NISPHERE

Manuale d'uso

Piattaforma di governance e operatività NIS2

OBIETTIVO Guidare CISO, responsabili, revisori, amministratori e componenti del board nell'uso quotidiano della piattaforma, dalla configurazione iniziale alla gestione delle evidenze e degli incidenti.

Versione	1.0
Data	27 agosto 2026
Destinatari	Utenti delle workspace Nisphere

Come usare questo manuale

Questo manuale descrive le funzionalità presenti nell'interfaccia web Nisphere e nell'agente Endpoint. Le voci, i pulsanti e i campi possono essere visibili o nascosti in base al ruolo, al perimetro assegnato e alla licenza della workspace.

IMPORTANTE Nisphere aiuta a organizzare, tracciare e dimostrare le attività NIS2; le decisioni legali, regolatorie e di notifica restano in capo all'organizzazione e ai suoi professionisti incaricati.

Indice operativo

Convenzioni usate

- I nomi tra virgolette, ad esempio "Concludi e genera gap", corrispondono a pulsanti o stati dell'interfaccia.
- Le istruzioni usano il percorso di navigazione della barra laterale; selezionare prima la workspace corretta.
- Quando un'azione non è disponibile, non aggirare il controllo: chiedere al tenant administrator o al CISO di verificare ruolo e perimetro.

1. Accesso, password e workspace

Accedere alla piattaforma

1. Aprire l'indirizzo Nisphere comunicato dall'amministratore della propria organizzazione.
2. Inserire indirizzo email e password nella schermata "Accedi alla workspace".
3. Se il profilo è collegato a più aziende, scegliere la workspace proposta e confermare l'accesso.
4. Al primo accesso o dopo un reset, impostare una nuova password quando richiesto.

PASSWORD DIMENTICATA Usare il collegamento “Hai dimenticato la password?” nella pagina di accesso. Inserire l’indirizzo registrato e seguire il collegamento ricevuto. Il reset non modifica ruoli, perimetri o collegamenti ad altre aziende.

Cambiare azienda di lavoro

Un’identità può essere condivisa tra più aziende. Dopo l’accesso, utilizzare il comando di cambio workspace disponibile nel profilo; verificare sempre il nome dell’azienda prima di creare o aggiornare informazioni. I dati di una workspace non sono visibili nelle altre, salvo collegamenti espressamente autorizzati.

Stati utente

Stato	Significato operativo
Invitato	L’utente è stato creato/invitato e deve completare l’attivazione.
Attivo	Può accedere nel rispetto di ruolo e scope.
Sospeso	Non può usare la piattaforma finché non viene riattivato.

2. Ruoli, scope e responsabilità

L’accesso è regolato da quattro elementi: autenticazione, appartenenza alla workspace, ruolo e perimetro (tenant, entità legale o soggetto regolato). Il sistema applica inoltre ownership e riservatezza del record.

Ruolo	Uso prevalente
Tenant administrator	Gestione utenti, ruoli, entità e impostazioni della workspace.
CISO	Guida del programma NIS2, visibilità completa, dashboard, incidenti e governance.
Governance manager	Obblighi, controlli, evidenze, assessment, gap e audit pack.
Incident manager	Gestione della incident room e del flusso di notifica.
Control owner	Aggiornamento dei controlli, evidenze e azioni assegnate.
Evidence reviewer	Revisione e approvazione/rifiuto delle evidenze.
Auditor	Consultazione tracciata, limitata agli ambiti assegnati.
Board viewer	KPI, trend e decision log in sola lettura.
Platform administrator	Amministrazione della piattaforma e dei clienti, separata dai contenuti del tenant.

SEGREGAZIONE Chi carica un’evidenza non dovrebbe approvarla. Se il ruolo non permette l’azione, assegnare la revisione a un evidence reviewer o al CISO secondo le policy interne.

3. Avvio del programma NIS2

Dashboard: orientarsi tra le priorità

La Dashboard sintetizza gli elementi da presidiare: obblighi, gap aperti, assessment, incidenti attivi, evidenze e formazione. Usarla come punto di partenza per il controllo periodico, quindi aprire il modulo indicato dalla metrica o dalla priorità.

1. Accedere alla Dashboard.
2. Controllare le metriche di attenzione, i gap aperti e gli incidenti attivi.
3. Aprire la sezione di lavoro corrispondente e assegnare un owner o una scadenza, se mancanti.
4. Aggiornare i record alla fonte: la Dashboard deve riflettere lo stato effettivo, non essere compilata manualmente.

Soggetti regolati e obblighi

Nella sezione “Soggetti regolati” si definisce il perimetro organizzativo soggetto alla governance NIS2. Per ciascun soggetto, la workspace espone obblighi e lo spazio di conformità collegato.

1. Aprire “Soggetti regolati” e selezionare “Nuovo soggetto” se autorizzati.
2. Compilare i dati identificativi e il perimetro richiesto.
3. Aprire il soggetto creato per consultare obblighi, controlli, evidenze e attività correlati.
4. Assegnare owner coerenti con la responsabilità effettiva e mantenere aggiornato lo stato operativo.

BUONA PRATICA Creare un soggetto distinto quando cambiano responsabilità, perimetro di rischio o obblighi applicabili; evitare duplicati generati per aggirare report o filtri.

Organizzazione, board e responsabilità

L’anagrafica organizzativa raccoglie persone, componenti del board e responsabilità. Serve a collegare ownership, formazione e flussi decisionali ai soggetti reali.

- Registrare nome, email, ruolo organizzativo, ufficio/reparto e sede quando disponibili.
- Usare le sezioni Board e responsabilità per rappresentare gli organi e gli incarichi di governance.
- Mantenere aggiornate le relazioni quando un responsabile cambia funzione o lascia l’organizzazione.

Asset

La sezione “Asset” crea e mantiene il registro degli asset organizzativi. Un asset può essere classificato, assegnato a un owner e collegato alle attività di fornitori, controlli e endpoint.

1. Aprire “Asset” e scegliere l’azione di creazione.
2. Inserire nome, tipologia, criticità, posizione e owner; usare la tipologia “Endpoint” per PC e Mac gestiti dall’agente.
3. Salvare e verificare che l’asset compaia nell’elenco filtrato.
4. Aggiornare ownership, stato e criticità quando cambiano nel ciclo di vita dell’asset.

4. Controlli, evidenze e assurance

Collegare obblighi e controlli

"Controlli ed evidenze" è l'area di assurance: mette in relazione gli obblighi del soggetto regolato, le misure implementate e le prove che ne dimostrano esistenza, applicazione ed efficacia.

1. Aprire "Controlli ed evidenze" e selezionare il soggetto regolato rilevante.
2. Consultare gli obblighi e il loro stato.
3. Creare o aggiornare il controllo, definendo owner, stato e informazioni operative richieste.
4. Collegare il controllo all'obbligo pertinente e verificare che il collegamento sia visibile nello spazio di compliance.

Gestire le evidenze

Un'evidenza rappresenta la prova controllabile di un controllo o di un'attività: documento, registro, attestazione, risultato o altro elemento previsto dalla policy. Le evidenze possono essere collegate ai record pertinenti e sottoposte a workflow di revisione.

1. Aprire il controllo o il workspace assurance e creare l'evidenza.
2. Compilare titolo, descrizione, owner, data e validità secondo la procedura interna.
3. Collegare l'evidenza al controllo, all'obbligo o al record di origine disponibile.
4. Inviare l'evidenza in revisione con "Submit" quando è completa.
5. Il reviewer approva o rifiuta; in caso di rifiuto, correggere la prova e ripresentarla.
6. Rinnovare l'evidenza prima della scadenza quando la validità temporale lo richiede.

Stato/azione	Quando usarlo
Bozza / aggiornamento	Durante preparazione e raccolta della prova.
Invio in revisione	Quando il contenuto è completo e collegato al record corretto.
Approvazione	Quando il reviewer valuta la prova adeguata.
Rifiuto	Quando mancano contenuti, collegamenti, validità o coerenza.
Rinnovo	Quando serve una nuova versione o una nuova validità.

ATTENZIONE Non allegare o descrivere più dati personali o tecnici sensibili del necessario. Applicare classificazione, accesso ristretto e policy di conservazione dell'organizzazione.

5. Assessment, gap e remediation

Eseguire un assessment

La sezione "Assessment" supporta la valutazione strutturata della conformità. Gli elementi vengono organizzati per gruppi; le risposte determinano lo stato e, alla conclusione, i gap da trattare.

1. Aprire "Assessment" e creare una nuova valutazione per il soggetto o il perimetro previsto.
2. Rispondere agli item, scegliendo lo stato più aderente alle evidenze disponibili.
3. Salvare i progressi durante il lavoro; non concludere finché le risposte non sono state controllate.

4. Selezionare “Concludi e genera gap”. Il sistema indica il numero di gap che saranno creati dagli item non conformi o non applicabili secondo la logica della valutazione.
5. Usare “Nuova valutazione” per un ciclo successivo; archiviare una valutazione conclusa solo quando deve restare nello storico.

Gestire gap e azioni correttive

Un gap rappresenta uno scostamento da trattare. Le remediation actions rendono il piano operativo: definiscono cosa fare, chi è responsabile e lo stato di avanzamento.

1. Aprire “Gap aperti” e selezionare il gap da analizzare.
2. Verificare origine, descrizione, impatto, owner e scadenza.
3. Creare una o più azioni correttive; usare azioni separate quando responsabilità o date differiscono.
4. Assegnare l’azione al control owner competente e aggiornare stato e note al progredire del lavoro.
5. Chiudere il gap solo dopo aver verificato l’azione e aggiornato i controlli/evidenze che dimostrano la correzione.

REGOLA OPERATIVA La conclusione di un’action non equivale automaticamente alla chiusura del gap: la chiusura richiede la verifica dell’efficacia e la documentazione della prova.

6. Gestione degli incidenti

Aprire e governare una incident room

La sezione “Incidenti” riunisce le informazioni operative dell’incidente: titolare, stato, azioni, attività, evidenze e notifiche. Per incidenti ristretti, il dettaglio resta visibile solo agli utenti autorizzati.

1. Aprire “Incidenti” e scegliere la creazione di un nuovo incidente.
2. Indicare titolo, soggetto regolato, owner e dati disponibili; usare descrizioni fattuali e aggiornabili.
3. Aprire l’incidente dall’elenco per accedere alla incident room.
4. Registrare azioni e attività via via che vengono svolte, mantenendo cronologia e responsabilità chiare.
5. Valutare se l’incidente è significativo e gestire le notifiche previste attraverso l’area “Notifiche ACN”.
6. Chiudere soltanto dopo avere compilato causa radice, risoluzione/ripristino e lesson learned.

Azioni, attività e notifiche ACN

Componente	Uso corretto
Azioni	Task operativi con owner e stato: contenimento, analisi, ripristino, verifica.
Attività	Traccia cronologica delle evidenze e degli eventi significativi della gestione.
Notifiche ACN	Gestione della predisposizione e dell’invio nel workflow previsto. Verificare sempre contenuto, autorità competente e responsabilità prima dell’invio.
Chiusura	Riepilogo finale di causa radice, risoluzione e miglioramenti; preserva l’apprendimento organizzativo.

CRITICITÀ Nisphere non sostituisce la valutazione legale o regolatoria sulla notifica. Per casi reali, coinvolgere tempestivamente CISO, incident manager, legale e le funzioni designate dalla procedura di incident response.

7. Fornitori e formazione

Fornitori e catena di approvvigionamento

Il modulo "Fornitori" raccoglie i fornitori, contatti, offerte e relazioni con l'organizzazione. Lo workspace della relazione organizza due diligence, assessment, contratti, review, finding, incidenti ed exit plan.

1. Creare il fornitore e registrare i contatti per sicurezza, incidenti, tecnico, privacy, commerciale e legale quando pertinenti.
2. Creare la relazione con il soggetto regolato o l'entità interessata e assegnarne l'owner.
3. Nello workspace, eseguire il security assessment e registrare i risultati.
4. Associare asset, contratti e clausole; inviare i documenti al legal review quando richiesto.
5. Pianificare la review successiva e registrare finding o incidenti connessi.
6. Preparare l'exit plan per relazioni critiche o da terminare.

Formazione cybersecurity

La sezione "Formazione" permette di organizzare persone, corsi, campagne e iscrizioni. Usarla per dimostrare che la formazione è pianificata, assegnata e monitorata.

1. Registrare o aggiornare i dipendenti con ruolo, reparto e sede.
2. Creare i corsi disponibili e indicare se la formazione è obbligatoria.
3. Creare una campagna, impostare il pubblico e la finestra temporale.
4. Generare o gestire le iscrizioni e aggiornare gli esiti.
5. Monitorare lo stato delle persone e intervenire sui ritardi prima delle scadenze.

8. Documenti, Board Portal ed Endpoint

Documenti e verbali

Il modulo "Documenti" governa documenti e verbali collegabili a soggetti, assessment, incidenti e altri record. Sono disponibili modelli, opzioni di collegamento, bozze, invio in revisione, review e rendering.

1. Aprire "Documenti" e scegliere un modello coerente con il contenuto.
2. Creare il documento, compilare titolo e contenuti richiesti e impostare i collegamenti di origine.
3. Salvare e aggiornare la bozza fino alla completezza.
4. Inviare in revisione; il reviewer decide secondo il workflow autorizzato.
5. Usare la funzione di rendering per verificare il risultato leggibile prima della distribuzione o del verbale finale.

Richieste di approvazione al board

Il Board Portal permette di creare richieste di approvazione e raccogliere voti dai componenti autorizzati. Le richieste mantengono un contenuto e una versione definiti; il voto è tracciato e non deve sostituire le formalità societarie applicabili.

1. Aprire la sezione Board Portal e creare una richiesta, includendo oggetto, documento/versione e motivazione.
2. Verificare che i membri del board siano aggiornati nell'anagrafica organizzativa.
3. I componenti autorizzati consultano la richiesta e registrano il voto.
4. Il proponente può annullare una richiesta, motivando l'operazione, se il processo interno lo richiede.
5. Conservare il verbale e la delibera secondo le procedure societarie e documentali applicabili.

Endpoint monitoring

Il modulo "Endpoint" visualizza gli endpoint registrati, i check-in e i dettagli raccolti dall'agente. L'agente desktop è disponibile per Windows 11 e macOS; registra il PC/Mac come asset Endpoint e invia un check-in giornaliero.

1. In "Endpoint", aprire "Configura un nuovo endpoint".
2. Selezionare piattaforma, criticità e posizione; scaricare il file di configurazione che contiene tenant, entità legale e token di enrollment.
3. Conservare il file in un percorso protetto e distribuirlo con il pacchetto dell'agente.
4. Su macOS estrarre il pacchetto e trascinare il config.json su "Installa Nisphere Agent"; su Windows usare il pacchetto/installer predisposto dall'organizzazione.
5. Dopo la prima registrazione, verificare nella dashboard che endpoint, asset e ultimo check-in siano presenti.
6. Aprire un endpoint per consultare inventario software, caratteristiche macchina, disco ed errori rilevati.

SICUREZZA DEL TOKEN Il token iniziale serve alla prima registrazione. Dopo il successo l'agente lo rimuove dal file e usa un segreto di enrollment per i check-in successivi. Non condividere config.json in canali non protetti e non archiviarlo in repository pubblici.

La dashboard locale dell'agente è disponibile esclusivamente sul PC endpoint all'indirizzo http://127.0.0.1:48 100. I dati locali vengono mantenuti come snapshot limitati; la piattaforma Nisphere resta il punto di controllo centrale.

9. Amministrazione piattaforma

L'area di amministrazione piattaforma è dedicata ai profili platform administrator. È distinta dalla gestione operativa del tenant e serve a governare clienti, licenze, utenti e collegamenti CISO.

1. Aprire l'amministrazione e selezionare il cliente.
2. Verificare dati cliente, stato della licenza e workspace abilitate.
3. Creare o aggiornare utenti, scegliendo il ruolo appropriato.
4. Attivare o sospendere un account quando necessario.
5. Usare il reset password solo quando richiesto: la password è condivisa tra le aziende collegate e l'utente dovrà cambiarla al prossimo accesso.
6. Collegare il CISO e verificare che accesso e ruolo riflettano la responsabilità reale.

PRIVILEGI Un platform administrator non deve consultare contenuti tenant salvo necessità autorizzata e tracciata. Separare sempre attività di supporto tecnico e decisioni operative di compliance.

10. Routine consigliate

Frequenza	Routine
Ogni giorno	Controllare Dashboard, incidenti attivi, azioni urgenti e check-in endpoint.
Ogni settimana	Aggiornare remediation, review fornitori, evidenze in attesa e corsi in scadenza.
Ogni mese	Rivedere asset/owner, stato controlli, evidenze in rinnovo e KPI per CISO.
A ogni assessment	Validare le risposte, analizzare i gap generati, assegnare azioni e pianificare il riesame.
A ogni incidente	Aggiornare incident room in tempo reale, preservare evidenze e completare lesson learned prima della chiusura.

Checklist di qualità prima di una review o audit

- Ogni soggetto regolato ha owner, obblighi e controlli aggiornati.
- Le evidenze sono collegate al record corretto, hanno owner e validità verificabili.
- I gap aperti hanno una remediation action, un responsabile e una data.
- Gli assessment conclusi hanno generato e tracciato gli scostamenti rilevanti.
- Le relazioni con fornitori critici hanno assessment, review e piano di uscita quando previsto.
- La formazione obbligatoria ha destinatari, stato e follow-up documentati.
- Incidenti e richieste board hanno cronologia e documenti coerenti con le procedure interne.

11. Risoluzione dei problemi

Situazione	Cosa verificare
Non vedo una sezione o un pulsante	Controllare ruolo, scope e workspace selezionata. Chiedere al tenant administrator se il permesso è necessario.
Non riesco ad accedere	Verificare email, password, stato account e workspace. Usare il recupero password se necessario.
Un'evidenza non può essere approvata	Verificare che il reviewer sia diverso dal caricatore e abbia il ruolo evidence reviewer o CISO autorizzato.
Non riesco a chiudere un incidente	Compilare causa radice, risoluzione/ripristino e lesson learned; controllare che le azioni richieste siano aggiornate.
Un endpoint non appare	Controllare il config.json, la connettività, la registrazione iniziale e l'ultimo check-in. Non riutilizzare il token dopo la registrazione.
Dati nella workspace errata	Non duplicare i record: passare alla workspace corretta e chiedere supporto per la rettifica secondo le procedure interne.

Supporto e tracciabilità

Quando si richiede supporto, indicare sempre: workspace coinvolta, modulo, record interessato, orario approssimativo, messaggio visualizzato e screenshot privo di dati sensibili. Non inviare password, token di enrollment o documenti riservati in chiaro.

Glossario

Termine	Definizione
Workspace	Ambiente di lavoro associato a un'azienda/tenant e ai relativi dati.
Soggetto regolato	Perimetro organizzativo gestito nel programma NIS2.
Controllo	Misura organizzativa, tecnica o procedurale da attuare e dimostrare.
Evidenza	Prova verificabile dell'esistenza, applicazione o efficacia di un controllo.
Assessment	Valutazione strutturata della conformità o maturità.
Gap	Scostamento da trattare con una o più azioni correttive.
Remediation action	Attività assegnata per correggere o ridurre un gap.
Endpoint	PC o Mac censito e monitorato dall'agente Nisphere.
Scope	Limite autorizzativo applicato a tenant, entità legale o soggetto regolato.