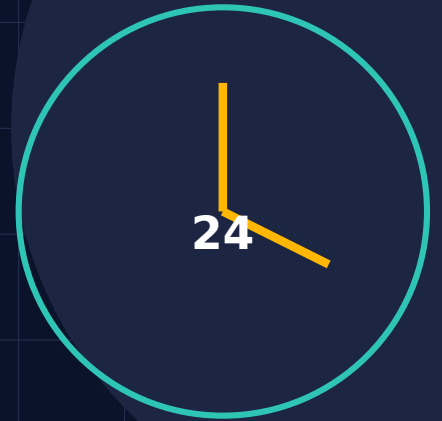


BLUE HARBOR EDITIONS

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.

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



BLUE HARBOR
STUDIO

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

Copyright © 2026 Blue Harbor Editions. Tutti i diritti riservati. L'acquirente può compilare e adattare i modelli per uso personale o interno alla propria attività. Non è consentito rivendere, distribuire o pubblicare parti sostanziali della guida senza autorizzazione scritta.

Scheda d'emergenza: i primi 15 minuti

PRIMA REGOLA

Non improvvisare una pulizia. Contieni il danno, conserva 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

Cyber Incident: Le prime 24 ore	2
Avvertenza importante	2
Copyright e licenza	2
Scheda d'emergenza: i primi 15 minuti	3
Come usare il manuale	4
Indice operativo	5
PRENDERE IL CONTROLLO	10
1. Evento, sospetto o incidente?	11
2. Le cinque priorità non negoziabili	12
3. Matrice di gravità S1-S4	13
4. Ruoli per team da una a dieci persone	14
5. Il canale pulito e la sala operativa minima	15
6. Contenere senza distruggere le prove	16
LA TIMELINE DELLE 24 ORE	17
7. Minuto 0-15: dichiarare e stabilizzare	18
Non fare	18
8. Minuto 15-60: definire il perimetro iniziale	19
9. Ora 1-2: contenere identità, dispositivi e pagamenti	20
Identità	20
Dispositivi e rete	20
Pagamenti	20
10. Ora 2-4: supporto, continuità e obblighi	21
11. Ora 4-8: verificare il contenimento	22
12. Ora 8-12: decidere comunicazioni e ripristino	23
13. Ora 12-24: recupero controllato e piano aperto	24
14. Chi contattare e in quale ordine	25
DODICI PLAYBOOK	26

15. Casella email compromessa	27
Segnali e conferme da cercare	27
Sequenza operativa	27
16. Ransomware o estorsione dati	28
Segnali e conferme da cercare	28
Sequenza operativa	28
17. Falso pagamento e business email compromise	29
Segnali e conferme da cercare	29
Sequenza operativa	29
18. Portatile o telefono perso o rubato	30
Segnali e conferme da cercare	30
Sequenza operativa	30
19. Malware o applicazione sospetta	31
Segnali e conferme da cercare	31
Sequenza operativa	31
20. Account cloud o amministratore compromesso	32
Segnali e conferme da cercare	32
Sequenza operativa	32
21. Sito web o e-commerce compromesso	33
Segnali e conferme da cercare	33
Sequenza operativa	33
22. Account social o pubblicitario rubato	34
Segnali e conferme da cercare	34
Sequenza operativa	34
23. Condivisione pubblica o invio errato di dati	35
Segnali e conferme da cercare	35
Sequenza operativa	35
24. DDoS, sito irraggiungibile o forte degrado	36
Segnali e conferme da cercare	36
Sequenza operativa	36
25. Incidente presso fornitore o SaaS	37
Segnali e conferme da cercare	37
Sequenza operativa	37
26. Accesso interno non autorizzato	38
Segnali e conferme da cercare	38
Sequenza operativa	38

RECUPERO, DATI E COMUNICAZIONI	39
27. Bonifica o ricostruzione?	40
28. Ordine di rotazione delle credenziali	41
29. Ripristinare backup senza reinfezione	42
30. Comunicare a staff, clienti e partner	43
31. Data breach e termine delle 72 ore	44
32. NIS, CSIRT, Polizia e assicurazione	45
33. Le prossime 72 ore, 7 giorni e 30 giorni	46
SEDICI TEMPLATE	47
Carta d'emergenza cyber	48
Matrice dei contatti verificati	49
Valutazione iniziale S1-S4	50
Registro cronologico dell'incidente	51
Mappa degli asset coinvolti	52
Inventario delle prove	53
Registro delle decisioni	54
Contenimento account e credenziali	55
Registro delle comunicazioni	56
Valutazione preliminare data breach	57
Preparazione notifica per fasi	58
Bozza di comunicazione a clienti o partner	59
Questionario urgente al fornitore	60
Scheda di validazione del ripristino	61
Post-incident review	62
Piano di rafforzamento in 30 giorni	63
Piano di 30 giorni - continuazione	64

CHECKLIST E RIFERIMENTI	65
20 checklist operative - gruppo 1	66
01 - Dichiarazione incidente	66
02 - Canale pulito	66
03 - Isolamento dispositivo	66
04 - Account email	66
05 - Ransomware	66
20 checklist operative - gruppo 2	67
06 - Pagamento fraudolento	67
07 - Dispositivo perso	67
08 - Cloud/admin	67
09 - Sito/e-commerce	67
10 - Social/advertising	67
20 checklist operative - gruppo 3	68
11 - Data leak	68
12 - Fornitore	68
13 - Evidenze	68
14 - Data breach	68
15 - Comunicazioni	68
20 checklist operative - gruppo 4	69
16 - Rotazione segreti	69
17 - Ripristino backup	69
18 - Rientro produzione	69
19 - Monitoraggio	69
20 - Chiusura incidente	69
Domande frequenti	70
Devo spegnere il computer?	70
Posso cambiare subito tutte le password?	70
Se non vedo file cifrati non è ransomware?	70
Devo pagare il riscatto?	70
Ogni incidente va notificato al Garante?	70
Le 72 ore partono dall'attacco?	70
CSIRT Italia sostituisce la denuncia?	70
Posso avvisare i clienti subito?	70
Quando posso chiudere l'incidente?	70
Come capisco se il fornitore ha risolto?	70
Glossario essenziale	71
Fonti ufficiali e aggiornamenti	72