Obblighi di base

Misure di sicurezza e tassonomia incidenti.

28.01.2025

Obblighi in materia di gestione dei rischi e notifica incidenti

Art. 24

Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica

1. I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali 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. Tali misure:

a) assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia e, ove applicabile, delle pertinenti norme nazionali, europee e internazionali, nonché dei costi di attuazione;

b) sono proporzionate al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico.

Art. 25

Obblighi in materia di notifica di incidente

1. I soggetti essenziali e i soggetti importanti notificano, senza ingiustificato ritardo, al CSIRT Italia ogni incidente che, ai sensi del comma 4, ha un impatto significativo sulla fornitura dei loro servizi, secondo le modalità e i termini di cui agli articoli 30, 31 e 32.

Art. 31

Proporzionalità e gradualità degli obblighi

1. 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.

Art. 40

Attuazione

5. Con una o più determinazioni dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS:

l) sono stabiliti obblighi proporzionati e graduali, a valenza multisettoriale e, ove opportuno, settoriale, di cui all'articolo 31, le modalità di applicazione dei medesimi obblighi per i soggetti che svolgono attività in più settori o sottosettori e per i soggetti di cui all'articolo 32, commi 1 e 2;

Art. 42

Fase di prima applicazione

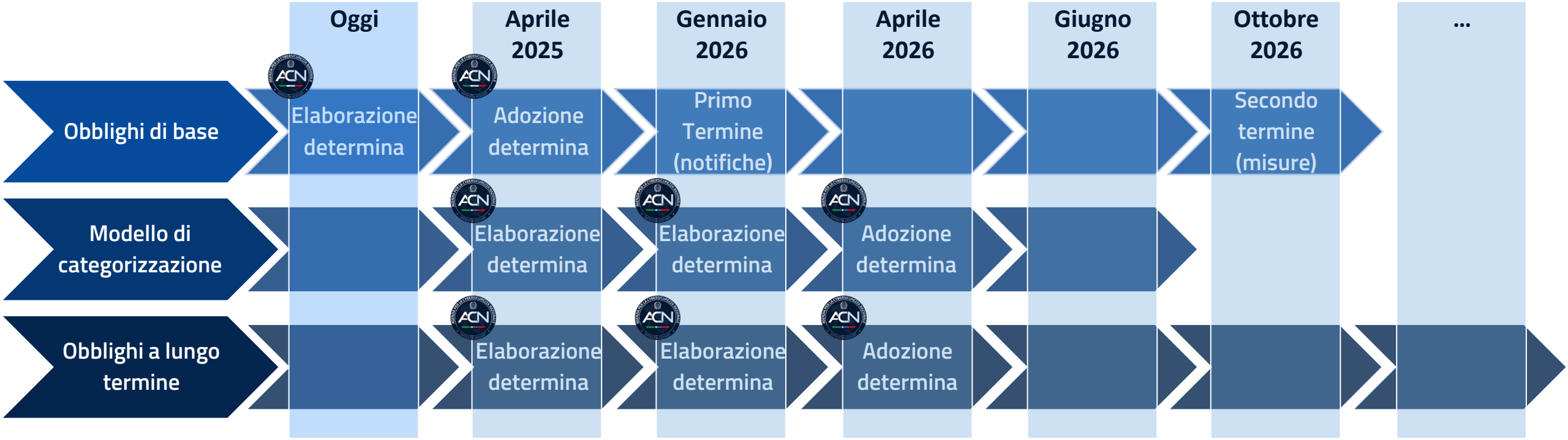
1. In fase di prima applicazione:

a) ai sensi dell'articolo 7, entro il 17 gennaio 2025, i fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network che rientrano nell'ambito di applicazione del presente decreto, si registrano sulla piattaforma digitale di cui all'articolo 7, comma 1;

b) sino al 31 dicembre 2025, il Tavolo per l'attuazione della disciplina NIS di cui all'articolo 12 si riunisce almeno una volta ogni sessanta giorni;

c) sino al 31 dicembre 2025, il termine per l'adempimento degli obblighi di cui all'articolo 25 è fissato in nove mesi dalla ricezione della comunicazione di cui all'articolo 7, comma 3, lettere a) e b), e il termine per l'adempimento degli obblighi di cui agli articoli 23, 24 e 29 è fissato in diciotto mesi dalla medesima comunicazione. Ai fini di cui al primo periodo, l'Autorità nazionale competente NIS può stabilire modalità e specifiche di base per assicurare la conformità dei soggetti essenziali e dei soggetti importanti.

Gradualità degli obblighi



Misure di sicurezza

Ambiti di applicazione delle misure di sicurezza

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

Misure di sicurezza

41 misure di sicurezza

- 31 per entrambi i soggetti.
- 10 per i soli soggetti essenziali.

Struttura misura: codice + descrizione + requisiti

- Il codice identificativo e la descrizione della misura fanno riferimento al FNSC.
- I requisiti indicano ciò che è richiesto ai fini dell'implementazione.

120 requisiti

- 72 per entrambi i soggetti.
- 48 per i soli soggetti essenziali.

Struttura misure di sicurezza

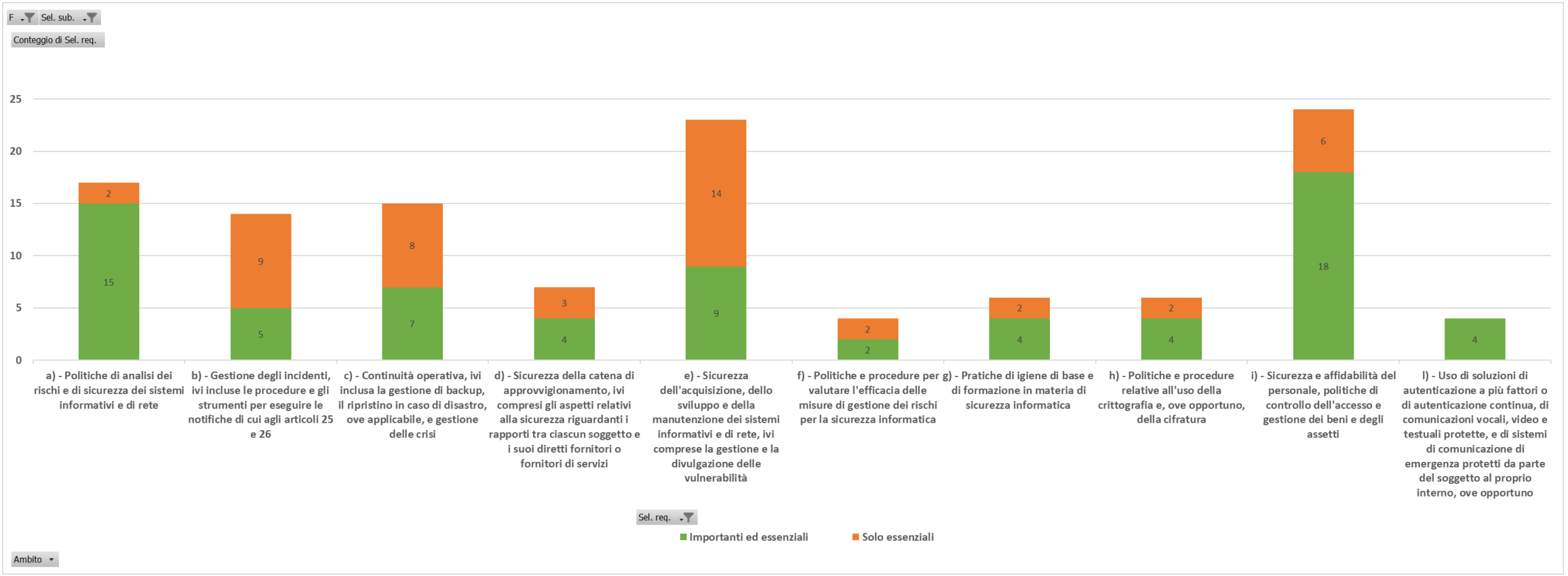
ID.RA-05 ← Codice identificativo

Minacce, vulnerabilità, probabilità e impatti sono utilizzati per comprendere il rischio inerente e per informare la prioritizzazione della risposta al rischio. ← Descrizione misura

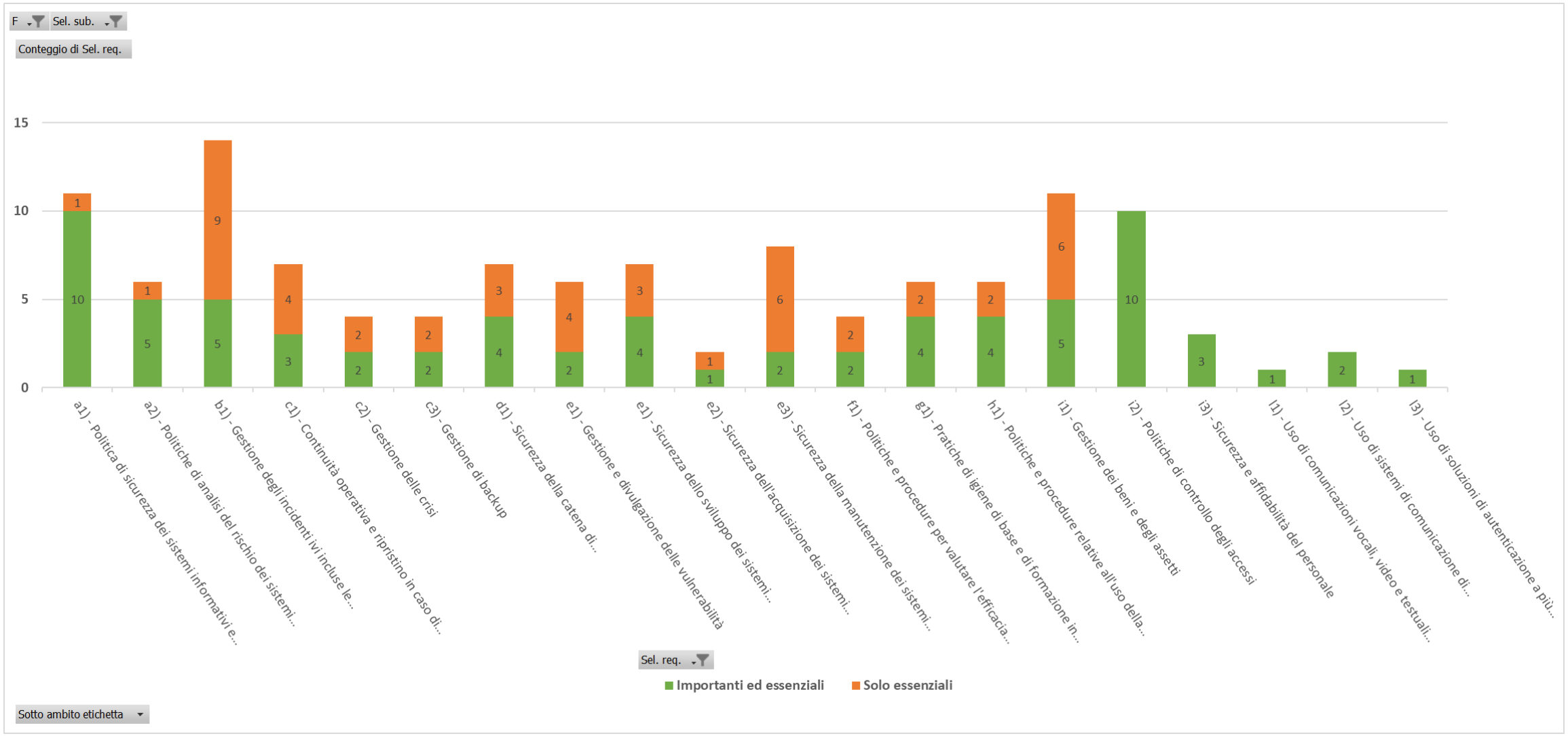
PUNTO	REQUISITO	S_I	S_E
1	In accordo al processo di gestione del rischio di cybersecurity di cui alla misura GV.RM-03, è eseguita e documentata la valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete, comprendendo almeno: a) l'identificazione del rischio; b) l'analisi del rischio; c) la ponderazione del rischio.	●	●
2	La valutazione del rischio di cui al punto 1 è eseguita a intervalli pianificati e almeno con cadenza annuale, nonché qualora si verifichino incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi.	●	●
3	La valutazione del rischio di cui al punto 1 è effettuata considerando le minacce interne ed esterne, le vulnerabilità, le probabilità di accadimento e i conseguenti impatti, nonché le eventuali dipendenze da fornitori e partner terzi.		●

Specifiche requisiti

Mappatura requisiti ambiti NIS



Mappatura requisiti sotto ambiti NIS



Approccio basato sul rischio (1/2)

Le misure di sicurezza si applicano a tutti i sistemi informativi e di rete.

Ogni sistema informativo e di rete è caratterizzato da un proprio livello di rischio.

Le misure sono definite secondo un approccio basato sul rischio.

I requisiti sono graduati e adattati sulla base dei rischi effettivi.

Usata la dicitura "*…. in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, è …*".

Le modalità di attuazione del requisito, possono essere adattate al contesto risultante dalla valutazione del rischio.

Approccio basato sul rischio (2/2)

PR.AA-03

Utenti, servizi e hardware sono autenticati

PUNTO	REQUISITO	S_I	S_E
1	Le modalità di autenticazione sono commisurate al rischio connesso ai privilegi delle utenze, alla criticità dei sistemi informativi e di rete a cui accedono e alla tipologia di operazioni che possono effettuare sugli stessi.	●	●
2	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 che attuano i punti 1 e 2.	●	●

Specifiche requisiti

Amministrative

- Adozione e approvazione di politiche e procedure
- Definizione di processi
- Redazione di documentazione
- …

Tecniche

- Cifratura dei dati
- Aggiornamento del software
- Modalità di autenticazione multifattore
- …

Evidenze documentali (1/2)

Piani

- Business continuity e disaster recovery
- Trattamento del rischio
- Gestione delle vulnerabilità
- Riesame periodico della conformità
- Monitoraggio e la misura efficacia misure gestione del rischio
- Formazione in materia di sicurezza informatica
- Risposta agli incidenti

Inventari

- Apparati fisici
- Servizi, sistemi e applicazioni software
- Flussi di dati
- Servizi erogati dai fornitori
- Fornitori e partner terzi

Evidenze documentali (2/2)

Elenchi

- Personale dell'organizzazione di cybersecurity
- Configurazioni di riferimento
- Sistemi dai quali è possibile accedere da remoto

Politiche

- Ambiti minimi indicati dalla misura GV.PO-01
- Per almeno i punti riportati in Appendice A

Registri

- Esiti del riesame delle politiche
- Audit fornitori
- Formazione ricevuta dai dipendenti
- Manutenzioni effettuate

Procedure

- Attuazione di specifici requisiti indicati nelle misure

Tassonomia incidenti

Tassonomia incidenti

IS-1 Il soggetto ha evidenza dell'accesso non autorizzato o abusivo ai dati digitali di proprietà del soggetto NIS o sui quali esercita il controllo, anche parziale.

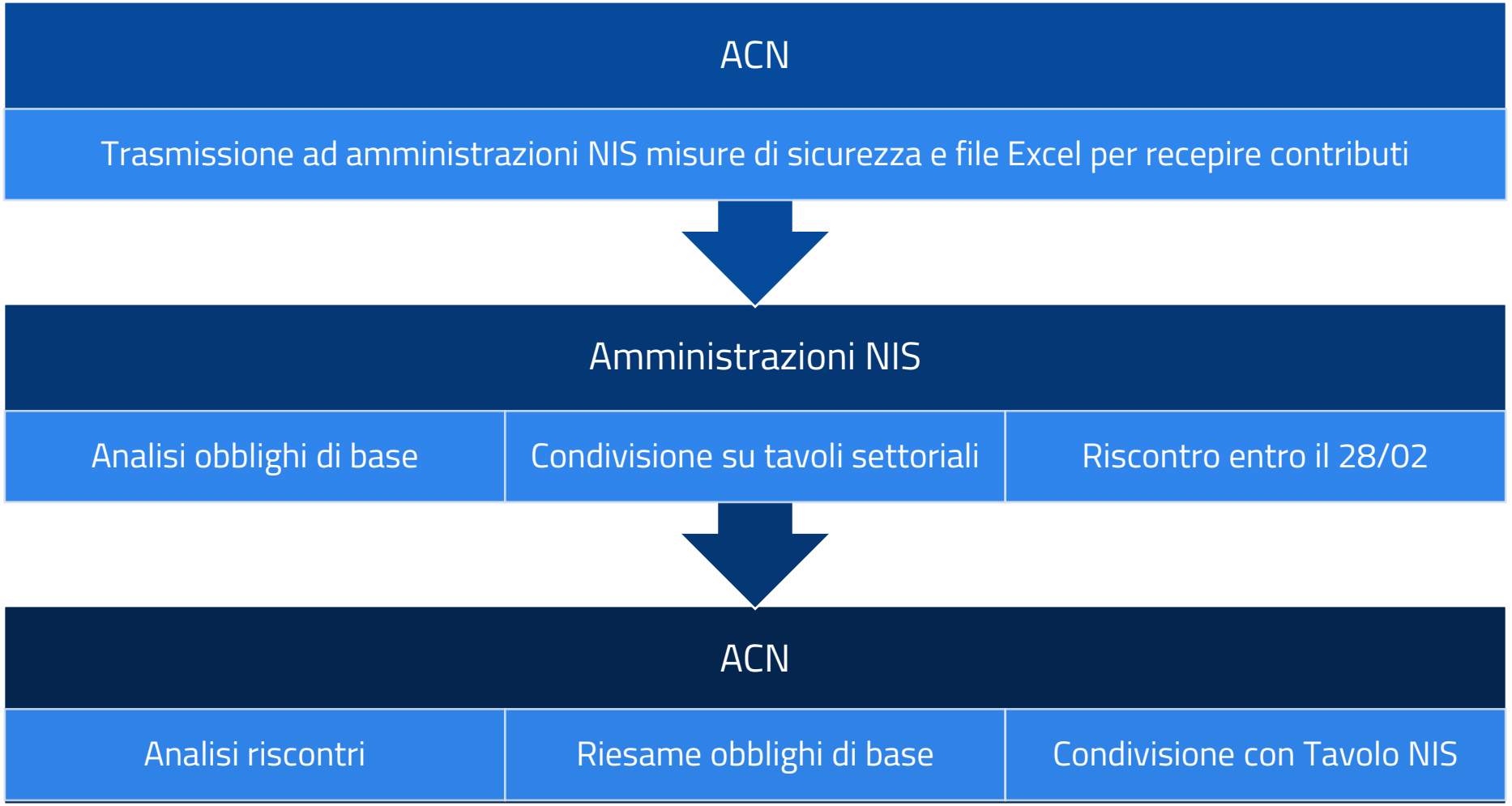
IS-2 Il soggetto ha evidenza della divulgazione non autorizzata o abusiva, all'esterno del soggetto NIS, di dati digitali di proprietà del soggetto NIS o sui quali esercita il controllo, anche parziale.

IS-3 Il soggetto ha evidenza della divulgazione, all'esterno del soggetto NIS, di dati corrotti di proprietà del soggetto NIS o sui quali ne esercita il controllo, anche parziale.

IS-4 Il soggetto ha evidenza della violazione del livello di servizio atteso dei servizi e/o delle attività del soggetto NIS, sulla base dei livelli di servizio atteso stabiliti dal soggetto NIS stesso.

Prossimi passi

Fasi del processo



File Excel di riscontro

Commenti generali

- Osservazioni di carattere generale

Commenti specifici

- Commenti su tabella tassonomie ed elenco requisiti.

Proposte

- Eventuali proposte nuovi requisiti o tipologie di incidenti.

Grazie per l'attenzione