioni normative o tecniche, 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 1e 2.

3.4.2. **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 conservati in modo sicuro, e possibilmente centralizzato, 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.

3.4.3. **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 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 1, 2 e 3.

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 ai punti 1 e 2.

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 delle postazioni terminali 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 verifichino 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 loro servizi, gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi;
   b) ai destinatari dei 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 rispristino 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.

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 e 3. 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 e 2.
d) Conformità e audit di sicurezza.	GV.PO-01: punti 1, 2 e 3. GV.PO-02: punti 1 e 2. ID.IM-01: punti 1 e 2.
e) Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento.	GV.SC-01: punto 1. 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-04: punto 1.
g) Gestione delle vulnerabilità.	ID.RA-01: punto 1. ID.RA-08: punti 1, 2, 3 e 4.
h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi.	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.
l) Sicurezza dei dati.	PR.DS-01: punti 1 e 2. PR.DS-02: punto 1. PR.DS-11: punto 1.
m) Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete.	PR.PS-02: punti 1, 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.
o) Monitoraggio degli eventi di sicurezza.	DE.CM-01: punti 1 e 2. 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.

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

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

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 compreso[1].

1.1.1. **GV.OC-4**: 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)**: I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.

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 almeno un suo sostituto, di cui alla determina 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 verifichino incidenti

[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".

significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

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;
   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.

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, le cui forniture hanno un potenziale impatto 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 impatto 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 verifichino incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.
3. La valutazione del rischio 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, prioritizzate, pianificate, monitorate e comunicate.

1. È definito, documentato, eseguito e monitorato un piano di trattamento del rischio 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 del rischio informatico 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 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 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 che comprende almeno:
   a) i ruoli e 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 verifichino 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 e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono impiegate modalità 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 1e 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 e 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 e documentate ragioni normative o tecniche, è disabilitata l'auto esecuzione dei supporti rimovibili 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, e 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, 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, 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 1e 2.
4. Fatte salve motivate e documentate ragioni normative o tecniche e 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 conservati in modo sicuro, e possibilmente centralizzato, 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 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 1, 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 ai punti 1 e 2.
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, alle postazioni terminali 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, 5 e 6.

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 delle postazioni terminali 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 verifichino 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 loro servizi, gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi;
   b) ai destinatari dei 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 rispristino 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.	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.

ALLEGATO 3

Incidenti significativi di base per i soggetti importanti

Codice	Descrizione
IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-3	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL) stabiliti ai sensi della misura DE.CM-01.

ALLEGATO 4

Incidenti significativi di base per i soggetti essenziali

Codice	Descrizione
IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-3	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL) definiti ai sensi della misura DE.CM-01.
IS-4	Il soggetto NIS ha evidenza, anche sulla base dei parametri quali-quantitativi definiti ai sensi della misura DE.CM-01, dell'accesso, non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.

Agenzia per la Cybersicurezza Nazionale

Determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale

di cui all'articolo 17, comma 4, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera f), recante le modalità con cui i soggetti essenziali e i soggetti importanti notificano all'Autorità nazionale competente NIS la loro partecipazione agli accordi di condivisione delle informazioni sulla sicurezza informatica

IL DIRETTORE GENERALE

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

VISTO il decreto legislativo 4 settembre 2024, n. 138, recante "*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148"* e, in particolare, l'articolo 17, commi 2 e 4, e l'articolo 40, comma 5, lettera f) del medesimo decreto;

CONSIDERATO che i soggetti di cui all'articolo 3 del medesimo decreto notificano all'Autorità nazionale competente NIS la loro partecipazione agli accordi di condivisione delle informazioni sulla sicurezza informatica, ai sensi del richiamato articolo 17, commi 2 e 4;

SENTITO il Tavolo per l'attuazione della disciplina NIS di cui all'articolo 12 del decreto legislativo 4 settembre 2024, n. 138, nella riunione del 10 aprile novembre 2025;

ADOTTA LA PRESENTE DETERMINAZIONE

Articolo 1
(Definizioni)

1. Ai fini della presente determinazione si intende per:
   a) "decreto NIS", il decreto legislativo 4 settembre 2024, n. 138;
   b) "Agenzia per la cybersicurezza nazionale", l'Agenzia per la cybersicurezza nazionale di cui all'articolo 5, comma 1, del decreto-legge 14 giugno 2021, n. 82;
   c) "Autorità nazionale competente NIS", l'Autorità nazionale competente di cui all'articolo 10, comma 1, del decreto NIS;

d) "Autorità di settore NIS", le Amministrazioni di cui all'articolo 11, commi 1 e 2, del decreto NIS;
e) "sito web", il sito web istituzionale dell'Agenzia per la cybersicurezza nazionale (acn.gov.it);
f) "piattaforma digitale", la piattaforma digitale di cui all'articolo 7, comma 1, del decreto NIS, accessibile tramite il Portale ACN per l'erogazione dei Servizi NIS;
g) "soggetto", un soggetto, di cui all'articolo 2, comma 1, lettera hhh), del decreto NIS, di natura giuridica pubblica o privata;
h) "soggetto NIS", un soggetto, che rientra nell'ambito di applicazione del decreto NIS;
i) "accordi di condivisione", gli accordi di condivisione delle informazioni sulla sicurezza informatica, di cui all'articolo 17, comma 2, del decreto NIS, per attuare lo scambio di informazioni pertinenti su base volontaria di cui al comma 1 del medesimo articolo.

Articolo 2
(Oggetto, ambito di applicazione e finalità)

1. La presente determinazione stabilisce le modalità con cui i soggetti NIS notificano all'Autorità nazionale competente NIS la loro partecipazione agli accordi di condivisione.

Articolo 3
(Notifica degli accordi di condivisione)

1. I soggetti NIS, tramite la piattaforma digitale, notificano all'Autorità nazionale competente NIS gli accordi di condivisione, sottoscritti successivamente all'entrata in vigore del decreto NIS.
2. I soggetti NIS condividono con l'Autorità nazionale competente NIS il testo dell'accordo di condivisione, la sua denominazione e l'elenco dei partecipanti.
3. Ai sensi dell'articolo 7, comma 4, del decreto NIS, i soggetti NIS aggiornano l'elenco degli accordi di condivisione dal 15 aprile al 31 maggio di ogni anno.
4. Ai sensi dell'articolo 7, comma 7, del decreto NIS, a partire dal 31 maggio 2025, i soggetti NIS assicurano che l'elenco degli accordi di condivisione notificati tramite la piattaforma digitale è corretto e aggiornato. Essi notificano qualsiasi modifica, ivi incluse la sottoscrizione di nuovi accordi, la risoluzione degli accordi già sottoscritti, le variazioni del testo o dei partecipanti, tempestivamente e, in ogni caso, entro quattordici giorni dalla data della modifica.
5. Le notifiche e gli aggiornamenti di cui al presente articolo sono effettuati secondo i termini, le modalità e i procedimenti stabiliti dalla determinazione di cui all'articolo 7, comma 6, del decreto NIS.

Articolo 4
(Notifica degli accordi di condivisione previgenti)

1. I soggetti NIS procedono alla notifica degli accordi di condivisione, sottoscritti antecedentemente all'entrata in vigore del decreto NIS, entro il 31 maggio 2026 e ancora in atto nella medesima data.

Articolo 5
(Disposizioni finanziarie)

1. Dalla presente determinazione non derivano nuovi o maggiori oneri a carico della finanza pubblica, anche ai sensi dell'articolo 12, comma 6, del decreto NIS.

Articolo 6
(Pubblicità)

1. La presente determinazione è pubblicata sul sito web e sui siti web istituzionali delle Autorità di settore NIS e ne sarà data, altresì, comunicazione tramite pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Articolo 7
(Entrata in vigore)

1. Per quanto non previsto dalla presente determinazione, si applicano le disposizioni del decreto NIS. La presente determinazione si applica a decorrere dal 15 aprile 2025.

Roma, *data del protocollo*

IL DIRETTORE GENERALE

Bruno Frattasi