Report tecnico di gestione incidente simulato

Modello didattico per esercitazione Day0 - Cyber Defence

Uso previsto: documento di lavoro per studenti ITS Cyber Defence. Serve a trasformare le scelte dello scenario in un report tecnico/formale comprensibile da direzione, IT interno, CDA e referenti di governance.

Nota: questo modello non e un modulo ufficiale di notifica verso ACN o altra autorita. E una traccia didattica per imparare a raccogliere e comunicare informazioni tecniche in modo ordinato.

Campo	Da compilare
Scenario	
Azienda simulata	
Gruppo / classe	
Componenti del gruppo	
Data esercitazione	
Versione report	

Regola d'oro: non scrivere solo cosa avete fatto. Scrivete perche lo avete fatto, quale evidenza lo supporta, cosa avete escluso e cosa non potete ancora affermare.

1. Istruzioni di compilazione

Compilate il report mentre svolgete lo scenario. Non aspettate la fine: in un incidente reale la qualita della documentazione dipende da cio che annotate durante le decisioni.

[ ]	Compilare dati generali, scenario e componenti del gruppo.
[ ]	Annotare ipotesi iniziale e ipotesi alternative.
[ ]	Registrare timeline, orari simulati, attese, escalation e decisioni.
[ ]	Riportare comandi/controlli e output rilevanti, distinguendo sano, sospetto e mancante.
[ ]	Separare fatti confermati, assunzioni e punti ancora incerti.
[ ]	Indicare impatto su disponibilita, integrita, riservatezza e operativita.
[ ]	Descrivere contenimento, recovery, monitoraggio e piano 7/30/90 giorni.
[ ]	Scrivere una comunicazione comprensibile per direzione/CDA, senza promesse non verificate.

2. Ruoli nel team

Assegnate ruoli prima di iniziare. Una buona risposta a incidente non e solo tecnica: serve coordinamento.

Ruolo	Nome/i	Responsabilita
Incident coordinator		Tiene il filo, decide priorita, gestisce tempi e passaggi.
Tecnico sistemi		Processi, servizi, utenti, filesystem, log locali.
Tecnico rete		Firewall, VPN, DNS, proxy, porte, segmentazione.
Responsabile evidenze		Annota output, log, anomalie, lacune, prove raccolte.
Comunicazione cliente		Scrive aggiornamenti per titolare, IT interno e management.

3. Executive summary per direzione / CDA

Scrivete questa sezione in linguaggio chiaro, non solo tecnico. Deve poter essere letta da un titolare o da un CDA.

Sintesi in massimo 10 righe: cosa e successo, quali sistemi sono coinvolti, impatto, stato contenimento, prossimi passi.

Domanda	Risposta sintetica
La situazione e contenuta?	
Il servizio e ripristinabile?	
Ci sono dati potenzialmente usciti?	
Quali decisioni servono alla direzione?	

4. Timeline degli eventi

La timeline deve distinguere eventi osservati, decisioni e prove. Usate orari simulati dello scenario o riferimenti T+ minuti.

Ora / T+	Evento osservato	Decisione presa	Evidenza

5. Ipotesi tecnica

Scrivete cosa pensate sia successo. Aggiornate l'ipotesi quando nuove evidenze la confermano o la indeboliscono.

Ipotesi principale

Ipotesi alternative considerate

Elemento	A favore dell'ipotesi	Contro / dubbio

6. Evidenze tecniche raccolte

Riportate comandi, controlli e output significativi. Non basta copiare: interpretate cio che vedete.

Area	Comando / controllo	Output rilevante	Interpretazione

6.1 Evidenze - continuazione

Usate questa pagina per ulteriori log, output, screenshot descritti o verifiche non ancora concluse.

Area	Comando / controllo	Output rilevante	Interpretazione / lacuna

7. Valutazione impatto

Valutate separatamente disponibilita, integrita e riservatezza. Un servizio funzionante non prova che il rischio sia chiuso.

Dimensione	Impatto rilevato / stimato	Evidenza / motivazione
Disponibilita		
Integrita		
Riservatezza		
Operativita business		
Reputazione / clienti		

Stima sintetica dell'impatto complessivo

8. Decisioni prese e motivazioni

Ogni decisione deve spiegare rischio ridotto e rischio introdotto. In un incidente reale anche non decidere e una decisione.

Decisione	Motivazione	Rischio ridotto	Rischio introdotto

9. Contenimento

Descrivete cosa e stato isolato, bloccato, limitato o mantenuto attivo con rischio accettato.

Azioni di contenimento eseguite

Azioni di contenimento NON eseguite e motivazione

10. Recovery e ripristino

Non promettete ripristino senza test. Indicate backup, restore test, RTO/RPO e condizioni minime di riapertura.

Elemento	Stato / risultato	Note / rischio
Backup disponibile		
Restore test		
RTO stimato		
RPO stimato		
Condizioni per riapertura		

11. Rischio residuo

Elencate i rischi ancora aperti. Un rischio puo essere accettato solo se e esplicito, documentato e comunicato.

Rischio residuo	Probabilita	Impatto	Azione proposta

12. Comunicazione a direzione / CDA

Scrivete una comunicazione in linguaggio non tecnico ma precisa. Evitate frasi assolute non dimostrate.

Bozza comunicazione per direzione / CDA

13. Informazioni utili per eventuale escalation istituzionale

Sezione didattica ACN/NIS2-style: non e un modulo ufficiale. Serve a capire quali informazioni tecniche devono essere pronte.

Informazione	Dato disponibile / da verificare
Data e ora rilevazione	
Servizi / sistemi impattati	
Impatto su disponibilita, integrita, riservatezza	
Misure di contenimento adottate	
Stato attuale incidente	
Referente tecnico	

14. Piano di azione 24/72 ore

Azioni immediate per stabilizzare, osservare e ridurre il rischio residuo.

Quando	Azione	Responsabile	Esito atteso

15. Piano 7/30/90 giorni

Azioni strutturali per evitare che il problema si ripresenti.

Orizzonte	Azioni consigliate
7 giorni	
30 giorni	
90 giorni	

16. Conclusioni e raccomandazione tecnica

Chiudete il report distinguendo stato finale, rischio residuo e decisioni richieste al management.

Conclusione tecnica

Raccomandazione al management / titolare

Campo	Compilazione
Report redatto da	
Data / ora	
Firma / gruppo	

Checklist finale: il report contiene ipotesi, timeline, evidenze, impatto, decisioni, contenimento, recovery, rischio residuo, comunicazione e piano 24/72 - 7/30/90 giorni.