Agenzia per la Cybersicurezza Nazionale

Linee Guida NIS

Specifiche di base

Guida alla lettura

Settembre 2025

Controllo di versione

VERSIONE	DATA PUBBLICAZIONE	NOTE
1.0	Settembre 2025	Prima pubblicazione.
1.0.1	Settembre 2025	Errata corrige in tabelle Appendice B.
2.0	Dicembre 2025	Correzione refusi. Aggiornamenti riferimenti alla Determinazione di cui all'articolo 31, commi 1 e 2, del decreto NIS, 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. Aggiunte figure con misure di sicurezza di esempio. Rielaborazione del Capitolo 3 con introduzione del modello tipologia di incidente. Errata corrige in tabelle Appendice A. Aggiornamento Appendice B.

INDICE

1. Introduzione

1.1. Premessa

Il decreto legislativo 4 settembre 2024, n. 138[1], da qui in poi indicato come **decreto NIS** o **decreto**, mira a garantire l'aumento del livello di sicurezza informatica del tessuto produttivo e delle Pubbliche Amministrazioni del Paese, in armonia con gli altri Stati membri dell'Unione Europea.

A tal fine, il decreto prevede, tra le varie disposizioni, una serie di adempimenti per i *soggetti di cui all'articolo 2, comma 1, lettera hhh), del decreto, di natura giuridica pubblica o privata che rientrano nell'ambito di applicazione del decreto*, da qui in poi indicati come **soggetti NIS** (o **soggetti**) che, ai sensi di quanto indicato dall'articolo 6 del decreto, sono distinti in **soggetti essenziali** e **soggetti importanti** a seconda del livello di criticità intrinseca dei settori e delle tipologie di soggetti in relazione al rischio informatico, nonché del dimensionamento del soggetto.

Nell'ambito di tali adempimenti, sono previsti, ai sensi degli articoli 23, 24 e 25 del decreto, obblighi per gli organi di amministrazione e direttivi, la gestione dei rischi per la sicurezza informatica e le notifiche di incidente. Nello specifico:

- l'**articolo 23** disciplina gli obblighi in carico agli organi di amministrazione e direttivi[2] dei soggetti NIS;
- l'**articolo 24** disciplina gli obblighi in materia di misure di gestione dei rischi per la sicurezza informatica prevedendo che i soggetti NIS adottino misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che i soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi;
- l'**articolo 25** disciplina gli obblighi sulle notifiche di incidente prevedendo che i soggetti NIS trasmettono al CSIRT Italia[3] ogni incidente che abbia un impatto significativo sulla fornitura dei loro servizi.

Le modalità e le specifiche di base[4] per l'adempimento dei suddetti obblighi sono state stabilite con la determinazione obblighi di base [5] che reca i seguenti allegati tecnici**:**

---

[1] 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.

[2] Organi di cui all'articolo 23 del decreto NIS.

[3] Il gruppo nazionale di risposta agli incidenti di sicurezza informatica ai sensi dell'articolo 15, comma 1, del decreto NIS operante all'interno dell'Agenzia per la cybersicurezza nazionale.

[4] Ai sensi dell'articolo 42, comma 1, lettera c), del decreto NIS, l'Agenzia per la Cybersicurezza Nazionale, in qualità di Autorità nazionale competente NIS, può stabilire, in fase di prima applicazione, modalità e specifiche di base per assicurare la conformità dei soggetti NIS all'adempimento degli obblighi di cui agli articoli 23, 24 e 25 del decreto.

[5] Determinazione di cui all'articolo 31, commi 1 e 2, del decreto NIS, 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.

- **Allegato 1**: misure di sicurezza di base per i soggetti importanti.
- **Allegato 2**: misure di sicurezza di base per i soggetti essenziali.
- **Allegato 3**: incidenti significativi di base per i soggetti importanti.
- **Allegato 4**: incidenti significativi di base per i soggetti essenziali.

Gli allegati tecnici costituiscono le cosiddette **specifiche di base**, ossia:

- le **misure di sicurezza di base** (per brevità indicate anche come **misure di sicurezza**) che i soggetti NIS, sia essenziali che importanti, sono tenuti ad adottare per l'assolvimento degli obblighi di cui agli articoli 23 e 24 del decreto;
- le tipologie di **incidenti significativi di base** (per brevità indicati anche come **incidenti significativi**) che i medesimi soggetti sono tenuti a notificare al CSRIT Italia per l'assolvimento degli obblighi di cui all'articolo 25 del decreto.

Il termine per l'adozione delle misure di sicurezza di base è fissato in **diciotto mesi** dalla ricezione, da parte del soggetto NIS della comunicazione di inserimento nell'elenco dei soggetti NIS[6], mentre quello per l'adempimento dell'obbligo di notifica degli incidenti significativi di base è fissato in **nove mesi** dalla ricezione, da parte del soggetto NIS, della medesima comunicazione.

Per i soggetti *PSNC-NIS*[7] gli *operatori di servizi essenziali*[8] e gli *operatori telco*[9] sono previste specifiche disposizioni in termini di misure di sicurezza e notifica degli incidenti. Nello specifico:

- i soggetti PSNC-NIS, ai sensi dell'articolo 33, comma 1 del decreto NIS, sui beni ICT[10] non sono tenuti ad applicare le disposizioni di cui al decreto NIS. Inoltre, i medesimi soggetti non sono sottoposti agli obblighi di notifica di cui all'articolo 25 decreto NIS per gli incidenti riconducibili a una notifica effettuata ai sensi normativa Perimetro;
- gli *operatori di servizi essenziali*, ai sensi di quanto previsto dalla *determinazione obblighi di base*, 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, sui sistemi informativi e di rete OSE*[11];

---

[6] A partire dal 12 aprile 2025, l'Agenzia per la Cybersicurezza Nazionale (ACN) ha provveduto a comunicare ai soggetti interessati il loro inserimento nell'elenco dei soggetti NIS.

[7] Soggetti di cui all'articolo 1, comma 2-bis, del decreto-legge n. 105 del 2019 che sono anche soggetti NIS.

[8] 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.

[9] 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 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 o a un milione.

[10] I cosiddetti beni ICT, ossia le reti, i sistemi informativi e i servizi informatici inseriti nell'elenco di cui all'articolo 1, comma 2, lettera b), del decreto-legge n. 105/2019, sui quali si applicano gli obblighi discendenti dal predetto decreto.

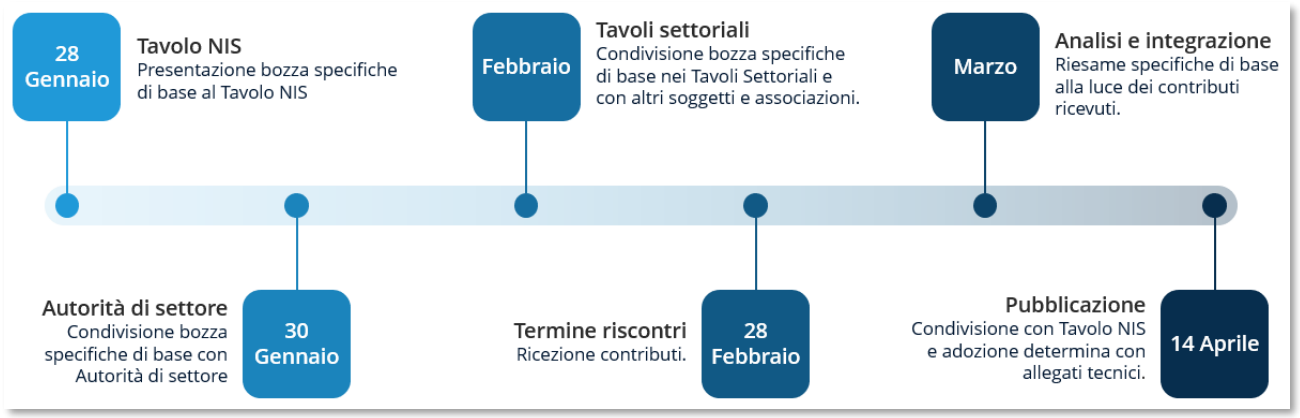
[11] Sistemi informativi e di rete dell'operatore di servizi essenziali che abilitano i servizi essenziali per i quali l'operatore stesso è stato identificato ai sensi del decreto legislativo 18 maggio 2018, n. 65.

- gli *operatori telco*, ai sensi di quanto previsto dalla *determinazione obblighi di base* , assicurano il mantenimento delle misure di sicurezza 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* e nella definizione del livello di servizio atteso di cui agli allegati 3 e 4 della determinazione considerano come incidenti significativi di base i casi di cui all'articolo 5, comma 2, del medesimo decreto ministeriale .

1.1.1. Processo di adozione

Le specifiche di base sono state adottate a seguito di un processo nel quale l'Agenzia per la cybersicurezza Nazionale (ACN) ha condiviso con le Autorità di settore NIS[12] e con le associazioni di categoria, anche per mezzo dei tavoli settoriali[13], il documento contenente la bozza di tali specifiche. Sulla base dei riscontri pervenuti nel corso delle consultazioni, l'ACN ha quindi provveduto a revisionare e finalizzare il documento che è stato infine approvato nel corso della riunione del Tavolo per l'attuazione della disciplina NIS[14] del 10 aprile 2025.

Nella seguente figura è schematizzato il processo di adozione delle specifiche di base.



1.2. Scopo e organizzazione del documento

Il presente documento si propone come una guida alla lettura delle **specifiche di base** (allegati tecnici della **determinazione obblighi di base** contenenti misure di sicurezza e incidenti significativi) ed è stata redatta con l'obiettivo di accompagnare il lettore nella comprensione e interpretazione del testo, evidenziandone e discutendone le caratteristiche peculiari.

Il documento, oltre al capitolo di introduzione, contiene i seguenti capitoli:

- **misure di sicurezza di base**: fornisce un quadro generale delle misure di sicurezza e della loro struttura, presenta l'approccio basato sul rischio secondo il quale sono state sviluppate le misure, esamina le tipologie di requisiti delle misure ed elenca le principali evidenze documentali richieste;

[12] Amministrazioni designate quali Autorità di settore di cui all'articolo 11, commi 1 e 2 del decreto NIS.

[13] Tavoli settoriali di cui all'articolo 11, comma 4, lettera f), del decreto NIS.

[14] Tavolo di cui all'articolo 12 del decreto NIS, costituito per assicurare l'implementazione e attuazione del decreto.

- **incidenti significativi di base**: fornisce un quadro generale degli incidenti significativi e della loro struttura e illustra i concetti di *evidenza dell'incidente* e di *abuso dei privilegi concessi*.

Sono inoltre presenti le seguenti appendici:

- **appendice A – corrispondenza elementi misure**: contiene la mappatura tra le misure di sicurezza e gli elementi di cui all'articolo 24, comma 2, del decreto NIS;
- **appendice B – requisiti con clausole basate sul rischio**: elenca i requisiti per i quali sono previste le clausole relative all'approccio basato sul rischio;
- **appendice C – documenti approvati dagli organi di amministrazione e direttivi**: elenca i documenti che devono essere approvati dagli organi di amministrazione e direttivi;
- **appendice D – glossario**: riporta le definizioni dei termini peculiari che ricorrono nelle specifiche di base.

1.3. Soggetti destinatari

I destinatari del presente documento sono i soggetti NIS essenziali e importanti .

1.4. Termini e definizioni

Nella seguente tabella sono elencate le definizioni dei termini peculiari usati nel presente documento.

TERMINE	DEFINIZIONE
Decreto NIS	Decreto legislativo 4 settembre 2024, n. 138.
Direttiva NIS	Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione.
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.
Soggetti essenziali	I soggetti NIS considerati essenziali ai sensi del decreto NIS.
Soggetti importanti	I soggetti NIS considerati importanti ai sensi del decreto NIS.
Determinazione obblighi di base	Determinazione di cui all'articolo 31, commi 1 e 2, del decreto NIS, 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.
Specifiche di base	Le specifiche di cui agli allegati 1, 2, 3 e 4 della determinazione obblighi di base.
Misure di sicurezza di base	Specifiche di base per gli obblighi di cui agli articoli 23 e 24 del decreto NIS.
Incidenti significativi di base	Specifiche di base che descrivono gli incidenti significativi di cui all'articolo 25 del decreto NIS.

1.5. Norme di riferimento

NORMA	DESCRIZIONE
Decreto legislativo 4 settembre 2024, n. 138.	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.
Determinazione obblighi di base.	Determinazione di cui all'articolo 31, commi 1 e 2, del decreto NIS, 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.

2. Misure di sicurezza di base

2.1. Quadro generale

Le misure di sicurezza per i soggetti importanti sono riportate nell'allegato 1 della *determinazione obblighi di base*, le misure di sicurezza per i soggetti essenziali sono riportate nell'allegato 2 della medesima determinazione[15].

Le misure sono state sviluppate in accordo al **Framework nazionale**[16] e sono organizzate in funzioni, categorie, sottocategorie e requisiti. Nello specifico, ogni misura è costituita da un **codice identificativo**[17], una **descrizione** e uno o più **requisiti:** il codice identificativo e la descrizione fanno riferimento alle **sottocategorie** del Framework nazionale, i requisiti indicano ciò che è richiesto ai fini dell'implementazione della misura.

Nel complesso sono state definite **37** misure di sicurezza con **87** requisiti per i soggetti importanti e **43** misure di sicurezza con **116** requisiti per i soggetti essenziali.

Sono stati definiti requisiti e misure di sicurezza aggiuntivi per i soggetti essenziali rispetto ai soggetti importanti, in considerazione di quanto indicato dall'articolo 31 del decreto NIS che prevede di tener conto – nello stabilire gli obblighi – 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.

Di questi 29 requisiti, **10** afferiscono a **6** misure previste per i soli soggetti essenziali[18] e **19** afferiscono a **10** misure previste anche per i soggetti importanti[19, 20]. Ad esempio, la misura identificata dal codice **PR.DS-11**, nella versione per i soggetti importanti ha 2 requisiti, nella versione per i soggetti essenziali ha 5 requisiti con 3 requisiti previsti per i soli soggetti essenziali.

Per maggiore chiarezza, si faccia riferimento alla figura seguente nella quale la rappresentazione tabellare e l'uso delle colonne **S_I** (soggetto importante) e **S_E** (soggetto essenziale) permettono di mostrare, in un'unica vista, le versioni della misura in questione per i soggetti importanti e per i soggetti essenziali.

---

[15] Sul sito dell'ACN sono pubblicate anche le versioni in formato **xlsx** delle specifiche di base per soggetti importanti ed essenziali.

[16] Il Framework Nazionale per la Cybersecurity e la Data Protection (FNCS) è uno strumento di supporto alle organizzazioni che necessitano di strategie e processi volti alla protezione dei dati personali e alla sicurezza cyber. L'elemento principale è il cosiddetto Framework Core strutturato in funzioni, categorie e sottocategorie. Le misure di sicurezza di base fanno uso della versione 2025 del framework (https://www.cybersecurityframework.it/).

[17] Il codice identificativo è del tipo **XX**.**YY**-**NN**, dove **XX** rappresenta la funzione, **YY** la categoria ed **NN** la sottocategoria del Framework nazionale.

[18] I codici identificativi di tali misure sono: ID.AM-03, PR.AT-02, PR.PS-01, PR.PS-03, PR.IR-03 e RC.CO-03.

[19] I codici identificativi di tali misure sono: GV.RR-04, GV.PO-02, GV.SC-01, ID.RA-01, ID.RA-05, ID.RA-08, ID.IM-01, PR.DS-11, PR.PS-02 e DE.CM-01.

[20] In considerazione di quanto sopra 27 misure hanno i medesimi requisiti per entrambe le tipologie di soggetto, 10 misure hanno requisiti aggiuntivi per i soggetti essenziali, 6 misure sono previste per i soli soggetti essenziali.

PR.DS-11 ← Codice identificativo

I backup dei dati sono creati, protetti, mantenuti e verificati. ← Descrizione

Requisiti

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

Il cerchio pieno di colore blu nella colona **S_I** indica che il corrispondente requisito si applica ai soggetti importanti e Il cerchio pieno di colore verde nella colona **S_E** indica che il corrispondente requisito si applica ai soggetti essenziali.

Le misure di sicurezza sono state definite in modo da coprire gli **elementi** di cui all'articolo 24, comma 2, del decreto NIS di seguito riportati:

a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi.	b) Gestione degli incidenti.	c) Continuità operativa, inclusa la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi.	d) Sicurezza catena di approvvigionamento, compresi aspetti relativi sicurezza rapporti con diretti fornitori o fornitori di servizi.	e) Sicurezza acquisizione, sviluppo e manutenzione sistemi informativi e di rete, ivi compresa gestione e divulgazione vulnerabilità.
f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza.	g) Pratiche di igiene informatica di base e formazione in materia di cybersicurezza.	h) Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura.	i) Sicurezza risorse umane, strategie di controllo dell'accesso e gestione degli assetti.	j) Uso di soluzioni di autenticazione a più fattori o di autenticazione continua e di sistemi di comunicazione protetti.

Elementi degli obblighi in materia di misure di gestione dei rischi per la sicurezza informatica (art. 24, c. 2 d.lgs. 138/2024)

In Appendice A è riportata la corrispondenza delle misure di sicurezza con tali elementi.

2.2. Ambito di applicazione

Le misure di sicurezza si applicano ai sistemi informativi e di rete che i soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi. L'articolo 2, comma 1, lettera p) definisce un **sistema informativo e di rete** come:

1) una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera vv), del decreto legislativo 1° agosto 2003, n. 259;
2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;
3) I dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione.

2.3. Approccio basato sul rischio

Come osservato nel paragrafo Quadro generale, l'articolo 31 del decreto prevede che, nello stabilire gli obblighi, si tenga conto, tra le altre cose, del grado di esposizione dei soggetti ai rischi.

Nel definire le misure di sicurezza, tale previsione è stata attuata formulando i requisiti in considerazione del differente **grado di esposizione al rischio** che caratterizza ogni sistema informativo e di rete.

Tale approccio è stato, in particolare, declinato prevedendo le seguenti **clausole** per specifici requisiti:

- *per almeno i sistemi informativi e di rete rilevanti*;
- *in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05*;
- *fatte salve motivate e documentate ragioni normative o tecniche*;
- *forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete*.

Quando in un requisito è presente una combinazione di tali clausole, le stesse sono da intendersi applicate *in cascata*. Ad esempio, la concatenazione delle clausole "*per almeno i sistemi informativi e di rete*" e "*in accordo agli esiti della valutazione del rischio*", determina che il requisito deve essere applicato almeno sui sistemi informativi e di rete rilevanti per i quali i risultati della valutazione del rischio ne richiedono l'attuazione[21].

In Appendice B è riportato l'elenco dei requisiti per i quali sono previste le suddette clausole.

2.3.1. Sistemi informativi e di rete rilevanti

Per i requisiti[22] in cui è presente la clausola "*… per almeno i sistemi informativi e di rete rilevanti …*", il soggetto NIS ha la facoltà di limitare **l'ambito di applicazione** delle relative disposizioni ai sistemi **informativi e di rete rilevanti**[23], definiti – ai sensi dell'articolo 1 della *determinazione obblighi di base* – come i *sistemi informativi e di rete la cui compromissione comporterebbe un impatto significativo sulla riservatezza, integrità e disponibilità delle attività e dei servizi per i quali il soggetto rientra nell'ambito di applicazione del decreto NIS*.

Ad esempio, per effetto di tale clausola, la verifica periodica mediante test di ripristino dell'utilizzabilità dei backup effettuati (misura prevista dal requisito 4 della misura PR.DS-11) potrà essere limitata ai soli sistemi informativi e di rete *rilevanti*.

---

[21] Come verrà discusso nel paragrafo Esiti della valutazione del rischio , la clausola *in accordo agli esiti della valutazione del rischio*, determina le modalità e l'ambito di attuazione in funzione dei risultati della valutazione del rischio.

[22] **13** requisiti per i soggetti importanti e **22** requisiti per i soggetti essenziali.

[23] La misura GV.OC-04 richiede di mantenere un elenco dei sistemi informativi e di rete rilevanti.

PR.DS-11

I backup dei dati sono creati, protetti, mantenuti e verificati.

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

Ai fini dell'individuazione dei sistemi informativi e di rete rilevanti, in accordo alla definizione presente nella determina, il soggetto:

1) identifica attività e servizi per i quali rientra nell'ambito di applicazione del decreto (*attività e servizi NIS*);
2) valuta l'impatto di una compromissione dei sistemi informativi e di rete, in termini di riservatezza, integrità e disponibilità, sulle attività e sui servizi NIS;
3) individua come sistemi informativi e di rete *rilevanti* quelli per i quali la valutazione di cui al punto 2 determina un impatto significativo.

Si osserva, inoltre, che ai fini della valutazione dell'impatto, non è richiesto l'uso di una specifica metodologia, ogni soggetto potrà pertanto utilizzare quella maggiormente adatta al proprio contesto.

2.3.2. In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05

Per i requisiti[24] in cui è presente la clausola "*... in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05 ...*", le **modalità di attuazione** (*come* è applicato il requisito) e **l'ambito di attuazione** (*dove* è applicato il requisito) sono definiti in funzione dei risultati della valutazione del rischio fatta dal soggetto ai sensi della misura ID.RA-05.

Con riferimento alle **modalità di attuazione**, si consideri ad esempio il requisito 2 della misura PR.AA-01 che richiede che le credenziali delle utenze siano robuste e aggiornate in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05.

[24] **6** requisiti per i soggetti importanti e **10** requisiti per i soggetti essenziali.

PR.AA-01

Le identità e le credenziali degli utenti, dei servizi e dell'hardware autorizzati sono gestite dall'organizzazione.

PUNTO	REQUISITO	S_I	S_E
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.	●	●

Sulla base di tale previsione, il soggetto potrà definire le modalità di attuazione (in questo caso requisiti, complessità e frequenza aggiornamento credenziali) stabilendo, ad esempio, requisiti e frequenza maggiori per le utenze con privilegi amministrativi (che tipicamente presentano rischi elevati) rispetto a quelle senza privilegi.

Con riferimento all'**ambito di attuazione**, si consideri ad esempio il requisito 2 della misura PR.AA-03 che richiede di impiegare soluzioni di autenticazione multifattore per almeno i sistemi informativi e di rete rilevanti, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05.

PR.AA-03

Utenti, servizi e hardware sono autenticati

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

Sulla base di tale previsione, il soggetto potrà definire l'ambito di attuazione (in questo caso su quali sistemi informativi e di rete rilevanti impiegare le soluzioni di autenticazione multifattore) sulla base della valutazione del rischio dalla quale potrebbe risultare che per – uno specifico sistema informativo e di rete rilevante (e.g., un sistema *standalone* e per il cui accesso fisico siano già in essere procedure di autenticazione e autorizzazione)

– il livello di rischio sia trascurabile, o comunque entro la soglia di accettazione del rischio, anche senza l'impiego dell'autenticazione multifattore[25].

2.3.3. Fatte salve motivate e documentate ragioni normative o tecniche

Per i requisiti[26] in cui è presente la clausola "… *fatte salve motivate e documentate ragioni normative o tecniche …*", il soggetto può derogare dall'applicazione se sussistono vincoli normativi (ad esempio, leggi o regolamenti) o tecnici (ad esempio, limiti tecnologici o funzionali) che non ne permettano l'implementazione.

In questi casi il soggetto dovrà motivare e documentare tali vincoli e, ai sensi del punto 2 della misura ID.RA-06, dovrà adottare, ove applicabile, **misure di mitigazione compensative** e includere nel piano di trattamento del rischio[27] la descrizione delle misure e dell'eventuale rischio residuo.

Si consideri al riguardo il requisito 1 della misura DE.CM-09 che richiede, *fatte salve motivate e documentate ragioni normative o tecniche,* la presenza sistemi di protezione dei punti terminali (*endpoint*) per il rilevamento del codice malevolo.

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.

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

Tale requisito potrebbe tuttavia non essere applicabile nel caso di *endpoint* come, ad esempio, i dispositivi medici per i quali un'eventuale installazione dei sistemi di protezione ne potrebbe invalidare la certificazione.

2.3.4. Forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete

Per i requisiti[28] in cui è presente la clausola "*… forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete …*", il soggetto ha la facoltà di limitare **l'ambito di attuazione** delle relative disposizioni alle forniture la cui eventuale compromissione può determinare effetti sulla sicurezza dei sistemi informativi e di rete, ossia– coerentemente con la definizione di cui all'articolo 2, comma 1, lettera q) del decreto NIS – sulla loro capacità

[25] Sia la clausola "…*in accordo agli esiti della valutazione del rischio* …" che la clausola "… *per almeno i sistemi informativi e di rete rilevanti* …" definiscono l'ambito di attuazione del requisito in cui sono presenti. La prima definisce un ambito sulla base dei risultati della valutazione del rischio, la seconda sulla base dei sistemi informativi e di rete rilevanti.

[26] **8** requisiti per i soggetti importanti e **10** per i soggetti essenziali.

[27] Richiesto ai sensi del punto 1 della misura ID.RA-06.

[28] **3** requisiti per i soggetti importanti ed essenziali.

di resistere, con un determinato livello di affidabilità, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi.

2.4. Tipologia requisiti

I requisiti indicano *cosa* deve fare un soggetto per essere conforme alle misure di sicurezza e possono essere distinti in due tipologie:

- **organizzativi**: riguardano principalmente la gestione, l'organizzazione, la documentazione e il controllo di processi e attività. Requisiti organizzativi sono, ad esempio, quelli che richiedono l'adozione e l'approvazione di politiche o procedure, la definizione di piani e processi o la redazione di documentazione;
- **tecnologici**: implicano l'adozione e l'utilizzo di strumenti e soluzioni tecnologiche. Requisiti tecnologici sono, ad esempio, quelli che richiedono la cifratura dei dati, l'aggiornamento del software o l'impiego di modalità di autenticazione multifattore.

In considerazione del fatto che si tratta di misure di sicurezza connesse agli obblighi di base, i relativi requisiti sono per la maggior parte di tipo organizzativo come, ad esempio, i requisiti della misura *GV.RR-02* (definizione dell'organizzazione di sicurezza informatica e relativi ruoli e responsabilità) oppure della misura *GV.PO-01* (adozione e documentazione di politiche di sicurezza informatica). Risulta, infatti, fondamentale costruire anzitutto una solida governance della sicurezza informatica. L'adozione e l'utilizzo di strumenti e soluzioni tecnologiche dovrebbero, infatti, essere a supporto dalle procedure e dei processi definiti dall'organizzazione, in coerenza con le politiche.

Requisiti come, ad esempio, quelli della misura *DE.CM-01* (monitoraggio di eventi potenzialmente avversi), sono invece di tipo tecnologico e, nello specifico, riguardano l'adozione di sistemi di rilevamento delle intrusioni e di strumenti di analisi e filtraggio del traffico in ingresso.

2.5. Evidenze documentali

Il soggetto, ai fini dell'attuazione delle misure di sicurezza e dell'attestazione dell'effettiva implementazione delle stesse, deve essere in possesso o provvedere all'elaborazione di una serie di documenti. A seguire sono riportati i principali documenti richiesti (in *corsivo* quelli relativi ai soli soggetti essenziali) raggruppati per tipologie:

- **elenchi**: personale dell'organizzazione di sicurezza informatica, *configurazioni di riferimento*, sistemi ai quali è possibile accedere da remoto;
- **inventari**: apparati fisici, servizi, sistemi e applicazioni software, *flussi di rete*, servizi erogati dai fornitori, fornitori;
- **piani**: valutazione dei rischi, continuità operativa, ripristino in caso di disastro, trattamento dei rischi, gestione delle vulnerabilità, adeguamento, *valutazione dell'efficacia delle misure di gestione del rischio*, formazione in materia di sicurezza informatica, risposta agli incidenti;

- **politiche di sicurezza informatica**: per almeno i requisiti riportati nella tabella 1 in appendice all'allegato 1, per i soggetti importanti, e all'allegato 2, per i soggetti essenziali, della *determinazione obblighi di base*;
- **procedure**: in relazione agli specifici requisiti per i quali sono richieste;
- **registri**: esiti del riesame delle politiche, attività formazione dei dipendenti, *manutenzioni effettuate*.

In base al proprio contesto, il soggetto può decidere come organizzare la propria documentazione la richiesta da una specifica misura, ad esempio raggruppando i contenuti in un unico documento o distribuendoli tra più documenti.

Per i documenti elencati in Appendice C è richiesta l'approvazione degli organi di amministrazione e direttivi.

I documenti possono essere resi disponibili in formato cartaceo o digitale, purché facilmente fruibili da chi ha la necessità di conoscerlo e consultarlo.

3. Incidenti significativi di base

3.1. Quadro generale

Gli incidenti significativi per i soggetti importanti sono riportati nell'allegato 3 della *determinazione obblighi di base*, gli incidenti significativi per i soggetti essenziali sono riportati nell'allegato 4 della medesima determinazione.

Ogni tipologia di incidente significativo è costituita da un **codice identificativo** e da una **descrizione**. Nel complesso sono state definite **3** tipologie di incidenti significativi per i soggetti importanti e **4** tipologie di incidenti significativi per i soggetti essenziali[29].

Nella seguente tabella sono riportati gli incidenti significativi di base previsti dalla determinazione dove il cerchio pieno di colore blu nella colona **S_I** indica che il corrispondente incidente si applica ai soggetti importanti, mentre Il cerchio pieno di colore verde nella colona **S_E** indica che si applica ai soggetti essenziali.

CODICE	DESCRIZIONE	S_I	S_E
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 digitali 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.		●

In considerazione del cosiddetto *approccio multi-rischio*[30] e della definizione di *incidente*[31] del decreto NIS, gli incidenti oggetto di notifica ricomprendono anche quelli dovuti ad eventi di natura accidentale – e dunque non

[29] Come fatto per le misure di sicurezza, si è proceduto a differenziare gli incidenti significativi in base alla tipologia di soggetto (essenziale o importante) prevedendo, per i soggetti essenziali, 1 tipologia di incidente aggiuntiva.

[30] L'articolo 2, comma 2, lettera dd), del decreto definisce *approccio multi-rischio* come "*approccio alla gestione dei rischi che considera quelli derivanti da tutte le tipologie di minaccia ai sistemi informativi e di rete nonché al loro contesto fisico, quali furti, incendi, inondazioni, interruzioni, anche parziali, delle telecomunicazioni e della corrente elettrica, e in generale accessi fisici non autorizzati*".

[31] L'articolo 2, comma 2, lettera t), del decreto definisce *incidente* come un "*evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi" considerando quindi sia la natura intenzionale che accidentale dell'evento*".

solo intenzionale – come, ad esempio, il *fault* o il malfunzionamento dei sistemi, anche generati a causa di un errore umano, che hanno impatto, ad esempio, sulla disponibilità dei sistemi.

3.2. Modello tipologia di incidente

Ogni tipologia di incidente può essere descritta da un modello costituito dai seguenti elementi:

- **condizione**: circostanza che determina l'obbligo di notifica;
- **compromissione**: evento di sicurezza per il quale si configura l'incidente significativo;
- **oggetto compromissione**: risorsa sul quale l'evento di sicurezza ha impatto.

Sulla base di tale modello, le tipologie di incidente possono essere rappresentate nella seguente tabella[32].

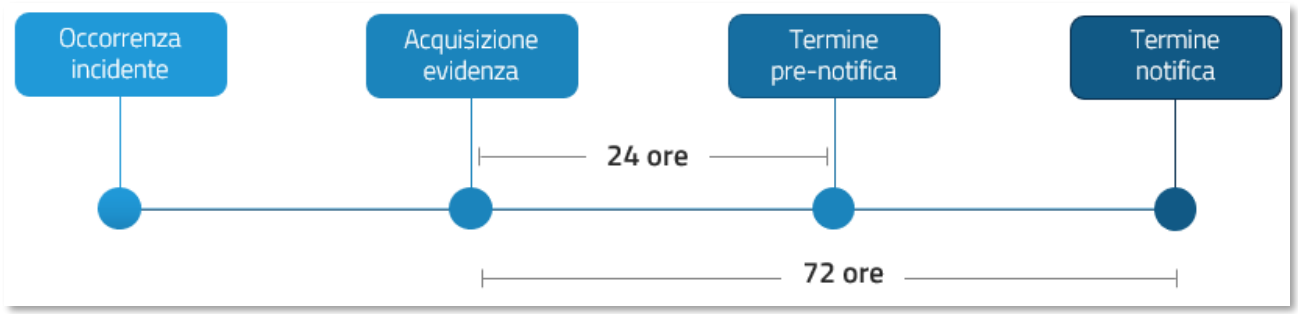
CODICE	CONDIZIONE	COMPROMISSIONE	OGGETTO COMPROMISSIONE
IS-1	Il soggetto ha evidenza	Perdita di riservatezza, verso l'esterno.	Dati digitali
IS-2		Perdita di integrità, con impatto verso l'esterno.	Dati digitali
IS-3		Violazione dei livelli di servizio attesi.	Servizi e/o attività
IS-4		Accesso non autorizzato o con abuso dei privilegi concessi	Dati digitali

Nelle successive sezioni del paragrafo sono discussi gli elementi sopra indicati.

3.2.1. Condizione

La *condizione* che determina l'obbligo di notifica è che il soggetto abbia **evidenza** dell'incidente, ossia sia venuto a conoscenza del verificarsi di una delle tipologie di incidente previste. Con *evidenza dell'incidente* si intende che il soggetto dispone di elementi oggettivi dai quali si evince che è occorso un incidente di sicurezza informatica.

L'acquisizione dell'evidenza è tipicamente successiva al verificarsi dell'incidente e definisce il momento dal quale decorre il termine per la trasmissione della pre-notifica (24 ore) e della notifica (72 ore), come si può osservare dalla figura seguente.



[32] Per semplificazione non è riportata la dicitura completa delle varie tipologie di incidenti significativi.

L'evidenza di un incidente viene generalmente acquisita tramite:

- analisi di segnalazioni fatte da attori esterni al soggetto, come ad esempio quelle effettuate dal CSIRT Italia;
- analisi di segnalazioni fatte da attori interni al soggetto, come ad esempio quelle di un utente che riporta un malfunzionamento al servizio di help desk;
- analisi degli eventi di sicurezza rilevati dai sistemi di monitoraggio.

Con riferimento alla tipologia di incidente identificata dal codice **IS-4**, prevista per i soli soggetti essenziali, si rileva che l'evidenza deve essere acquisita anche sulla base dei **parametri quali-quantitativi**[33] che sono definiti dal soggetto ai sensi di quanto previsto dalla misura DE.CM-01.

3.2.2. Compromissione

In questa sezione sono discusse le varie tipologie di compromissione per le quali si configura un incidente significativo.

Perdita di riservatezza verso l'esterno

La *perdita di riservatezza verso l'esterno* si configura quando dati digitali, che dovrebbero essere accessibili solo a utenti o sistemi autorizzati, sono divulgati o esposti, in modo intenzionale o accidentale, a utenti o sistemi esterni al soggetto, configurando così una compromissione che comporta la fuoriuscita dei dati verso l'esterno.

Esempi di tale fattispecie sono l'esfiltrazione di documenti dagli archivi digitali dell'organizzazione o l'esposizione sulla rete *Internet* di credenziali degli utenti.

Perdita di integrità con impatto verso l'esterno

la *perdita di integrità con impatto verso l'esterno* si configura quando dati digitali sono modificati senza autorizzazione determinando impatti verso utenti o sistemi esterni al soggetto.

Esempi di tale fattispecie sono il *defacement* del sito web dell'organizzazione, la corruzione o l'alterazione di un database che rende disponibili all'esterno dati inconsistenti o errati.

Violazione dei livelli di servizio attesi

la *violazione dei livelli di servizio attesi* si configura quando i livelli di servizio attesi – definiti dal soggetto ai sensi di quanto previsto dalla misura DE.CM-01 – non sono rispettati.

I *livelli di servizio attesi* (indicati con l'acronimo SL) sono stabiliti in autonomia dal soggetto e rappresentano gli obiettivi, indicati in termini misurabili, che definiscono le prestazioni attese dei servizi e delle attività del soggetto. Sono generalmente espressi in termini di disponibilità del servizio/attività e non necessariamente coincidono con i livelli di servizio definiti nei contratti (denominati generalmente *SLA* o *Service Level Agreement*).

[33] Insieme di indicatori di tipo qualitativo e quantitativo, definiti dal soggetto al fine di rilevare accessi non autorizzati o con abuso dei privilegi concessi sui propri sistemi informativi e di rete. Un esempio di indicatore di tipo quantitativo è il superamento di una soglia per le interrogazioni di una banca dati da parte di un singolo utente, un esempio di indicatore di tipo qualitativo è l'accesso di un amministratore di sistema al di fuori dell'orario di servizio.

Esempi di tale fattispecie sono l'indisponibilità del sito *web* per oltre 30 minuti consecutivi o la limitata disponibilità di un servizio *online* per oltre il 5% degli utenti[34].

Accesso non autorizzato o con abuso dei privilegi concessi

l'*accesso non autorizzato o con abuso dei privilegi concessi* si configura quando un utente o un sistema ottiene accesso a dati digitali senza avere i permessi o i diritti per farlo.

L'uso della dicitura *con abuso dei privilegi concessi* ricomprende quelle fattispecie in cui un utente, ivi inclusi quelli con privilegi amministrativi, ha l'*autorizzazione tecnica*[35] per accedere a determinati dati ma utilizza tale accesso in modo illecito, ad esempio in violazione delle politiche dell'organizzazione o per perseguire scopi estranei alle necessità funzionali per le quali gli è stato attribuito l'accesso.

Esempi di tale fattispecie sono l'uso di credenziali rubate per accedere a specifici *account* di posta elettronica o la consultazione di banche dati da parte di personale che ha l'autorizzazione tecnica ad accedervi, ma in violazione delle politiche.

3.2.3. Oggetto compromissione

Le tipologie di incidente identificate dai codici **IS-1**, **IS-2** e **IS-4** hanno come oggetto della compromissione i dati digitali di proprietà del soggetto o sui quali esercita il controllo anche parziale.

Per *dati digitali di proprietà del soggetto* si intendono i dati creati dall'organizzazione o dei quali ne assume la titolarità, mentre per i *dati digitali sui quali esercita il controllo anche parziale* si intendono i dati per i quali non si detiene la proprietà, ma si dispone di una responsabilità, anche parziale, per il loro trattamento, in forza di contratti, accordi o della normativa vigente, come ad esempio nel caso di un fornitore di servizi *cloud* che gestisce, tramite i propri sistemi informativi e di rete, i dati di un cliente

La tipologia di incidente identificata dal codice **IS-3** ha invece come oggetto dell'evento di sicurezza i servizi o le attività del soggetto NIS.

Per *servizi e attività* si intende tutto quello che *fa* un'organizzazione per il perseguimento dei propri obiettivi, come, ad esempio, la produzione, la logistica o la gestione del personale[36].

[34] Nel primo caso sarà stato definito, come livello di servizio atteso, che il sito web non deve essere indisponibile per più di 30 minuti consecutivi, nel secondo che il servizio *online* deve essere disponibile per almeno il 95% degli utenti.

[35] Per autorizzazione tecnica si intende la disponibilità di credenziali che sono configurate per accedere ai dati.

[36] Nelle attività e servizi sono ricompresi anche le attività e i servizi di supporto.

Appendice A – corrispondenza elementi misure

La seguente tabella riporta la mappatura tra le misure di sicurezza di base e gli elementi di cui all'articolo 24, comma 2 del decreto NIS.

Elemento decreto NIS	Codice misura di sicurezza
a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete.	GV.OC-04, GV.RM-03, GV.RR-02, GV.PO-01, GV.PO-02, ID.RA-05, ID.RA-06.
b) Gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26.	PR.PS-04, DE.CM-01, DE.CM-09, RS.MA-01, RS.CO-02, RC.RP-01, RC.CO-03.
c) Continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi.	ID.IM-04, PR.DS-11.
d) Sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi.	GV.SC-01, GV.SC-02, GV.SC-04, GV.SC-05, GV.SC-07.
e) Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità.	GV.SC-05, ID.RA-01, ID.RA-08, PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-06.
f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica.	ID.IM-01.
g) Pratiche di igiene di base e di formazione in materia di sicurezza informatica.	PR.AT-01, PR.AT-02.
h) Politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura.	PR.DS-01, PR.DS-02.
i) Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti.	GV.RR-04, ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, PR.AA-01, PR.AA-03, PR.AA-05, PR.AA-06, PR.IR-01.
l) Uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.	PR.AA-03, PR.DS-02, PR.IR-03.

Appendice B – requisiti con clausole basate sul rischio

Le seguenti tabelle elencano, rispettivamente per i soggetti essenziali e per i soggetti importanti, i requisiti in cui sono previste le clausole con le quali è declinato l'approccio basato sul rischio delle misure di sicurezza.

Soggetti importanti

Clausola	Riferimento requisito
Per almeno i sistemi informativi e di rete rilevanti	GV.RR-04 punto 1, ID.IM-04 punto 1, ID.IM-04 punto 2, ID.IM-04 punto 3, PR.AA-01 punto 3, PR.AA-03 punto 2, PR.AA-06 punto 1, PR.DS-01 punto 1, PR.DS-02 punto 1, PR.DS-11 punto 1, PR.PS-04 punto 2, PR.IR-01 punto 1, DE.CM-01 punto 1.
In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05	PR.AA-01 punto 1, PR.AA-01 punto 2, PR.AA-03 punto 2, PR.DS-01 punto 1, PR.DS-02 punto 2, PR.PS-02 punto 1.
Fatte salve motivate e documentate ragioni normative o tecniche	GV.SC-05 punto 1, PR.AA-01 punto 1, PR.DS-01 punto 1, PR.DS-01 punto 2, PR.DS-02 punto 1, PR.PS-02 punto 1, PR.PS-02 punto 2, DE.CM-09 punto 1.
Forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete	GV.SC-01 punto 1, GV.SC-04 punto 1, GV.SC-05 punto 1.

Soggetti essenziali

Clausola	Riferimento requisito
Per almeno i sistemi informativi e di rete rilevanti	GV.RR-04 punto 1, ID.RA-01 punto 2, ID.IM-04 punto 1, ID.IM-04 punto 2, ID.IM-04 punto 3, PR.AA-01 punto 3, PR.AA-03 punto 2, PR.AA-06 punto 1, PR.DS-01 punto 1, PR.DS-02 punto 1, PR.DS-11 punto 1, PR.DS-11 punto 3, PR.DS-11 punto 4, PR.PS-01 punto 1, PR.PS-03 punto 1, PR.PS-03 punto 2, PR.PS-04 punto 2, PR.IR-01 punto 1, DE.CM-01 punto 1, DE.CM-01 punto 4, DE.CM-01 punto 5, DE.CM-01 punto 6.
In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05	GV.RR-04 punto 4, PR.AA-01 punto 1, PR.AA-01 punto 2, PR.AA-03 punto 2, PR.DS-01 punto 1, PR.DS-02 punto 2, PR.DS-11 punto 4, PR.PS-02 punto 1, PR.PS-02 punto 4, PR.IR-03 punto 1.
Fatte salve motivate e documentate ragioni normative o tecniche	GV.SC-05 punto 1, ID.RA-01 punto 2, PR.AA-01 punto 1, PR.DS-01 punto 1, PR.DS-01 punto 2, PR.DS-02 punto 1, PR.PS-02 punto 1, PR.PS-02 punto 2, PR.PS-02 punto 4, DE.CM-09 punto 1.
Forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete	GV.SC-01 punto 1, GV.SC-04 punto 1, GV.SC-05 punto 1.

Appendice C – documenti approvati dagli organi di amministrazione e direttivi

La seguente tabella elenca i documenti che devono essere approvati dagli organi di amministrazione e direttivi e i riferimenti ai requisiti che ne richiedono l'approvazione.

Documento	Riferimento requisito
Organizzazione per la sicurezza informatica.	GV.RR-02 punto 1.
Politiche di sicurezza informatica.	GV.PO-01 punto 1.
Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete.	ID.RA-05 punto 3.
Piano di trattamento del rischio.	ID.RA-06 punto 3.
Piano di gestione delle vulnerabilità.	ID.RA-08 punto 4.
Piano di adeguamento.	ID.IM-01 punto 1.
Piano di continuità operativa.	ID.IM-04 punto 1.
Piano di ripristino in caso di disastro.	ID.IM-04 punto 1.
Piano di gestione delle crisi.	ID.IM-04 punto 1.
Piano di formazione.	PR.AT-01 punto 1.
Piano per la gestione degli incidenti di sicurezza informatica.	RS.MA-01 punto 2.

Appendice D – glossario

A seguire sono riportate le definizioni dei termini peculiari che ricorrono nelle specifiche di base.

Abuso dei privilegi concessi

Fattispecie in cui l'utente di un sistema informativo e di rete abbia l'autorizzazione tecnica (disponibilità di credenziali che sono configurate per accedere ai dati) per accedere a determinati dati ma tale acceso sia effettivamente illecito in quanto, ad esempio, effettuato in violazione delle politiche del soggetto o risulti strumentale al perseguimento di scopi estranei alle necessità funzionali di accesso.

Amministratori di sistema

Figure professionali incaricate della gestione e manutenzione dei sistemi informativi e di rete, o di parti di essi, e dotati di accessi privilegiati a tali sistemi per configurarli, monitorarli, aggiornarli o controllarli. Esempi di amministratori di sistema sono gli amministratori dei sistemi operativi, gli amministratori di database, gli amministratori degli apparati di rete, gli amministratori delle soluzioni di sicurezza e gli amministratori di applicazioni software.

Attori interni al soggetto

Figure, appartenenti al soggetto, deputate alla gestione della sicurezza dei sistemi informativi e di rete come, ad esempio, quelle operanti all'interno dell'organizzazione di sicurezza informatica.

Catena di approvvigionamento

Insieme di individui, organizzazioni, risorse e attività coinvolte nella creazione e/o vendita di un bene o di un servizio, quali ad esempio i fornitori di beni e servizi informatici.

Decreto NIS

Il decreto legislativo 4 settembre 2024, n. 138.

Flussi di rete tra i sistemi informativi e di rete del soggetto NIS e l'esterno

Flussi a livello perimetrale e identificati almeno dai seguenti attributi: indirizzo/i IP sorgente, indirizzo/i IP di destinazione, protocollo di trasporto, porta di destinazione, protocollo a livello applicativo (ove presente). Qualora un determinato flusso sia permesso verso qualunque destinazione o provenga da qualunque sorgente, i relativi indirizzi IP possono essere indicati in modo aggregato (e.g. tramite *Any* oppure *).

Ad esempio, il flusso di rete per la navigazione Internet delle postazioni della rete LAN di un soggetto che permette connessioni verso qualunque destinazione, potrà essere identificato da: IP_GW_LAN, Any, TCP, 443, HTTPS, dove *IP_GW_LAN* è l'indirizzo del gateway della rete LAN attestato sul firewall perimetrale, *Any* indica

che il flusso è verso qualunque destinazione, TCP è il protocollo di trasporto, 443 è la porta di destinazione e HTTPS è il protocollo a livello applicativo.

Forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete

Forniture la cui eventuale compromissione può determinare effetti sulla capacità dei sistemi informativi e di rete di resistere, con un determinato livello di affidabilità, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi.

Livelli di servizio attesi dei servizi e delle attività del soggetto NIS

Obiettivi, indicati in termini misurabili, che definiscono le prestazioni attese dei servizi e delle attività del soggetto. Sono generalmente espressi in termini di disponibilità del servizio/attività. Nel caso, ad esempio, di un soggetto che fornisce un servizio di prenotazione *online*, un possibile livello di servizio atteso è *il sistema di prenotazione online deve essere disponibile per almeno il 99% del tempo su base giornaliera*. Si parla di violazione del livello di servizio quando tale livello non è rispettato. Con riferimento all'esempio precedente, qualora il sistema di prenotazione non dovesse essere disponibile per più di 14 minuti e 24 secondi (1% del tempo su base giornaliera) si avrà pertanto una violazione del livello di servizio atteso.

Misure di mitigazione compensative

Misure di sicurezza messe in atto quando non è possibile implementare i requisiti delle misure di sicurezza in cui è presente la dicitura *fatte salve motivate e documentate ragioni normative o tecniche*, e che permettono di ridurre il rischio residuo a un livello accettabile.

Organizzazione per la sicurezza informatica

Insieme delle articolazioni preposte al governo (o *governance*) e alla gestione della sicurezza dei sistemi informativi e di rete del soggetto NIS. Questa comprende, altresì, le articolazioni di eventuali terze parti coinvolte nelle attività di sicurezza informatica.

Parametri quali-quantitativi

Insieme di indicatori di tipo qualitativo e quantitativo, definiti dal soggetto al fine di rilevare accessi non autorizzati o con abuso dei privilegi concessi sui propri sistemi informativi e di rete. Un esempio di indicatore di tipo quantitativo è il superamento di una soglia per le interrogazioni di una banca dati da parte di un singolo utente, un esempio di indicatore di tipo qualitativo è l'accesso di un amministratore di sistema al di fuori dell'orario di servizio.

Politiche di sicurezza informatica

Insieme di principi e regole stabiliti da un'organizzazione per garantire la protezione dei sistemi informativi, dei dati e delle comunicazioni digitali da ogni forma di minaccia o uso improprio. Rappresentano l'impegno formale dell'organizzazione alla gestione del rischio e al miglioramento continuo della sicurezza, in conformità con le normative vigenti e gli standard internazionali, guidano le decisioni e sono attuate tramite processi e procedure.

Punto di contatto

Persona fisica designata dal soggetto NIS ai sensi dell'articolo 7, comma 1, lettera c), del decreto NIS.

Sicurezza dei sistemi informativi e di rete

Capacità dei sistemi informativi e di rete di resistere, con un determinato livello di affidabilità, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi.

Sistemi di comunicazione di emergenza protetti

Sistemi per comunicare in modo sicuro in casi di emergenza (e.g. attacchi informatici o disastri) ove i sistemi di comunicazione primari dovessero risultare non disponibili.

Sistema informativo e di rete

1. Una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera vv), del decreto legislativo 1° agosto 2003, n. 259;

2. Qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;

3. I dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione.

Sistemi informativi e di rete rilevanti

Sistemi informativi e di rete la cui compromissione comporterebbe un impatto significativo sulla riservatezza, integrità e disponibilità delle attività e dei servizi per i quali il soggetto NIS rientra nell'ambito di applicazione del decreto NIS.

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.

Sostituto del punto di contatto

La persona fisica designata dal soggetto NIS ai sensi dell'articolo 7, comma 4, lettera d), del decreto NIS.