NIS 2 - Analisi dei rischi cyber

identificazione sistemi rilevanti a rischio, identificazione asset e minacce, identificazione vulnerabilità, analisi probabilità e impatto (matrice di rischio), definizione opzioni di trattamento (remediation plan), Monitoraggio e Revisione

Per un'organizzazione "importante" ai sensi della normativa NIS 2, l'identificazione delle attività e dei servizi NIS-rilevanti e la valutazione del rischio sono passaggi cruciali. I documenti ufficiali indicano che non è richiesta una metodologia specifica per la valutazione dell'impatto, permettendo all'organizzazione di utilizzare quella più adatta al proprio contesto (Linee Guida per 164179-2025.pdf, pagina 11, sezione 2.3.1).

Propongo una metodologia di **Valutazione Qualitativa del Rischio basata su Matrice**, che è strutturata, efficace per la prioritizzazione e relativamente semplice da implementare.

1. Identificazione delle attività e dei servizi NIS-rilevanti

Per identificare le attività e i servizi che rientrano nell'ambito di applicazione del Decreto NIS (D.Lgs. 138/2024), la tua organizzazione deve:

1. **Consultare il Decreto NIS (D.Lgs. 138/2024):** Esaminare l'**articolo 3** e gli **Allegati I e II** del Decreto NIS. Questi documenti definiscono i settori e le tipologie di entità (es. fornitori di servizi digitali, enti della pubblica amministrazione, operatori di infrastrutture critiche) che sono considerati "essenziali" o "importanti" in base a criteri specifici (es. dimensione, fatturato, numero di dipendenti, impatto potenziale di un incidente).
2. **Verificare i propri codici ATECO e normative settoriali:** La "Determina ACN n. 333017 del 2025" (Articolo 11, punto 2, lettere d) ed e)) richiede ai soggetti di indicare i propri codici ATECO e le normative settoriali dell'Unione europea pertinenti. Questo aiuta a confermare l'appartenenza a un settore NIS.
3. **Considerare la comunicazione ACN:** Se la tua organizzazione ha ricevuto una comunicazione dall'ACN di inserimento nell'elenco dei soggetti NIS, è già stata formalmente identificata come tale (Linee Guida per 164179-2025.pdf, pagina 6, sezione 1.3).

Una volta identificata come soggetto NIS "importante", l'organizzazione deve procedere con la valutazione del rischio.

2. Metodologia di Valutazione Qualitativa del Rischio (per organizzazioni "importanti")

Questa metodologia si articola in fasi che permettono di comprendere il rischio inerente e di informare la prioritizzazione della risposta al rischio, come richiesto dalla misura **ID.RA-05**.

Fase 1: Preparazione e Definizione dello Scopo

1. **Definizione del Contesto (GV.OC-04):**
   - Comprendere gli obiettivi, le capacità e i servizi critici dell'organizzazione da cui dipendono gli stakeholder.
   - **Scopo:** La valutazione del rischio si concentrerà sui **sistemi informativi e di rete rilevanti**, ovvero quelli la cui compromissione

comporterebbe un impatto significativo sulla riservatezza, integrità e disponibilità delle attività e dei servizi NIS dell'organizzazione (Linee Guida per 164179-2025.pdf, pagina 11, sezione 2.3.1).
- **Output:** Un elenco aggiornato dei sistemi informativi e di rete rilevanti. [[RELATED_CODES: ["GV.OC-04"]]]

2. **Stabilire il Piano di Gestione dei Rischi (GV.RM-03):**
   - Definire, attuare, aggiornare e documentare un piano di gestione dei rischi per la sicurezza informatica. Questo piano deve essere parte integrante dei processi di gestione del rischio dell'organizzazione e rispettare le politiche di sicurezza (GV.PO-01).
   - **Output:** Piano di gestione dei rischi documentato. [[RELATED_CODES: ["GV.RM-03", "GV.PO-01"]]]

Fase 2: Identificazione e Analisi del Rischio (ID.RA-05)

1. **Identificazione degli Asset (ID.AM-01, ID.AM-02, ID.AM-04):**
   - Creare e mantenere inventari aggiornati di tutti gli asset che compongono i sistemi informativi e di rete rilevanti:
     - **Hardware:** Apparati fisici (server, dispositivi di rete, endpoint, ecc.).
     - **Software:** Servizi, sistemi e applicazioni software (commerciali, open-source, custom).
     - **Servizi Esterni:** Servizi informatici erogati da fornitori, inclusi i servizi cloud.
   - **Output:** Inventari aggiornati degli asset. [[RELATED_CODES: ["ID.AM-01", "ID.AM-02", "ID.AM-04"]]]
2. **Identificazione delle Minacce (ID.RA-05):**
   - Per ciascun asset rilevante, identificare le potenziali minacce (es. attacchi malware, phishing, denial of service, errori umani, disastri naturali).
   - **Input:** Monitorare i canali del CSIRT Italia e altri pertinenti per informazioni sulle vulnerabilità e minacce (ID.RA-08).
   - **Output:** Elenco delle minacce rilevanti. [[RELATED_CODES: ["ID.RA-05", "ID.RA-08"]]]
3. **Identificazione delle Vulnerabilità (ID.RA-01, ID.RA-08):**
   - Per ciascun asset rilevante, identificare le debolezze (vulnerabilità) che potrebbero essere sfruttate dalle minacce (es. software non aggiornato, configurazioni deboli, mancanza di controlli).
   - **Input:** Utilizzare le informazioni sulle vulnerabilità identificate tramite il monitoraggio (ID.RA-08) per identificare eventuali vulnerabilità sui sistemi.
   - **Output:** Elenco delle vulnerabilità associate agli asset. [[RELATED_CODES: ["ID.RA-01", "ID.RA-08"]]]
4. **Valutazione dell'Impatto (ID.RA-05):**
   - Per ogni scenario di rischio (minaccia + vulnerabilità), valutare le conseguenze se l'incidente si verificasse. L'impatto deve essere classificato in termini di:

    - **Riservatezza:** Danno derivante dalla divulgazione non autorizzata di dati.
    - **Integrità:** Danno derivante dalla modifica o distruzione non autorizzata di dati.
    - **Disponibilità:** Danno derivante dall'indisponibilità di sistemi o servizi.
  - **Scala Qualitativa:** Utilizzare una scala qualitativa, ad esempio:
    - **Basso:** Impatto minimo, facilmente gestibile, senza interruzioni significative.
    - **Medio:** Impatto moderato, interruzioni gestibili, possibili danni reputazionali o finanziari limitati.
    - **Alto:** Impatto significativo, interruzioni prolungate, danni reputazionali o finanziari gravi, possibili sanzioni.
    - **Critico:** Impatto devastante, interruzione totale dei servizi critici, danni irreparabili, gravi sanzioni.
  - **Considerazioni:** Impatto operativo, finanziario, reputazionale, legale/normativo (sanzioni NIS 2).
  - **Output:** Classificazione dell'impatto per ogni scenario di rischio. [[RELATED_CODES: ["ID.RA-05"]]]
5. **Valutazione della Probabilità (ID.RA-05):**
  - Per ogni scenario di rischio, valutare la probabilità che la minaccia si concretizzi sfruttando la vulnerabilità.
  - **Scala Qualitativa:** Utilizzare una scala qualitativa, ad esempio:
    - **Molto Bassa:** Estremamente improbabile.
    - **Bassa:** Improbabile.
    - **Media:** Potrebbe verificarsi occasionalmente.
    - **Alta:** Probabile.
    - **Molto Alta:** Quasi certo.
  - **Considerazioni:** Frequenza storica di incidenti, efficacia dei controlli esistenti, attrattività dell'asset per gli attaccanti.
  - **Output:** Classificazione della probabilità per ogni scenario di rischio. [[RELATED_CODES: ["ID.RA-05"]]]
6. **Ponderazione del Rischio (Matrice di Rischio) (ID.RA-05):**
  - Combinare i valori di Impatto e Probabilità utilizzando una matrice di rischio per determinare il livello di rischio complessivo.
  - **Esempio di Matrice di Rischio (semplificata):**

Probabilità \ Impatto	Basso	Medio	Alto	Critico
Molto Alta	Medio	Alto	Alto	Critico
Alta	Basso	Medio	Alto	Critico
Media	Basso	Basso	Medio	Alto
Bassa	Basso	Basso	Basso	Medio
Molto Bassa	Basso	Basso	Basso	Basso

```
*   **Output:** Livello di rischio (es. Basso, Medio, Alto, Critico) per ogni scenario. [[RE
```

Fase 3: Trattamento del Rischio (ID.RA-06)

1. **Definizione delle Opzioni di Trattamento:**
   - Per ogni rischio, definire le opzioni di trattamento:
     - **Accettare:** Se il rischio è al di sotto della soglia di tolleranza. Richiede documentazione e approvazione.
     - **Mitigare:** Implementare controlli per ridurre impatto o probabilità.
     - **Trasferire:** Trasferire il rischio a terzi (es. assicurazione).
     - **Evitare:** Eliminare l'attività che genera il rischio.
   - **Piano di Trattamento del Rischio:** Definire, documentare, eseguire e monitorare un piano che specifichi le misure da attuare, le priorità, le responsabilità e le tempistiche. Se per ragioni motivate non si attuano certi requisiti, adottare misure compensative e descriverle nel piano.
   - **Approvazione:** Il piano di trattamento, inclusa l'accettazione dei rischi residui, deve essere approvato dagli organi di amministrazione e direttivi.
   - **Output:** Piano di trattamento del rischio approvato. [[RELATED_CODES: ["ID.RA-06"]]]

Fase 4: Monitoraggio e Revisione

1. **Monitoraggio Continuo (GV.RM-03, ID.RA-06):**
   - Monitorare l'efficacia delle misure di trattamento e l'evoluzione dei rischi.
2. **Revisione Periodica (ID.RA-05):**
   - La valutazione del rischio deve essere riesaminata e aggiornata periodicamente, **almeno ogni due anni**, o in caso di eventi significativi (es. incidenti, variazioni organizzative, mutamenti dell'esposizione alle minacce e ai relativi rischi).
   - **Output:** Rapporti di monitoraggio e revisioni periodiche. [[RELATED_CODES: ["GV.RM-03", "ID.RA-05", "ID.RA-06"]]]

Integrazione con i requisiti NIS 2 per un'organizzazione "importante":

- **Ruoli e Responsabilità (GV.RR-02):** Assicurati che l'organizzazione per la sicurezza informatica sia definita e approvata, con ruoli e responsabilità chiari per la gestione del rischio. Il punto di contatto e il suo sostituto devono essere inclusi. [[RELATED_CODES: ["GV.RR-02"]]]
- **Sicurezza nelle Risorse Umane (GV.RR-04):** Il personale autorizzato ad accedere ai sistemi rilevanti deve essere individuato previa valutazione di esperienza, capacità e affidabilità. [[RELATED_CODES: ["GV.RR-04"]]]
- **Politiche di Sicurezza (GV.PO-01):** Adottare e documentare politiche di sicurezza informatica per ambiti specifici, inclusa la gestione del rischio. Tali politiche devono essere approvate dagli organi di amministrazione e direttivi. [[RELATED_CODES: ["GV.PO-01"]]]

- **Gestione Rischio Catena Approvvigionamento (GV.SC-07):** Nell'ambito della valutazione del rischio (ID.RA-05), è fondamentale valutare e documentare il rischio associato alle forniture, considerando il livello di accesso del fornitore, l'impatto di un'interruzione e i ruoli/responsabilità del fornitore. [[RELATED_CODES: ["GV.SC-07"]]]
- **Documentazione e Approvazione:** Tutti i documenti chiave (politiche, piani di gestione e trattamento del rischio, piani di gestione delle vulnerabilità, piani di continuità operativa, ripristino e crisi, piano di formazione) devono essere approvati dagli organi di amministrazione e direttivi (Appendice C della Det. 164179).

Questa metodologia, pur essendo flessibile nella sua implementazione, garantisce che tutti gli aspetti richiesti dalla normativa NIS 2 per la valutazione e il trattamento del rischio siano coperti in modo sistematico.