Per essere compliant alla normativa NIS 2, un'impresa importante deve adottare le misure di sicurezza tecnico-organizzative di base specificate nell'Allegato 1 della Determinazione ACN n. 164179 del 2025. Queste misure sono organizzate in funzioni, categorie, sottocategorie e requisiti, e sono state sviluppate in accordo al Framework Nazionale per la Cybersecurity e la Data Protection (FNCS) edizione 2025.

Le aree principali coperte da queste misure includono:

1. **Governo (GOVERN)**:
   - **Contesto organizzativo (GV.OC)**: Comprendere e comunicare gli obiettivi, le capacità e i servizi critici. È richiesto un elenco aggiornato dei sistemi informativi e di rete rilevanti. [[RELATED_CODES: ["GV.OC-04"]]]
   - **Strategia di gestione del rischio (GV.RM)**: Integrare la gestione del rischio di cybersecurity nei processi organizzativi, definendo, attuando e documentando un piano di gestione dei rischi. [[RELATED_CODES: ["GV.RM-03"]]]
   - **Ruoli, responsabilità e correlati poteri (GV.RR)**: Stabilire, comunicare e applicare ruoli e responsabilità per la gestione del rischio di cybersecurity, inclusa l'organizzazione per la sicurezza informatica, il punto di contatto e il suo sostituto. La cybersecurity deve essere inclusa nelle pratiche delle risorse umane, con valutazione di esperienza, capacità e affidabilità per il personale autorizzato e gli amministratori di sistema. [[RELATED_CODES: ["GV.RR-02", "GV.RR-04"]]]
   - **Politica (GV.PO)**: Stabilire, comunicare e applicare politiche di sicurezza informatica per la gestione del rischio, che devono essere revisionate e aggiornate periodicamente (almeno annualmente) o in caso di eventi significativi. [[RELATED_CODES: ["GV.PO-01", "GV.PO-02"]]]
   - **Gestione rischio catena approvvigionamento (GV.SC)**: Stabilire strategie, obiettivi, politiche e processi per la gestione del rischio della catena di approvvigionamento. Questo include il coinvolgimento dell'organizzazione di sicurezza, la definizione di requisiti di sicurezza nei contratti per forniture critiche, la gestione dei ruoli delle terze parti e il mantenimento di un inventario aggiornato dei fornitori. I rischi associati alle forniture devono essere valutati e documentati. [[RELATED_CODES: ["GV.SC-01", "GV.SC-02", "GV.SC-04", "GV.SC-05", "GV.SC-07"]]]
2. **Identificazione (IDENTIFY)**:
   - **Gestione degli asset (ID.AM)**: Mantenere inventari aggiornati di hardware, software, servizi e sistemi gestiti dall'organizzazione, inclusi quelli erogati dai fornitori. [[RELATED_CODES: ["ID.AM-01", "ID.AM-02", "ID.AM-04"]]]
   - **Valutazione del rischio (ID.RA)**: Identificare, confermare e registrare le vulnerabilità negli asset, eseguendo e documentando valutazioni del rischio a intervalli pianificati (almeno ogni due anni o

in caso di eventi significativi). Definire e monitorare un piano di trattamento del rischio e stabilire processi per la ricezione, l'analisi e la risposta alle divulgazioni di vulnerabilità. [[RELATED_CODES: ["ID.RA-01", "ID.RA-05", "ID.RA-06", "ID.RA-08"]]]
    - **Miglioramento (ID.IM)**: Identificare miglioramenti in esito alle valutazioni, definendo e attuando un piano di adeguamento. Stabilire, comunicare, mantenere e migliorare i piani di risposta agli incidenti, continuità operativa, ripristino in caso di disastro e gestione delle crisi per i sistemi rilevanti. [[RELATED_CODES: ["ID.IM-01", "ID.IM-04"]]]
3. **Protezione (PROTECT)**:
    - **Gestione identità e accessi (PR.AA)**: Gestire identità, credenziali e permessi degli utenti, dei servizi e dell'hardware, applicando i principi del minimo privilegio e della separazione dei compiti. Proteggere l'accesso fisico agli asset. [[RELATED_CODES: ["PR.AA-01", "PR.AA-03", "PR.AA-05", "PR.AA-06"]]]
    - **Consapevolezza e formazione (PR.AT)**: Sensibilizzare e formare il personale sui rischi di cybersecurity, inclusi gli organi direttivi, e mantenere un registro dei dipendenti formati. [[RELATED_CODES: ["PR.AT-01"]]]
    - **Sicurezza dei dati (PR.DS)**: Proteggere la riservatezza, l'integrità e la disponibilità dei dati a riposo e in transito (es. cifratura per dispositivi portatili e trasmissioni esterne). Effettuare backup periodici e conservare copie offline per i sistemi rilevanti. [[RELATED_CODES: ["PR.DS-01", "PR.DS-02", "PR.DS-11"]]]
    - **Sicurezza delle piattaforme (PR.PS)**: Gestire il software (installazione, aggiornamenti di sicurezza) e generare log per il monitoraggio continuo. Adottare pratiche di sviluppo sicuro del software. [[RELATED_CODES: ["PR.PS-02", "PR.PS-04", "PR.PS-06"]]]
    - **Resilienza infrastruttura (PR.IR)**: Proteggere le reti e gli ambienti dall'accesso non autorizzato, definendo attività remote consentite e configurando sistemi perimetrali come i firewall. [[RELATED_CODES: ["PR.IR-01"]]]
4. **Rilevamento (DETECT)**:
    - **Monitoraggio continuo (DE.CM)**: Monitorare reti, servizi, hardware e software per individuare eventi avversi, con strumenti tecnici adeguati e definizione di livelli di servizio attesi (SL). [[RELATED_CODES: ["DE.CM-01", "DE.CM-09"]]]
5. **Risposta (RESPOND)**:
    - **Gestione incidenti (RS.MA)**: Definire, attuare e aggiornare un piano per la gestione degli incidenti di sicurezza informatica e la notifica al CSIRT Italia, che deve essere approvato dagli organi direttivi e riesaminato periodicamente. [[RELATED_CODES: ["RS.MA-01"]]]
    - **Segnalazione (RS.CO)**: Documentare procedure per comunicare gli incidenti agli stakeholder interni ed esterni, inclusi i destinatari dei servizi e il pubblico, se richiesto dall'Agenzia. [[RELATED_CODES:

[“RS.CO-02”]]]

6. **Ripristino (RECOVER)**:
    - **Esecuzione piano ripristino (RC.RP)**: Adottare procedure per il ripristino del normale funzionamento dei sistemi dopo incidenti. [[RELATED_CODES: [“RC.RP-01”]]]

Queste misure sono dettagliate nell’Allegato 1 della “DetACN_nis_specifiche_2025_164179_allegato1-Misure minime aziende IMPORTANTI.pdf” e sono riassunte nella Tabella 1 in appendice a tale allegato.

Registrazione al Portale ACN

Per quanto riguarda la registrazione al Portale ACN, un’impresa importante deve seguire le modalità definite nella “DetACN_2025-333017.pdf”.

1. **Designazione del Punto di Contatto e Sostituto**:
    - Il soggetto NIS deve designare una persona fisica come “punto di contatto” con il compito di curare l’attuazione delle disposizioni del decreto NIS e di interloquire con l’Autorità nazionale competente NIS. Questa persona accede al Portale ACN e ai Servizi NIS ed effettua la registrazione per conto del soggetto (Articolo 4, comma 1, “DetACN_2025-333017.pdf”).
    - Le funzioni di punto di contatto possono essere svolte dal rappresentante legale, da uno dei procuratori generali o da un dipendente delegato del soggetto NIS (Articolo 4, comma 2, “DetACN_2025-333017.pdf”).
    - Deve essere designato anche un “sostituto punto di contatto”, una persona fisica distinta dal punto di contatto, con le medesime modalità. Il sostituto supporta il punto di contatto e può interloquire con l’Autorità nazionale competente NIS ed effettuare azioni sulla piattaforma digitale, ad eccezione della registrazione (Articolo 5, commi 1 e 2, “DetACN_2025-333017.pdf”).
    - Il sostituto punto di contatto deve essere designato entro il 31 maggio dell’anno in cui il soggetto NIS ha ricevuto comunicazione di inserimento nell’elenco dei soggetti NIS (Articolo 5, comma 3, “DetACN_2025-333017.pdf”).
    - In caso di avvicendamento del punto di contatto, gli organi di amministrazione e direttivi devono provvedere senza ingiustificato ritardo alla designazione del nuovo punto di contatto e assicurare il suo censimento sul Portale ACN (Articolo 4, comma 7, “DetACN_2025-333017.pdf”).
2. **Censimento degli utenti e Associazione al Soggetto NIS**:
    - Gli utenti (inclusi i componenti degli organi di amministrazione e direttivi, il punto di contatto, il sostituto punto di contatto, la segreteria, il referente CSIRT e gli operatori) si autenticano sul Portale ACN tramite CIE o SPID personale (Articolo 8, comma 1, “DetACN_2025-333017.pdf”).
    - Gli utenti devono completare la propria anagrafica fornendo le infor-

mazioni richieste (nome, cognome, codice fiscale, ecc.) (Articolo 8, comma 2, "DetACN_2025-333017.pdf").
    - Il punto di contatto, una volta censito, effettua l'associazione della sua utenza con il soggetto NIS che lo ha designato, tramite il codice fiscale del soggetto o il codice IPA (Articolo 9, comma 1, "DetACN_2025-333017.pdf").
    - L'associazione dell'utenza del punto di contatto è sottoposta a convalida da parte del soggetto NIS (Articolo 9, comma 4, "DetACN_2025-333017.pdf"). Il sostituto punto di contatto effettua l'associazione con le medesime modalità su invito del punto di contatto (Articolo 9, comma 7, "DetACN_2025-333017.pdf").
3. **Registrazione Annuale**:
    - 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 (Articolo 11, comma 1, "DetACN_2025-333017.pdf").
    - La dichiarazione include informazioni sulla natura del soggetto (impresa autonoma o parte di un gruppo), codici ATECO, normative settoriali, valori di fatturato, bilancio e numero di dipendenti (Articolo 11, comma 2, "DetACN_2025-333017.pdf").
    - Al termine della compilazione, l'utente conferma la valutazione preliminare e trasmette le informazioni telematicamente all'Autorità nazionale competente NIS (Articolo 11, commi 6 e 7, "DetACN_2025-333017.pdf").
4. **Aggiornamento Annuale e Continuo delle Informazioni**:
    - Dal 15 aprile al 31 maggio di ogni anno, gli utenti aggiornano, tramite il Servizio NIS/Aggiornamento annuale, le informazioni per conto del soggetto (Articolo 16, comma 1, "DetACN_2025-333017.pdf").
    - L'aggiornamento include i dati anagrafici e di contatto del soggetto NIS, l'elenco dei componenti degli organi di amministrazione e direttivi, l'elenco dei servizi NIS, lo spazio di indirizzamento IP pubblico e i nomi di dominio in uso, e gli accordi di condivisione delle informazioni (Articolo 16, comma 3, "DetACN_2025-333017.pdf").
    - In caso di modifiche alle informazioni trasmesse, i soggetti NIS devono comunicarle tempestivamente, e comunque entro quattordici giorni dalla data della modifica, tramite il Servizio NIS/Aggiornamento continuo (Articolo 18, comma 1, "DetACN_2025-333017.pdf").

Gli organi di amministrazione e direttivi dei soggetti NIS sovrintendono alla registrazione, comunicazione o aggiornamento delle informazioni e sono responsabili delle eventuali violazioni (Articolo 2, comma 3, "DetACN_2025-333017.pdf"). La mancata registrazione, comunicazione o aggiornamento è punita ai sensi dell'articolo 38 del decreto NIS (Articolo 2, comma 4, "DetACN_2025-333017.pdf").