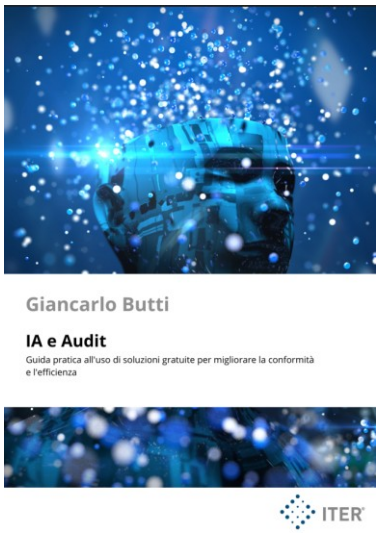
Basata sui seguenti testi



E su questa applicazione

ATTENZIONE: i testi e le applicazioni generati con sistemi di AI non possono essere usati direttamente, ma devono essere controllati da chi ha competenza specifica sull'argomento trattato prima del loro utilizzo, in quanto possono contenere errori.

Esempio di Rapporto di Valutazione NIS2 per Fornitori

Data: 13/11/2025

Punteggio totale: 59.5%

Riepilogo per Sezione

Sezione	Domande Completate	Punteggio
Governance e Gestione del Rischio nella Catena di Approvvigionamento	20/20	59.0%
Sicurezza Operativa e Protezione	20/20	65.0%
Continuità Operativa e Ripristino	20/20	59.2%
Risposta agli Incidenti e Formazione	20/20	61.0%
Conformità, Vigilanza e Requisiti Aggiuntivi	19/20	52.8%

Governance e Gestione del Rischio nella Catena di Approvvigionamento

Domanda 1: Il Soggetto NIS mantiene un inventario aggiornato dei fornitori le cui forniture hanno un potenziale impatto sulla sicurezza dei sistemi informativi e di rete (GV.SC-04.1)?

Peso: 5

Risposta: Livello 2 (45%)

Descrizione: Inventario esistente ma incompleto o non aggiornato (es. solo i fornitori Tier 1).

Domanda 2: Esiste una Politica di Sicurezza della Catena di Approvvigionamento (GV.SC-01.1 / EU Reg. 5.1.1) che disciplina i rapporti con i fornitori diretti?

Peso: 5

Risposta: Livello 2 (45%)

Descrizione: La politica esiste ma non è formalmente approvata o non copre tutti gli aspetti (es. subforniture).

Domanda 3: La valutazione del rischio del Soggetto NIS include e documenta specificamente il rischio associato alle forniture (GV.SC-07.1 / ID.RA-05.1)?

Peso: 5

Risposta: Livello 3 (65%)

Descrizione: La VA è documentata e considera i rischi di dipendenza (es. impatto di interruzione grave).

Domanda 4: Nel processo di approvvigionamento di forniture con potenziale impatto sulla sicurezza, è coinvolta l'Organizzazione per la sicurezza informatica del Soggetto NIS? (GV.SC-01.1.a)

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: L'Organizzazione di cybersecurity fornisce input e approvazione obbligatori prima della stipula del contratto.

Domanda 5: I requisiti di sicurezza per la fornitura sono definiti e sono coerenti con le misure di sicurezza applicate dal Soggetto NIS ai sistemi informativi e di rete? (GV.SC-01.1.b)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: I requisiti sono specificati ma non basati sugli esiti della valutazione del rischio.

Domanda 6: I ruoli e le responsabilità in materia di cybersecurity per il fornitore e il suo personale sono stabiliti e comunicati (GV.SC-02.1 / EU Reg. 5.1.4)?

Peso: 5

Risposta: Livello 2 (45%)

Descrizione: Ruoli definiti in modo generico; comunicati solo al referente principale.

Domanda 7: Il fornitore assicura l'affidabilità delle risorse umane che accedono ai sistemi del Soggetto NIS (es. screening del personale)? (GV.SC-01.2.a / GV.RR-04.1 / EU Reg. 10.2)

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: Screening periodico e processo disciplinare documentato per le violazioni di sicurezza.

Domanda 8: I rischi di subappalto o subfornitura sono gestiti e i requisiti di sicurezza sono estesi ai subappaltatori? (GV.SC-01.2.q / EU Reg. 5.1.4.g)

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: Il fornitore valuta il rischio posto dai subappaltatori e applica requisiti di sicurezza proporzionati al rischio.

Domanda 9: Il Soggetto NIS verifica periodicamente e documenta la conformità delle forniture ai requisiti di sicurezza contrattuali stabiliti (GV.SC-07.2)?

Peso: 5

Risposta: Livello 3 (65%)

Descrizione: La conformità è verificata periodicamente (es. annualmente) e documentata.

Domanda 10: Il fornitore identifica, valuta e gestisce i rischi legati alla propria catena di approvvigionamento? (ID.SC-1 / ID.SC-2)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: I fornitori del fornitore sono identificati ma non valutati sistematicamente.

Domanda 11: La valutazione del rischio (VA) tiene conto dell'impatto di una grave interruzione della fornitura (GV.SC-07.1.c)?

Peso: 4

Risposta: Livello 1 (25%)

Descrizione: L'impatto dell'interruzione non è mappato.

Domanda 12: I rischi residui (ad esempio, derivanti da deroghe) sono documentati e accettati dal management del fornitore? (ID.RA-06.1.c)

Peso: 4

Risposta: Livello 5 (100%)

Descrizione: L'accettazione del rischio è parte integrante del ciclo di gestione del rischio che viene riesaminato annualmente.

Domanda 13: I requisiti di sicurezza stabiliti per la fornitura sono stati inseriti nelle richieste di offerta o bandi di gara (GV.SC-05.1)?

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: Vengono considerati, nei criteri di selezione, i risultati delle valutazioni coordinate dei rischi della catena di approvvigionamento (se applicabile).

Domanda 14: Il fornitore ha definito i propri livelli di servizio attesi (SL) per i servizi erogati, anche ai fini della rilevazione tempestiva degli incidenti significativi? (DE.CM-01.2)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Gli SL sono definiti solo in termini generici di disponibilità.

Domanda 15: La documentazione del Soggetto NIS include un inventario aggiornato dei servizi informatici erogati dai fornitori, inclusi i servizi cloud? (ID.AM-04.1)

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: Inventario aggiornato che include la tipologia di servizio e, se applicabile, i servizi cloud.

Domanda 16: Il Soggetto NIS/Fornitore verifica che i contratti contengano la clausola che impone la gestione delle vulnerabilità che presentano un rischio per la sicurezza del Soggetto NIS? (EU Reg. 5.1.4.f)

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: Obbligo contrattuale che prevede scadenze specifiche per la mitigazione delle vulnerabilità critiche (es. entro 72 ore).

Domanda 17: La valutazione del rischio (VA) del fornitore tiene conto dei rischi posti dai suoi prodotti e servizi e dalle altre terze parti (GV.SC-07.1)?

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: La valutazione copre i rischi intrinseci e la qualità complessiva dei prodotti.

Domanda 18: Il fornitore dispone di procedure definite per il recupero e lo smaltimento sicuro delle informazioni del Soggetto NIS al momento della risoluzione del contratto? (EU Reg. 5.1.4.h)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Esistono procedure informali di cancellazione dei dati.

Domanda 19: I requisiti di conformità e audit di sicurezza del fornitore sono definiti, stabiliti e monitorati (GV.SC-01.2.d)?

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Obbligo di conformità legale generico.

Domanda 20: Il Soggetto NIS si riserva contrattualmente il diritto di effettuare audit o di ricevere le relazioni di audit del fornitore? (EU Reg. 5.1.4.e)

Peso: 5

Risposta: Livello 1 (25%)

Descrizione: Il diritto di audit non è previsto.

Sicurezza Operativa e Protezione

Domanda 21: Il fornitore applica il principio del minimo privilegio (least privilege) e della separazione delle funzioni per gli accessi ai sistemi del Soggetto NIS (PR.AA-05.1)?

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: Accessi definiti e limitati alle funzioni necessarie (need to know), con separazione dei compiti.

Domanda 22: Le utenze del fornitore (incluse quelle amministrative e di accesso remoto) sono individuali per gli utenti? (PR.AA-01.1)

Peso: 5

Risposta: Livello 4 (85%)

Descrizione: Le identità condivise sono consentite solo per motivi operativi, con approvazione esplicita e tracciabilità dell'uso.

Domanda 23: Per l'accesso ai sistemi e dati critici del Soggetto NIS, il fornitore utilizza l'autenticazione a più fattori (MFA)? (PR.AA-03.2 / EU Reg. 11.7.1)

Peso: 5

Risposta: Livello 5 (100%)

Descrizione: È adottata una politica di autenticazione continua, con forza MFA adeguata alla classificazione della risorsa.

Domanda 24: Il fornitore garantisce che le credenziali (password) siano robuste e aggiornate in base agli esiti della valutazione del rischio? (PR.AA-01.2)

Peso: 4

Risposta: Livello 5 (100%)

Descrizione: Vengono utilizzate soluzioni di gestione delle credenziali privilegiate (PAM) e le credenziali sono soggette a rotazione automatizzata.

Domanda 25: Il fornitore adotta misure per proteggere la riservatezza e l'integrità dei dati memorizzati e trasferiti (PR.DS-01)?

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Cifratura implementata solo per alcuni dati sensibili a riposo.

Domanda 26: Il fornitore garantisce che gli ambienti di sviluppo e test siano logicamente separati dall'ambiente di produzione utilizzato per i servizi al Soggetto NIS? (PR.DS-06 / EU Reg. 6.2.2.c)

Peso: 4

Risposta: Livello 1 (25%)

Descrizione: Nessuna separazione.

Domanda 27: Il fornitore gestisce in modo appropriato l'accesso fisico agli asset (es. server, apparecchiature di rete) rilevanti per la fornitura del servizio? (PR.AA-06.1)

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: Accesso fisico protetto per i sistemi rilevanti, con procedure documentate.

Domanda 28: Il fornitore utilizza solo software e applicazioni approvati e censiti (inventario software)? (ID.AM-02.1)

Peso: 3

Risposta: Livello 5 (100%)

Descrizione: L'inventario è integrato nel processo di gestione delle vulnerabilità e include identificatori univoci del codice oggetto (se possibile).

Domanda 29: Il fornitore adotta misure adeguate per la gestione della configurazione sicura di hardware, software e reti? (PR.PS-04 / EU Reg. 6.3.1)

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: Esistono processi di controllo delle modifiche (Change Management) formalizzati e applicati (PR.IP-3).

Domanda 30: Il fornitore esegue il patch management per gli aggiornamenti di sicurezza in modo tempestivo e coerente? (PR.PS-02 / EU Reg. 6.6.1)

Peso: 5

Risposta: Livello 2 (45%)

Descrizione: Patch applicate solo a sistemi critici con ritardo.

Domanda 31: Il fornitore ha un piano per la gestione delle vulnerabilità che include le procedure, i ruoli e le responsabilità? (ID.RA-08.3 / EU Reg. 6.10)

Peso: 4

Risposta: Livello 1 (25%)

Descrizione: Nessun piano di gestione delle vulnerabilità.

Domanda 32: Il fornitore esegue test di sicurezza periodici (es. penetration test, vulnerability assessment) sulle piattaforme critiche? (ID.RA-01.2 / DE.CM-8)

Peso: 5

Risposta: Livello 2 (45%)

Descrizione: Esecuzione di vulnerabilità assessment semplici e non sistematici.

Domanda 33: Il fornitore effettua una revisione periodica delle utenze e delle relative autorizzazioni, revocandole in caso di variazioni (es. cessazione del personale)? (PR.AA-01.3)

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: La revoca è immediata e documentata; le procedure di deposito/restituzione delle risorse sono chiare al termine del rapporto.

Domanda 34: Le comunicazioni vocali, video e testuali (interne ed esterne) sono effettuate utilizzando protocolli e algoritmi di cifratura allo stato dell'arte? (PR.DS-01.1)

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: Utilizzo di protocolli e algoritmi di cifratura allo stato dell'arte per la trasmissione dei dati da e verso l'esterno.

Domanda 35: Il fornitore protegge le sue reti e i suoi sistemi informativi dai software malevoli e non autorizzati? (EU Reg. 6.9.1)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Software di rilevamento presente ma non monitorato centralmente.

Domanda 36: Il fornitore attua la segmentazione della rete in reti o zone conformemente alla valutazione dei rischi? (EU Reg. 6.8.1)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Segmentazione di base senza giustificazione basata sul rischio.

Domanda 37: Esiste un registro (log) degli accessi da remoto eseguiti dal personale del fornitore ai sistemi del Soggetto NIS? (PR.AC-3.4)

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: Log degli accessi da remoto eseguiti e conservati per un periodo definito.

Domanda 38: Il fornitore garantisce che l'aggiornamento e la manutenzione delle risorse e dei sistemi siano eseguiti e registrati con strumenti controllati e autorizzati? (PR.MA-1.1)

Peso: 3

Risposta: Livello 2 (45%)

Descrizione: Esiste un registro ma è incompleto.

Domanda 39: I servizi gestiti o i servizi di sicurezza gestiti forniti sono progettati per essere resilienti in situazioni normali e avverse? (PR.IR-03.1 Sogg. Essenziali)

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: Utilizzo di sistemi di comunicazione di emergenza protetti, in accordo con la VA.

Domanda 40: Il fornitore ha un sistema per monitorare e registrare eventi potenzialmente avversi relativi alla fornitura del servizio? (DE.CM-09.1)

Peso: 4

Risposta: Livello 5 (100%)

Descrizione: Viene effettuata un'analisi e correlazione automatizzata dei dati per rilevare tempestivamente anomalie e gli strumenti sono ridondanti.

Continuità Operativa e Ripristino

Domanda 41: Il fornitore dispone di un Piano di Continuità Operativa (BCP) e di Ripristino in caso di Disastro (DRP) per i servizi forniti al Soggetto NIS (ID.IM-04.1/2)?

Peso: 5

Risposta: Livello 2 (45%)

Descrizione: Piani esistenti ma non documentati o non approvati.

Domanda 42: Il fornitore conserva copie di backup dei dati del Soggetto NIS e fornisce risorse sufficienti (personale, sistemi) per un adeguato livello di ridondanza? (PR.DS-11.1 / EU Reg. 4.2.1)

Peso: 5

Risposta: Livello 1 (25%)

Descrizione: Backup assenti o non gestiti.

Domanda 43: Il fornitore ha un Piano per la Gestione delle Crisi (CMP) che specifica i ruoli e le responsabilità in situazioni di crisi, inclusi quelli dei fornitori? (ID.IM-04.3.a)

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: Il CMP include modalità di comunicazione tra Soggetto NIS e autorità competenti.

Domanda 44: I ruoli del personale del fornitore nel piano di continuità operativa sono definiti, compresa la relativa istruzione e formazione? (ID.IM-04.1.b / PR.AT-01.1)

Peso: 3

Risposta: Livello 3 (65%)

Descrizione: Ruoli e responsabilità definiti nei piani; registro di formazione mantenuto (PR.AT-01.3).

Domanda 45: Il fornitore si impegna contrattualmente a rispettare i tempi e costi di ripristino in caso di indisponibilità dei servizi? (GV.SC-07.1.d)

Peso: 4

Risposta: Livello 5 (100%)

Descrizione: Esistono meccanismi di penalità o incentivi per garantire il rispetto degli SL/tempi di ripristino.

Domanda 46: Le procedure di ripristino del fornitore sono documentate per assicurare il recupero dei sistemi o asset coinvolti da un incidente di cybersecurity? (RC.RP-1.1)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Procedure informali o non testate.

Domanda 47: Il Soggetto NIS/Fornitore verifica che i piani di continuità siano riesaminati e aggiornati periodicamente o dopo incidenti significativi? (ID.IM-04.5)

Peso: 3

Risposta: Livello 2 (45%)

Descrizione: Aggiornamento solo in caso di grande cambiamento aziendale.

Domanda 48: Sono definite e documentate le tempistiche di conservazione dei log del fornitore, in accordo con la valutazione del rischio (ID.RA-05)? (DE.CM-01.3 / EU Reg. 3.2.5)

Peso: 3

Risposta: Livello 2 (45%)

Descrizione: Log conservati per un periodo indefinito o troppo breve.

Domanda 49: Il piano di trattamento del rischio del fornitore include la descrizione di eventuali misure di mitigazione compensative adottate per deroghe tecniche/normative? (ID.RA-06.2)

Peso: 4

Risposta: Livello 1 (25%)

Descrizione: Le deroghe non sono giustificate o compensate.

Domanda 50: Il fornitore ha definito un chiaro ordine di ripristino delle operazioni nel suo BCP/DRP per garantire una ripresa efficace dei servizi? (EU Reg. 4.1.2.e)

Peso: 3

Risposta: Livello 2 (45%)

Descrizione: Ordine di ripristino generico o basato solo su ipotesi non verificate.

Domanda 51: Il fornitore effettua regolarmente il monitoraggio e l'adeguamento delle risorse (impianti, sistemi, personale) in base ai requisiti di backup e ridondanza? (EU Reg. 4.2.5)

Peso: 3

Risposta: Livello 2 (45%)

Descrizione: Adeguamento delle risorse solo su base budgetaria.

Domanda 52: Il fornitore ha procedure per la gestione degli incidenti che consentono la valutazione e la classificazione tempestiva degli eventi sospetti? (EU Reg. 3.4.1)

Peso: 4

Risposta: Livello 5 (100%)

Descrizione: La classificazione e la rivalutazione degli eventi avvengono in modo dinamico non appena sono disponibili nuove informazioni.

Domanda 53: Il fornitore esegue una Business Impact Analysis (BIA) per valutare il potenziale impatto delle perturbazioni sui servizi forniti? (EU Reg. 4.1.3)

Peso: 4

Risposta: Livello 5 (100%)

Descrizione: La BIA è integrata con la valutazione del rischio (ID.RA-05) e informa direttamente i piani di continuità.

Domanda 54: Il fornitore conserva copie di backup protette da adeguati controlli di accesso fisici e logici? (EU Reg. 4.2.2.d)

Peso: 4

Risposta: Livello 1 (25%)

Descrizione: Accesso ai backup non controllato.

Domanda 55: Il fornitore ha procedure per la gestione di quasi-incidenti (near misses) e utilizza questi dati per il miglioramento? (RS.MA-01.3 / RC.IM)

Peso: 3

Risposta: Livello 3 (65%)

Descrizione: I piani di risposta (RS.MA-01.3) sono riesaminati e aggiornati periodicamente, integrando le lezioni apprese (lesson learned).

Domanda 56: Il fornitore definisce e monitora gli indicatori e le misure volti a monitorare lo stato di attuazione della propria politica di sicurezza (livello di maturità)? (EU Reg. 1.1.2.j)

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: I risultati del monitoraggio sono inclusi nelle relazioni periodiche agli organi di gestione (EU Reg. 2.2.1).

Domanda 57: Il fornitore garantisce che la valutazione del rischio sia riesaminata periodicamente (almeno ogni due anni) e in caso di cambiamenti significativi? (ID.RA-05.2)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Riesame solo quando richiesto dal cliente.

Domanda 58: Il fornitore dispone di un Piano di Sviluppo Sicuro per lo sviluppo di software/servizi TIC utilizzati nella fornitura? (PR.PS-02 / EU Reg. 6.2.1)

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: Norme stabilite per lo sviluppo sicuro di sistemi informativi e di rete, applicate a tutte le fasi (specifiche, progettazione, sviluppo, test).

Domanda 59: Il Soggetto NIS valuta contrattualmente i requisiti in materia di subappalto o subfornitura del fornitore (GV.SC-01.2.q)?

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: Il fornitore monitora e valuta le modifiche nelle pratiche di cibersicurezza dei subappaltatori (EU Reg. 5.1.6).

Domanda 60: Il fornitore ha un piano per la divulgazione coordinata delle vulnerabilità (CVD), in linea con la politica nazionale applicabile? (EU Reg. 6.10.2.e)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Procedura informale di risposta alle segnalazioni esterne.

Risposta agli Incidenti e Formazione

Domanda 61: Il fornitore ha l'obbligo contrattuale di notificare gli incidenti che presentano un rischio per la sicurezza del Soggetto NIS senza indebito ritardo? (EU Reg. 5.1.4.d / RS.CO-02)

Peso: 5

Risposta: Livello 2 (45%)

Descrizione: Obbligo di notifica, ma solo per incidenti che comportano indisponibilità completa.

Domanda 62: Il fornitore ha un Piano di Risposta agli Incidenti (IRP) che coordina le attività con le terze parti interessate? (RS.MA-01.1)

Peso: 4

Risposta: Livello 5 (100%)

Descrizione: L'IRP è testato periodicamente in esercizi congiunti (es. simulazioni di attacco) che coinvolgono il Soggetto NIS.

Domanda 63: Il fornitore si impegna a comunicare al Soggetto NIS le misure correttive o di mitigazione che possono essere adottate in risposta a una minaccia informatica significativa? (RS.CO-02.1.b)

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: Il fornitore offre attivamente supporto tecnico aggiuntivo al Soggetto NIS per la mitigazione.

Domanda 64: Il fornitore fornisce al proprio personale (e a quello con ruoli specializzati) una formazione periodica in materia di sicurezza? (PR.AT-01.1 / EU Reg. 8.2.1)

Peso: 5

Risposta: Livello 1 (25%)

Descrizione: Nessuna formazione o sensibilizzazione.

Domanda 65: La formazione include istruzioni sul comportamento da tenere in caso di eventi rilevanti per la sicurezza? (PR.AT-02.1.c)

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: Esercitazioni periodiche sul piano di risposta agli incidenti per testare la preparazione del personale (RS.CO-1.3).

Domanda 66: Il fornitore monitora i canali di comunicazione ufficiali (es. CSIRT Italia, Autorità di settore) per ricevere informazioni sulle vulnerabilità e minacce? (ID.RA-08.1 / EU Reg. 6.10.2.a)

Peso: 4

Risposta: Livello 1 (25%)

Descrizione: Nessun monitoraggio dei bollettini di sicurezza.

Domanda 67: Il fornitore garantisce che gli eventi di sicurezza siano monitorati per individuare un accesso non autorizzato o l'abuso dei privilegi concessi (IS-4)?

Peso: 4

Risposta: Livello 1 (25%)

Descrizione: Nessun monitoraggio attivo dei comportamenti anomali.

Domanda 68: Il fornitore ha definito procedure per l'analisi forense e la conservazione delle prove in caso di incidente?

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: Procedure documentate per la gestione delle prove (es. acquisizione di immagini forensi) in caso di incidente critico.

Domanda 69: Il fornitore gestisce in modo appropriato la Disclosures (divulgazione) dei dati personali al Soggetto NIS e a terzi in caso di incidente che comporta violazione dei dati?

Peso: 3

Risposta: Livello 2 (45%)

Descrizione: Procedura base di notifica del Soggetto NIS/Titolare.

Domanda 70: Il fornitore si impegna contrattualmente a rispettare i requisiti di certificazione della cibersicurezza richiesti dal Soggetto NIS? (Art. 27 NIS2)

Peso: 4

Risposta: Livello 1 (25%)

Descrizione: Il fornitore non possiede o non si impegna a ottenere certificazioni.

Domanda 71: Le procedure di risposta agli incidenti del fornitore sono sottoposte a esercitazioni periodiche (es. simulazioni di attacco) per testare l'efficacia? (RS.CO-1.3)

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: Esercitazioni periodiche (es. tabletop o funzionali) e mantenimento di un registro aggiornato delle esercitazioni e dei partecipanti.

Domanda 72: Il fornitore ha un processo definito per la gestione degli asset, che comprende l'identificazione di un proprietario (owner) responsabile della protezione della risorsa? (EU Reg. 12.2.1)

Peso: 3

Risposta: Livello 4 (85%)

Descrizione: L'inventario degli asset (HW/SW) è collegato al proprietario e al livello di classificazione.

Domanda 73: Il fornitore adotta pratiche di 'igiene informatica di base' (es. zero trust principles, configurazione sicura dei dispositivi, segmentazione)? (Art. 24.2.g / EU Reg. 8.1)

Peso: 4

Risposta: Livello 5 (100%)

Descrizione: Implementazione di principi Zero Trust e misure tecniche avanzate di segmentazione della rete.

Domanda 74: Il fornitore garantisce che gli amministratori di sistema siano individuati previa valutazione dell'esperienza, capacità e affidabilità? (GV.RR-04.2 - Sogg. Essenziali)

Peso: 3

Risposta: Livello 2 (45%)

Descrizione: Valutazione basata solo sulla competenza tecnica.

Domanda 75: Il fornitore dispone di procedure per la gestione della sicurezza dei supporti rimovibili (es. chiavette USB)? (PR.DS-11.2 - Sogg. Essenziali / EU Reg. 12.3)

Peso: 4

Risposta: Livello 5 (100%)

Descrizione: L'utilizzo dei supporti rimovibili sui sistemi rilevanti è limitato o completamente bloccato.

Domanda 76: Il fornitore gestisce in modo sicuro i dati relativi ai test di sicurezza (es. sanificazione o anonimizzazione) per evitare fughe di dati? (EU Reg. 6.2.2.e/f)

Peso: 4

Risposta: Livello 1 (25%)

Descrizione: Dati di test non protetti (es. dati di produzione reali).

Domanda 77: Il fornitore dispone di una politica di divulgazione dei dati (data handling policy) coerente con la classificazione degli asset (EU Reg. 12.1.2.b)?

Peso: 3

Risposta: Livello 5 (100%)

Descrizione: La classificazione è continuamente allineata agli obiettivi di business (BIA) e ai requisiti di protezione NIS2.

Domanda 78: Il fornitore si impegna contrattualmente a fornire al Soggetto NIS la documentazione necessaria per dimostrare la conformità NIS2? (EU Reg. 5.1.4)

Peso: 5

Risposta: Livello 3 (65%)

Descrizione: Obbligo contrattuale di fornire, su richiesta, i principali documenti (es. Politiche di sicurezza, report di audit, piano BCP/DRP).

Domanda 79: Il fornitore ha stabilito una politica e procedure relative alla gestione delle chiavi crittografiche? (EU Reg. 9.2)

Peso: 4

Risposta: Livello 4 (85%)

Descrizione: Viene applicata la gestione delle chiavi in base alla classificazione della risorsa e sono definiti ruoli specifici (Key Custodians).

Domanda 80: Il fornitore riesamina i suoi processi di sicurezza a intervalli pianificati e in seguito a incidenti significativi o cambiamenti significativi delle operazioni? (EU Reg. 2.0.5)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Riesame solo annuale, indipendentemente dagli incidenti.

Conformità, Vigilanza e Requisiti Aggiuntivi

Domanda 81: Il fornitore ha adottato e attuato un Piano di Trattamento del Rischio basato sugli esiti della valutazione del rischio (ID.RA-06.1)?

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Il piano esiste ma non definisce le priorità o le tempistiche.

Domanda 82: Il fornitore si impegna contrattualmente a fornire al Soggetto NIS i risultati degli audit sulla sicurezza (Art. 32.7 NIS2)?

Peso: 3

Risposta: Livello 2 (45%)

Descrizione: Condivisione limitata a estratti o su richiesta formale.

Domanda 83: Il personale del fornitore partecipa ai programmi di formazione e sensibilizzazione sulla sicurezza informatica del Soggetto NIS? (PR.AT-01.2)

Peso: 3

Risposta: Livello 2 (45%)

Descrizione: Partecipazione reattiva e non obbligatoria.

Domanda 84: Il fornitore ha un processo per identificare le vulnerabilità utilizzando informazioni provenienti da fonti interne ed esterne? (ID.RA-08.2)

Peso: 4

Risposta: Livello 1 (25%)

Descrizione: Nessun processo per identificare le vulnerabilità.

Domanda 85: I processi di gestione del rischio del fornitore sono approvati dagli organi di amministrazione e direttivi (se Soggetto NIS) o dal management appropriato? (ID.RA-05.3)

Peso: 5

Risposta: Livello 4 (85%)

Descrizione: Gli organi direttivi ricevono relazioni periodiche sullo stato del rischio e della conformità.

Domanda 86: Il fornitore dispone di un meccanismo per la registrazione di tutte le attività privilegiate e amministrative sui sistemi rilevanti? (DE.CM-01.1)

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: Tutte le attività, inclusi gli accessi e le operazioni privilegiate, sono registrate e conservate in modo sicuro.

Domanda 87: Il fornitore utilizza la Divulgazione Coordinata delle Vulnerabilità (CVD) per interagire con i produttori di software/servizi TIC che utilizza nella fornitura?

Peso: 4

Risposta: Livello 1 (25%)

Descrizione: Nessuna interazione formale con i produttori per le vulnerabilità.

Domanda 88: Il Soggetto NIS/Fornitore verifica che i contratti includano clausole che limitano la dipendenza da un unico fornitore (single point of failure), se applicabile? (EU Reg. 5.1.2.d)

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: La VA del Soggetto NIS identifica eventuali singoli punti di vulnerabilità (EU Reg. 2.1.2.d).

Domanda 89: Il fornitore stabilisce procedure adeguate per la gestione dell'accesso remoto (PR.AC-3) e il monitoraggio degli stessi?

Peso: 4

Risposta: Non risposta

Descrizione: N/A

Domanda 90: Il fornitore garantisce che l'aggiornamento del software critico avvenga in un ambiente di test prima della messa in produzione, fatte salve motivate urgenze di sicurezza? (PR.MA-1.3 - PSNC/Sogg. Essenziali)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Test eseguiti solo su aggiornamenti maggiori.

Domanda 91: Il fornitore supporta il Soggetto NIS nel rispondere alle richieste di accesso a dati, documenti e informazioni da parte dell'Autorità Competente NIS (Art. 36.1.c)?

Peso: 5

Risposta: Livello 4 (85%)

Descrizione: Il fornitore ha procedure interne per facilitare la fornitura tempestiva delle informazioni richieste.

Domanda 92: Il fornitore si impegna a prevenire o ridurre le conseguenze di eventi derivanti da minacce fisiche e ambientali (es. catastrofi naturali)? (EU Reg. 13.2.1)

Peso: 3

Risposta: Livello 2 (45%)

Descrizione: Misure di protezione base non basate sul rischio.

Domanda 93: Il Soggetto NIS/Fornitore si assicura che i requisiti di sicurezza siano rispettati anche per le applicazioni custom, commerciali o open-source utilizzate nella fornitura? (ID.AM-03 / GV.SC-01)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Valutazione limitata al software custom.

Domanda 94: Il fornitore adotta un processo disciplinare per la gestione delle violazioni delle politiche di sicurezza? (EU Reg. 10.1.3)

Peso: 3

Risposta: Livello 4 (85%)

Descrizione: Il processo è applicato in modo coerente e i risultati sono documentati per l'analisi dei rischi residui.

Domanda 95: Il fornitore utilizza sistemi di comunicazione di emergenza protetti in accordo agli esiti della valutazione del rischio? (PR.IR-03.1 - Sogg. Essenziali)

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Sistemi di comunicazione di emergenza non testati.

Domanda 96: Il Soggetto NIS definisce a livello contrattuale gli obblighi di sicurezza che rimangono validi dopo la cessazione o modifica del rapporto di lavoro del personale del fornitore (es. clausole di riservatezza)? (GV.RR-04.4 - Sogg. Essenziali)

Peso: 4

Risposta: Livello 1 (25%)

Descrizione: Nessuna clausola post-contrattuale di sicurezza.

Domanda 97: Il fornitore ha un piano per la valutazione dell'efficacia delle misure di gestione del rischio per la sicurezza informatica (ID.IM-01.3 - Sogg. Essenziali)?

Peso: 4

Risposta: Livello 2 (45%)

Descrizione: Valutazione limitata ai risultati di audit interni.

Domanda 98: Il fornitore garantisce la piena collaborazione nell'analisi e mitigazione di incidenti che impattano la fornitura? (Art. 36.1.c)

Peso: 5

Risposta: Livello 2 (45%)

Descrizione: Collaborazione limitata e lenta.

Domanda 99: La fornitura richiede l'accesso a Proprietà Intellettuale (IP) o dati critici del Soggetto NIS e, in tal caso, tale accesso è gestito in base alla criticità? (GV.SC-07.1.b)

Peso: 4

Risposta: Livello 3 (65%)

Descrizione: L'accesso alla PI e ai dati è valutato e documentato in base alla criticità.

Domanda 100: La documentazione di cybersecurity del fornitore è organizzata e mantenuta in modo che sia facilmente fruibile e consultabile per chi ne ha necessità? (Guida alla lettura NIS2)

Peso: 3

Risposta: Livello 3 (65%)

Descrizione: Documentazione (policy, procedure, registri) mantenuta in formato cartaceo o digitale, facilmente fruibile.
