

# GUIDA INTEGRATIVA ALL'IMPLEMENTAZIONE

## Come applicare il modello CSI per la sicurezza del cloud nella tua organizzazione

Guida di accompagnamento al progetto «*Go Cloud! Go Secure! A Cloud Security Implementation Model for SMEs*» (Erasmus+ 2024-1-AT01-KA220-VET-000245093).

Materiali formativi e strumenti interattivi: [gocloudsecure.eu](https://gocloudsecure.eu)

### 1. Obiettivo della guida

Il modello CSI si articola in cinque fasi e aiuta le piccole e medie imprese (PMI) a proteggere i servizi cloud che utilizzano, siano essi software (SaaS), piattaforme (PaaS) o infrastrutture (IaaS).

Questa guida integra la documentazione ufficiale del modello CSI. Presenta ogni fase in modo sintetico e, attraverso un esempio pratico, mostra come seguire il percorso e adattarlo alle esigenze della propria impresa.

Per approfondimenti, modelli e istruzioni dettagliate, consulta i documenti dedicati alle cinque fasi del modello CSI.

Usa questa guida insieme ai due principali strumenti CSI:

- **CSI Matrix:** Strumento interattivo per individuare minacce, vulnerabilità e rischi dei servizi cloud e valutarli secondo l'OWASP Top 10. Si utilizza nelle fasi 1–3.
- **CSI Self-Assessment & CSI Course (SecureCloud SME):** Autovalutazione e materiali formativi sulle basi del cloud, le minacce informatiche, la progettazione sicura e la governance. Aiutano a preparare e svolgere la formazione nelle fasi 3–4.

*Suggerimento: Tieni aperti la guida e CSI Matrix durante le fasi 1–3. Segui le istruzioni, completa la valutazione e utilizza i risultati nelle fasi successive.*

## 2. Il modello CSI in sintesi

Il modello CSI segue un ciclo continuo di cinque fasi. Ognuna ha un obiettivo preciso, passaggi essenziali e risultati che diventano la base della fase successiva.

| Fase                     | Obiettivo                                                         | Passaggi principali                                                             | Risultati                                                                   |
|--------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| <b>1. Analisi</b>        | Comprendere l'uso del cloud, le minacce e gli obblighi normativi. | Inventario dei servizi · Valutazione con CSI Matrix · Verifica della conformità | Inventario cloud, prima valutazione CSI Matrix, requisiti applicabili.      |
| <b>2. Definizione</b>    | Definire regole, priorità dei rischi e obiettivi di protezione.   | Politica di sicurezza · Priorità · Obiettivi · Ruoli e responsabilità           | Politica di sicurezza cloud, rischi prioritari, obiettivi e responsabilità. |
| <b>3. Pianificazione</b> | Tradurre rischi e obiettivi in un piano operativo concreto.       | Mitigazione · Associazione delle misure · Documentazione · Formazione           | Piano di intervento, tabella, modelli, checklist e piano formativo.         |
| <b>4. Attuazione</b>     | Applicare le misure e formare il personale.                       | Interventi tecnici · Formazione e sensibilizzazione                             | Misure applicate, formazione svolta e ambiente più sicuro e conforme.       |
| <b>5. Verifica</b>       | Verificare l'efficacia e migliorare continuamente.                | Test · Monitoraggio KPI · Registro incidenti e feedback                         | Controlli verificati, cruscotto, lezioni apprese e politiche migliorate.    |

## 3. Istruzioni passo dopo passo

Segui le cinque fasi nell'ordine indicato: i risultati di ciascuna costituiscono il punto di partenza della successiva.

### Fase 1 – Analisi

**Obiettivo:** Capire quali servizi cloud utilizza la tua impresa, a quali minacce e vulnerabilità è esposta e quali obblighi di conformità deve rispettare.

- **Inventario dei servizi cloud:** Elenca tutti i servizi utilizzati (IaaS, PaaS, SaaS, archiviazione, database, reti e servizi di sicurezza). Indica quelli essenziali per l'attività.
- **Valutazione dei rischi:** Usa CSI Matrix per individuare le minacce di ogni servizio (es. violazioni dei dati, attacchi DDoS), le vulnerabilità (es. autenticazione debole) e i possibili rischi (es. perdita di dati, furto di account).
- **Verifica della conformità:** Controlla le norme UE applicabili (GDPR, DORA, NIS2) e gli standard già adottati o che intendi adottare (ISO/IEC 27001, ISO/IEC 27017, ISO 22301).

**Risultato:** Inventario dei servizi cloud, valutazione completata con CSI Matrix ed elenco dei requisiti di conformità pertinenti.

## Fase 2 – Definizione

**Obiettivo:** Stabilire regole di sicurezza, dare priorità ai rischi e definire gli obiettivi di protezione dell'impresa.

- **Politica di sicurezza:** Redigi una politica di sicurezza del cloud che disciplini l'uso sicuro dei servizi, la gestione degli accessi e la protezione dei dati.
- **Priorità dei rischi:** Valuta ogni rischio di CSI Matrix in base alla probabilità che si verifichi e al suo impatto. Concentrati su quelli più rilevanti.
- **Obiettivi di protezione:** Fissa un obiettivo chiaro per ogni rischio prioritario. Ad esempio, a «autenticazione debole» può corrispondere «rafforzare la sicurezza degli account».
- **Ruoli e responsabilità:** Stabilisci chi gestisce il cloud, i dati, la sicurezza e la conformità normativa. Nelle PMI più piccole, una persona può ricoprire più ruoli.

**Risultato:** Politica di sicurezza del cloud, rischi ordinati per priorità, obiettivi definiti e responsabilità assegnate.

## Fase 3 – Pianificazione

**Obiettivo:** Trasformare rischi e obiettivi di protezione in un piano operativo con misure tecniche, documentazione e formazione.

- **Misure di mitigazione:** Definisci un'azione concreta per ogni obiettivo. Ad esempio, per «rafforzare la sicurezza degli account» attiva l'autenticazione a più fattori (MFA).
- **Associazione delle misure:** Crea una tabella che indichi quale servizio cloud viene protetto da ciascuna misura.
- **Documentazione:** Prepara una checklist di implementazione, un modello per la gestione degli incidenti e una scheda di revisione dei log di audit.
- **Piano formativo:** Organizza brevi moduli pratici basati sui materiali CSI e adatti alle competenze e alle esigenze del gruppo di lavoro.

**Risultato:** Elenco delle misure di mitigazione, tabella di associazione, documenti operativi e piano formativo.

## Fase 4 – Attuazione

**Obiettivo:** Applicare le misure previste ai servizi cloud interessati e formare il personale.

- **Interventi tecnici:** Attua il piano della fase 3: abilita, ad esempio, MFA, crittografia e politiche di gestione delle identità e degli accessi (IAM, RBAC). Inizia dagli interventi semplici e di immediata utilità, sfruttando strumenti integrati come AWS Config o Azure Security Center.
- **Formazione e sensibilizzazione:** Realizza il programma formativo, concentrandoti sui rischi emersi da CSI Matrix e utilizzando i materiali didattici CSI.

**Risultato:** Misure di sicurezza applicate, personale formato ed evidenze dell'implementazione.

## Fase 5 – Verifica

**Obiettivo:** Valutare l'efficacia delle misure adottate e migliorare continuamente la sicurezza dell'impresa.

- **Test:** Esegui attacchi simulati, verifiche dei controlli e valutazioni di sicurezza.

- **Monitoraggio:** Tieni sotto controllo indicatori (KPI) come accessi non riusciti, avvisi di configurazioni errate e aggiornamenti di sicurezza mancanti, anche con un semplice cruscotto di monitoraggio.
- **Feedback:** Registra gli incidenti di sicurezza, indicando cosa è successo, le cause, l'impatto e le misure adottate. Usa quanto appreso per migliorare le fasi 1 e 2.

**Risultato:** Controlli verificati, risultati dei KPI, azioni correttive e insegnamenti per il ciclo CSI successivo.

## 4. Esempio pratico

### Impresa fittizia: NordicCraft Handicrafts

NordicCraft è una PMI di commercio elettronico con 25 dipendenti che vende prodotti artigianali online.

L'esempio mostra come applicare le cinque fasi del modello CSI. Dati e risultati hanno valore puramente illustrativo.

#### Fase 1 – Analisi: Inventario cloud e valutazione dei rischi

| Servizio cloud    | Modello di servizio  | Utilizzo nell'impresa                                                              |
|-------------------|----------------------|------------------------------------------------------------------------------------|
| Shopify           | SaaS                 | Negozio online, ordini, dati personali dei clienti e inoltro dei pagamenti.        |
| Google Workspace  | SaaS                 | Email aziendale, file condivisi e calendari.                                       |
| AWS S3            | IaaS / Archiviazione | Foto dei prodotti e backup giornalieri dei dati sugli ordini.                      |
| Azure App Service | PaaS                 | Applicazione web personalizzata per gli ordini, integrata con Shopify e magazzino. |

#### Risultati di CSI Matrix (estratto):

| Servizio               | Minaccia                                                       | Vulnerabilità                                         | Rischio                                              | Priorità |
|------------------------|----------------------------------------------------------------|-------------------------------------------------------|------------------------------------------------------|----------|
| Pannello admin Shopify | Furto di account / phishing                                    | MFA assente per gli amministratori.                   | Modifiche non autorizzate, fuga di dati dei clienti. | Alta     |
| AWS S3                 | Esposizione dei dati                                           | Il bucket S3 consente la lettura pubblica.            | Diffusione di immagini clienti e backup.             | Alta     |
| App ordini Azure       | Iniezione di codice / sfruttamento di vulnerabilità note (CVE) | Librerie obsolete, WAF assente.                       | Violazione dei dati, interruzione del servizio.      | Media    |
| Google Workspace       | Compromissione email aziendali                                 | Password deboli o riutilizzate, MFA non obbligatoria. | Perdita di dati, false richieste di pagamento.       | Media    |

### Verifica della conformità:

NordicCraft tratta dati personali dei clienti; pertanto si applica il GDPR.

L'impresa non rientra direttamente nell'ambito di DORA o NIS2, ma ha scelto di seguire volontariamente le buone pratiche della norma ISO/IEC 27001.

### Fase 2 – Definizione: Politica, priorità e ruoli

NordicCraft ha redatto una politica di sicurezza del cloud di una pagina, relativa all'accesso agli account, alla classificazione dei dati e ai backup.

Ha dato priorità immediata ai due rischi elevati: gli account amministratore di Shopify e l'accesso pubblico all'archivio AWS S3.

### Le responsabilità sono state assegnate così:

- **Amministratore cloud:** Responsabile IT – configura e gestisce tutte le piattaforme cloud.
- **Responsabile dei dati:** Responsabile operativo – definisce la classificazione dei dati dei clienti e le regole di accesso.
- **Responsabile della sicurezza:** Responsabile IT con il supporto di un partner IT esterno – monitora la sicurezza, gestisce gli incidenti e aggiorna la politica.
- **Responsabile della conformità:** Direttore generale – assicura la conformità al GDPR e l'allineamento alla ISO/IEC 27001.

### Fase 3 – Pianificazione: Misure di mitigazione dei rischi

| Rischio                              | Obiettivo di protezione                       | Contromisura                                                             | Responsabile       |
|--------------------------------------|-----------------------------------------------|--------------------------------------------------------------------------|--------------------|
| Sicurezza debole degli admin Shopify | Rafforzare la protezione degli account        | Rendere obbligatoria l'MFA per tutti gli amministratori Shopify.         | Responsabile IT    |
| Accesso pubblico ad AWS S3           | Limitare l'accesso ai soli permessi necessari | Rendere privato il bucket, applicare regole di accesso e attivare i log. | Responsabile IT    |
| Librerie obsolete dell'app Azure     | Ridurre la superficie d'attacco               | Aggiornare librerie, attivare Azure WAF e aggiornamenti automatici.      | Partner IT esterno |
| MFA assente in Google Workspace      | Rafforzare la protezione degli account        | MFA obbligatoria per tutti e avvisi di accesso.                          | Responsabile IT    |

### Documenti predisposti:

- Politica di sicurezza del cloud.
- Checklist di implementazione, con una riga per ogni misura.
- Modello per la gestione degli incidenti di sicurezza.
- Scheda di revisione dei log di audit (Audit Logs).

### Programma formativo:

Sono state previste due sessioni da 45 minuti basate sui materiali CSI:

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o di OeAD-GmbH. Né l'Unione europea né l'autorità concedente possono esserne ritenute responsabili.

Numero del progetto: 2024-1-AT01-KA220-VET-000245093.

- «MFA e corretta gestione delle password»
- «Riconoscere il phishing e segnalare gli incidenti»

#### Fase 4 – Attuazione: Interventi tecnici e formazione

NordicCraft ha svolto le seguenti attività:

- Ha reso obbligatoria l'MFA per tutti gli account amministratore Shopify e Google Workspace. La misura è stata completata nella prima settimana.
- Ha reso privato l'archivio AWS S3, applicando regole di accesso e attivando la registrazione degli accessi.
- Ha aggiornato le librerie di Azure App Service e attivato Azure WAF per proteggere l'applicazione di gestione ordini.
- Ha erogato entrambe le sessioni ai 25 dipendenti. Le presenze sono state registrate in un foglio di calcolo condiviso.

#### Fase 5 – Verifica: Test, monitoraggio e feedback

Un mese dopo l'implementazione, il partner IT esterno ha eseguito un test di phishing simulato e una scansione di base delle vulnerabilità dell'applicazione Azure.

È stato inoltre creato un semplice cruscotto KPI in un foglio di calcolo.

| Indicatore (KPI)                                     | Metodo di misurazione                                  | Soglia di allerta                               |
|------------------------------------------------------|--------------------------------------------------------|-------------------------------------------------|
| Tentativi di accesso falliti (tutte le piattaforme)  | Esportazione settimanale dalle console amministrative. | Oltre 10 tentativi per account a settimana.     |
| Account amministratore con MFA attiva (%)            | Controllo mensile delle impostazioni.                  | Meno del 100%.                                  |
| Giorni dall'ultimo aggiornamento o patch (app Azure) | Registro mensile degli aggiornamenti.                  | Oltre 30 giorni.                                |
| Incidenti di sicurezza aperti                        | Monitoraggio continuo.                                 | Qualsiasi incidente aperto da più di 14 giorni. |

È stato istituito un registro degli incidenti per documentare eventi, cause, conseguenze e contromisure adottate.

I risultati delle verifiche e le lezioni apprese vengono utilizzati per aggiornare CSI Matrix, le politiche, i controlli e la formazione.

L'impresa può così avviare un nuovo ciclo CSI dalla fase 1 e migliorare costantemente la propria sicurezza.

## 5. Checklist prima di iniziare

---

Prima di applicare il modello CSI per la prima volta, assicurati di aver:

- Individuato un referente per coordinare l'intero processo. Nelle imprese più piccole non serve un ruolo dedicato esclusivamente alla sicurezza.
- Riservato del tempo per completare l'autovalutazione CSI con il team e rilevare il livello iniziale di conoscenze.
- Preparato l'accesso a CSI Matrix per la valutazione dei rischi nella fase 1.
- Creato una cartella condivisa per la politica di sicurezza del cloud, le checklist e il registro degli incidenti.
- Impostato un promemoria periodico per ripetere la fase 1, ad esempio ogni 6–12 mesi o dopo modifiche importanti ai servizi cloud.

## 6. Risorse utili

---

Tutti gli strumenti citati nella guida sono disponibili su [gocloudsecure.eu](https://gocloudsecure.eu).

- [CSI Model](#): Documentazione completa delle cinque fasi del modello CSI.
- [CSI Matrix](#): Strumento interattivo per individuare e valutare minacce e rischi per la sicurezza del cloud.
- [CSI Self-Assessment](#): Strumento per valutare le conoscenze del team sulla sicurezza del cloud.
- [CSI Course-SecureCloud SME](#): Materiali formativi per sviluppare conoscenze e competenze pratiche sulla sicurezza del cloud.

### *Nota sulla guida*

*Questa guida è un documento integrativo non ufficiale, pensato per agevolare l'applicazione del modello CSI.*

*Non sostituisce la pubblicazione ufficiale «Go Cloud! Go Secure! — A Cloud Security Implementation Model for SMEs» (Erasmus+ 2024-1-AT01-KA220-VET-000245093), distribuita con licenza CC BY-NC-ND 4.0.*