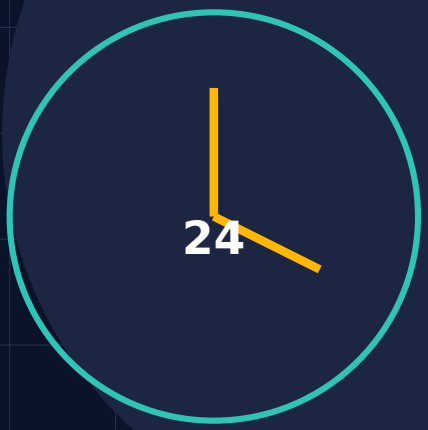
BLUE HARBOR EDITIONS



CYBER INCIDENT

LE PRIME 24 ORE

Piano d'emergenza per freelance
e piccole aziende

16 TEMPLATE | 20 CHECKLIST | 12 PLAYBOOK

0-15 MIN **1 ORA** **4 ORE** **24 ORE**

CONTENERE. DOCUMENTARE. RIPRISTINARE.

Decisioni chiare quando ogni minuto conta.

BLUE HARBOR STUDIO

EDIZIONE 2026 | CODICE BH-008 | AGGIORNATO AL 20 LUGLIO 2026

Cyber Incident: Le prime 24 ore

Piano d'emergenza per freelance e piccole aziende

Blue Harbor Editions - BH-008 - Edizione italiana 2026

VERSIONE E CONTROLLO

Versione 1.0. Fonti controllate il 20 luglio 2026. Canali, obblighi e interfacce dei fornitori cambiano: verifica sempre le fonti ufficiali e le condizioni applicabili al tuo caso.

Avvertenza importante

Questa guida è uno strumento educativo e organizzativo. Non sostituisce un servizio professionale di incident response, un avvocato, un DPO, un consulente del lavoro, un assicuratore, una banca, un provider o le autorità. Non certifica la conformità e non garantisce il recupero di dati o denaro.

Se esiste un rischio fisico immediato, chiama il 112. Se è coinvolto denaro, contatta subito la banca attraverso un numero ufficiale. Se l'attacco è attivo, usa un dispositivo e un canale che ritieni puliti per coordinare la risposta.

Copyright e licenza

Scheda d'emergenza: i primi 15 minuti

PRIMA REGOLA

Non improvvisare una pulizia. Contieni il danno, preserva le prove e registra ogni decisione.

[ ] Annota l'ora esatta in cui hai scoperto il problema e chi lo ha segnalato.

[ ] Sposta il coordinamento su un dispositivo e un canale non coinvolti nell'incidente.

[ ] Se un dispositivo è attivamente compromesso, scollegalo dalla rete senza cancellare file o log.

[ ] Se è coinvolto un pagamento, chiama immediatamente la banca e chiedi blocco o richiamo.

[ ] Nomina una persona responsabile e una persona che tenga il registro cronologico.

[ ] Acquisisci schermate, messaggi, orari, URL, mittenti e avvisi senza interagire con file sospetti.

[ ] Contatta il provider o un professionista di incident response dal canale pulito.

[ ] Non inviare comunicazioni pubbliche finché fatti e autorizzazioni non sono verificati.

NUMERI DA PREPARARE PRIMA

Provider IT o MSP - banca - assicurazione cyber - consulente legale/DPO - hosting/cloud - Polizia Postale - referente interno.

Come usare il manuale

Durante un incidente non si legge un libro dall'inizio alla fine. Si usa la timeline, poi il playbook specifico e infine i template. La priorità è prendere decisioni ripetibili con le informazioni disponibili, senza confondere velocità con fretta.

- Prima dell'incidente: compila contatti, ruoli, inventario essenziale e soglie di gravità.
- Nei primi 15 minuti: usa la Scheda d'emergenza e apri il Registro dell'incidente.
- Entro un'ora: identifica cosa è noto, cosa è ipotizzato e cosa deve essere verificato.
- Entro quattro ore: contiene identità, dispositivi, servizi e pagamenti secondo priorità.
- Entro 24 ore: avvia recupero controllato, valutazioni legali e comunicazioni autorizzate.
- Dopo l'incidente: trasforma ogni lezione in una modifica con responsabile e scadenza.

Profilo	Responsabile minimo	Supporto da attivare
Freelance	Titolare	Provider, banca, legale/DPO se necessario
Team 2-5	Incident lead + log keeper	MSP/fornitore e responsabile clienti
Piccola azienda	Lead + tecnico + comunicazioni	Direzione, DPO/legale, assicurazione
Attività regolata	Ruoli previsti dal piano	Autorità e consulenti secondo obblighi

Indice operativo