SECURITY LAB
sicurezza on line

Protocollo Rapido di Gestione Incidenti (PRGI)

Fase 1: Rilevamento e Analisi (Primi 60 minuti)

Non appena viene segnalata un'anomalia (es. file criptati, email sospette inviate in massa, accesso negato agli amministratori):

- **Isolamento immediato:** Se un PC è sospetto, stacca il cavo di rete o disattiva il Wi-Fi. **NON spegnere la macchina** (per non cancellare tracce volatili nella RAM utili all'analisi).
- **Verifica la portata:** È colpita una sola postazione o l'intero server?
- **Registro eventi:** Segna l'ora esatta della scoperta e chi ha dato l'allarme.

Fase 2: Comunicazione e Escalation (Entro le prime 4 ore)

In base alle nuove norme, il tempo è il tuo peggior nemico:

- **Avvisa il Team IT/Security:** Attiva il partner tecnologico (es. SecurityLab) per l'analisi forense.
- **Coinvolgi il DPO (Data Protection Officer):** Valuta se sono stati esposti dati personali (obbligo GDPR).
- **Pre-notifica ACN/Garante:** Se l'attacco è grave, prepara la segnalazione preliminare. **Hai solo 24 ore** per la Cybersecurity Nazionale e **72 ore** per il Garante Privacy.

Fase 3: Contenimento e Eradicazione (Entro le 12-24 ore)

- **Reset Credenziali:** Cambia tutte le password amministrative (Domain Admin, Cloud, Backup).
- **Chiusura vulnerabilità:** Identifica da dove sono entrati (es. una VPN senza MFA o un server non patchato) e chiudi l'accesso.
- **Bonifica:** Scansiona l'intera rete alla ricerca di "backdoor" lasciate dagli hacker per rientrare in futuro.

Fase 4: Ripristino e Post-Incidente (Dopo la bonifica)

- **Ripristino da Backup:** Solo dopo essere certi che la rete è pulita, procedi al restore dei dati.
- **Monitoraggio Rafforzato:** Per i successivi 15 giorni, osserva i log in modo maniacale per escludere recidive.
- **Report Finale:** Documenta tutto ciò che è successo. Questo documento ti servirà per dimostrare alle autorità che hai agito con "Accountability".

SECURITY LAB
sicurezza on line

📝 Tabella di Emergenza: Chi chiamare?

Ruolo	Nome/Azienda	Contatto Rapido
Responsabile IT	[Inserire Nome]	[Inserire Cellulare]
Partner Cybersecurity	**SecurityLab.Service**	[Inserire Numero Emergenza]
Consulente Legale/DPO	[Inserire Nome]	[Inserire Email/Tel]
Provider Cloud/Mail	[Es. Microsoft/Google]	[Link Portale Supporto]