ODA.8 Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti all'articolo 23, commi 1 e 2 del decreto NIS possono delegare al proprio interno lo svolgimento delle attività finalizzate all'assolvimento degli obblighi di cui all'articolo 23, commi 1 e 2 del decreto NIS?

Si, è possibile conferire tale delega fermo restando in capo agli organi di amministrazione e agli organi direttivi dei soggetti essenziali e dei soggetti importanti la responsabilità ai sensi dell'articolo 23 del decreto NIS di (i) approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica di cui alla Determinazione ACN 379907/2025 (comma 1, lett. a)); (ii) sovrintendere alla loro implementazione (comma 1, lett. b)); (iii) essere responsabili delle violazioni di cui al decreto NIS (comma 1, lett. c)); (iv) seguire una formazione in materia di sicurezza informatica (comma 2, lett. a)); (v) promuovere l'offerta periodica di formazione per i dipendenti coerente con quella seguita dagli organi di amministrazione e dagli organi direttivi (comma 2, lett. b)).

Tale delega non può riguardare l'approvazione dei documenti di cui all'articolo 23, comma 1, lett. a), e 2 del decreto NIS, riportati sotto forma tabellare nell'appendice C della guida alla lettura delle specifiche di base (vds. ODA.10) che resta in capo unicamente ed esclusivamente agli organi di amministrazione e direttivi del soggetto NIS (sulla cui individuazione si vedano le ODA.1, ODA.3, ODA.5 e ODA.6), nella loro collegialità, ovvero all'organo monocratico, ove applicabile. Inoltre, tale obbligo non è suscettibile di essere trasferito né a membri specifici, né a distinti organi e funzioni del soggetto NIS, indipendentemente dal modello di *governance* societaria adottato.

ODA.9 L'eventuale delega per lo svolgimento di attività finalizzate all'assolvimento degli obblighi di cui all'articolo 23, commi 1 e 2 del decreto NIS, può escludere la responsabilità degli organi di amministrazione e degli organi direttivi ai sensi del predetto articolo?

Come illustrato nella ODA.8 la responsabilità ex articolo 23 del decreto NIS discende per legge in capo agli organi di amministrazione e direttivi, in caso di inadempimento dei seguenti obblighi:

1. approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24 del predetto decreto NIS;

2. sovrintendere all'implementazione degli obblighi di cui al capo IV e di cui all'articolo 7 del citato decreto NIS;
3. seguire una formazione in materia di sicurezza informatica;
4. promuovere l'offerta periodica di una formazione coerente a quella di cui al punto precedente ai loro dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti.

Si tratta di obblighi di indirizzo e pianificazione strategica che, in quanto tali, non sono delegabili.

È invece possibile la delega per lo svolgimento delle attività finalizzate all'attuazione dei predetti obblighi di cui all'articolo 23, commi 1 e 2 del decreto NIS.

In tal caso, ai fini delle responsabilità, per le società, resta fermo quanto previsto dagli artt. 2381 c.c. e 2392 c.c.

Per mera completezza, si precisa che tale rinvio non implica né consente di trasferire in capo a singoli membri degli organi di amministrazione e direttivi, né ad altri organi e funzioni del soggetto NIS, l'adempimento degli obblighi di cui all'articolo 23, commi 1 e 2 del decreto NIS.

Difatti, l'introduzione di tali obblighi ha la finalità specifica di elevare la sicurezza informatica a priorità strategica degli organi di amministrazione e direttivi.

ODA.10 Qual è il livello di dettaglio richiesto nei documenti che devono essere approvati dagli organi di amministrazione e direttivi ai fini dell'implementazione delle cd. misure di sicurezza di base?

I documenti da sottoporre all'approvazione degli organi di amministrazione e direttivi di cui all'articolo 23, comma 1, lett. a) del decreto NIS sono indicati nell'elenco a seguire che riporta tra parentesi il riferimento ai requisiti delle misure di sicurezza che ne impongono l'approvazione:

- Organizzazione per la sicurezza informatica (GV.RR-02 punto 1).
- Politiche di sicurezza informatica (GV.PO-01 punto 3).
- 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 4).
- Piano di ripristino in caso di disastro (ID.IM-04 punto 4).
- Piano di gestione delle crisi (ID.IM-04 punto 4).
- Piano di formazione (PR.AT-01 punto 2).
- Piano per la gestione degli incidenti di sicurezza informatica (RS.MA-01 punto 2).

L'elenco dei documenti e dei relativi riferimenti è anche riportato sotto forma tabellare nell'appendice C della guida alla lettura delle specifiche di base.

Essi devono avere un contenuto minimo coerente con le funzioni tipiche di gestione, indirizzo e pianificazione strategica proprie degli stessi.

Pertanto, è richiesto che tali documenti riflettano e declinino i requisiti delle misure di sicurezza almeno a livello di indirizzo e pianificazione strategica, in modo da consentire agli organi di amministrazione e direttivi di esercitare consapevolmente la propria funzione (v. anche ODA.8 e ODA.9).

Conseguentemente, il dettaglio tecnico e operativo dei succitati documenti può essere disciplinato attraverso ulteriori e diversi presidi documentali e organizzativi (e.g., procedure tecniche, istruzioni operative, manuali, documenti e relazioni interne) a cura delle articolazioni competenti del soggetto NIS.

ODA.11 È necessario che gli organi di amministrazione e direttivi approvino anche gli ulteriori e diversi presidi documentali e organizzativi eventualmente referenziati nei documenti di cui alla FAQ ODA.10?

Non è richiesto che gli organi di amministrazione e direttivi approvino gli ulteriori e diversi presidi documentali e organizzativi eventualmente referenziati nei documenti di cui alla FAQ ODA.10.

Con riferimento all'organizzazione dell'impianto documentale, si osserva infatti che – come riportato nella guida alla lettura delle specifiche di base – il soggetto può decidere come organizzare la documentazione richiesta raggruppando i contenuti in un unico documento o distribuendoli tra più documenti.

In considerazione di quanto sopra, nel caso, ad esempio, del piano per la gestione degli incidenti di sicurezza informatica, non è richiesto che tale documento contenga il dettaglio delle pertinenti procedure, ma è sufficiente che ne riporti l'elenco con i riferimenti ai relativi documenti.

ODA.12 Qualora sia aggiornato uno degli ulteriori e diversi presidi documentali e organizzativi referenziati nei documenti approvati dagli organi di amministrazione e direttivi è necessario sottoporre nuovamente all'approvazione degli organi di amministrazione e direttivi tali documenti?

Fermo restando quanto previsto dalla FAQ ODA.10, non è richiesto che gli organi di amministrazione e direttivi procedano ad una nuova approvazione dei documenti di cui alla sopracitata FAQ, qualora siano aggiornati gli ulteriori e diversi presidi documentali e organizzativi cui fanno eventualmente riferimento gli stessi documenti.

ODA.13 Nell'elencazione dei componenti degli organi di amministrazione e direttivi è necessario indicare la PEC personale?

Non è richiesta, per quanto auspicabile, l'indicazione dell'indirizzo PEC individuale e/o nominativo dei componenti degli organi di amministrazione e direttivi che vengono elencati. È anche sufficiente indicare un indirizzo PEC funzionale dell'organizzazione (come il domicilio digitale) o, qualora non disponibile, un indirizzo PEO aziendale.