

*La Sicurezza Informatica e delle Telecomunicazioni
(ICT Security)*

*VALUTAZIONE DEL LIVELLO DI SICUREZZA
Auto Valutazione*

Allegato 1

gennaio 2002

Note sul questionario di Auto – diagnosi

- Il questionario ha lo scopo di guidare l'Amministrazione nel processo di auto-valutazione del proprio livello di sicurezza, rispetto alla base minima raccomandata.
- I risultati dell'auto-valutazione sono *proprietà riservata* dell'Amministrazione, la quale é libera di decidere come utilizzarli.
- Il questionario é stato impostato al fine di consentire un processo operativo affidabile e rapido

A tale scopo sono state definite sei schede, una per ciascuna delle aree chiave della sicurezza: Policy, Ruoli e Responsabilità, Norme e Procedure, Amministrazione della Sicurezza, Analisi del Rischio, Formazione e Sensibilizzazione.

Ogni scheda comprende una lista di modalità operative, una guida alle domande che dovrebbero essere poste e un insieme di possibili risposte (1,2,3,4) nell'ambito delle quali ci dovrebbe essere quella maggiormente coerente con la situazione riscontrata.

- Valutare la scheda comporta semplicemente selezionare una delle 4 possibili risposte predefinite su ciascuna delle 6 schede.

Policy della Sicurezza

Obiettivo: Ci dovrebbe essere una appropriata Policy di sicurezza informatica

Tick	Passi suggeriti	Commenti
<input type="checkbox"/>	Ottenere e valutare il documento di policy	
<input type="checkbox"/>	Intervistare alcuni responsabili per verificare l'adeguatezza della policy per supportare la sicurezza	
<input type="checkbox"/>	Considerare la rilevanza della policy per l'attività dell'Amministrazione	

Tick	Considerazioni di valutazione	Commenti
<input type="checkbox"/>	La policy indirizza sia la sicurezza informatica che quella informativa ?	
<input type="checkbox"/>	Fornisce una base per gli obiettivi di sicurezza e di continuità ?	
<input type="checkbox"/>	Fornisce una base sufficiente per realizzare la sicurezza ?	
<input type="checkbox"/>	Fornisce una base sufficiente per misurare la coerenza della sicurezza alla policy ?	
<input type="checkbox"/>	L'amministrazione supporta adeguatamente il rispetto delle policy ?	

Val.	Conclusioni	Commenti
<input type="checkbox"/>	1. La policy è formalizzata e completa	
<input type="checkbox"/>	2. La policy esiste e può essere migliorata	
<input type="checkbox"/>	3. La sicurezza è solo parzialmente e indirettamente indirizzata dalla policy	
<input type="checkbox"/>	4. Non esiste alcuna policy	

Tick: apporre l'indicazione (✓) di effettuazione del passo suggerito e del tipo di considerazione

Val.: apporre la cifra (1, 2, 3 o 4) corrispondente al rating valutato più opportuno

Ruoli e Responsabilità

Obiettivo: Le Responsabilità della sicurezza informatica dovrebbero essere formalmente descritti ed efficacemente implementati

Tick	Passi suggeriti	Commenti
<input type="checkbox"/>	Intervistare i ruoli utente sulla loro consapevolezza circa le responsabilità della sicurezza in azienda	
<input type="checkbox"/>	Rivedere le job description per verificare la presenza di specifiche responsabilità sulla sicurezza	
<input type="checkbox"/>	Verificare la documentazione relativa ad analisi del rischio, a classificazioni e ad autorizzazioni per valutare le responsabilità esercitate	

Tick	Considerazioni di valutazione	Commenti
<input type="checkbox"/>	I Proprietari richiedono/sviluppano analisi del rischio e classificazioni delle risorse ?	
<input type="checkbox"/>	Autorizzano chiaramente i privilegi di accesso ai dati ?	
<input type="checkbox"/>	Hanno la responsabilità sulla sicurezza chiaramente specificata ?	
<input type="checkbox"/>	Autorizzano gli investimenti in sicurezza ?	

Val.	Conclusioni	Commenti
<input type="checkbox"/>	1. Le responsabilità sulla sic.zza sembrano essere specificate e suff.nte implementate	
<input type="checkbox"/>	2. Le responsabilità non sono documentate ma sembrano essere ragionevolmente applicate in pratica	
<input type="checkbox"/>	3. Le responsabilità sono documentate ma sembrano inefficaci	
<input type="checkbox"/>	4. Le responsabilità non esistono	

Tick: apporre l'indicazione (✓) di effettuazione del passo suggerito e del tipo di considerazione

Val.: apporre la cifra (1, 2, 3 o 4) corrispondente al rating valutato più opportuno

Norme e Procedure

Obiettivo: Un insieme organico di norme e procedure dovrebbe fornire una guida efficace all'utilizzo e allo sviluppo sicuro del sistema ICT

Tick	Passi suggeriti	Commenti
<input type="checkbox"/>	Ottenere informazioni e documenti sulle metodologie di sviluppo e gestione dei sistemi informatici	
<input type="checkbox"/>	Valutare la completezza degli standard di sicurezza informatica	
<input type="checkbox"/>	Valutare l'esistenza, l'utilizzo, il rispetto e l'adeguatezza delle norme di sicurezza	

Tick	Considerazioni di valutazione	Commenti
<input type="checkbox"/>	Gli standard e le procedure di IT considerano le implicazioni di sicurezza ?	
<input type="checkbox"/>	Gli standard e le procedure e le norme di sicurezza sono aggiornate ?	
<input type="checkbox"/>	Le risorse sono classificate in base alla loro sensitività ?	
<input type="checkbox"/>	La sicurezza informatica è considerata in tutte le fasi del ciclo di vita delle applicazioni ?	

Val.	Conclusioni	Commenti
<input type="checkbox"/>	1. Norme e procedure sono formalizzate e sembrano essere complete e attuali	
<input type="checkbox"/>	2. Esistono ma devono essere significativamente migliorate	
<input type="checkbox"/>	3. Esistono ma a livello informale o non documentate	
<input type="checkbox"/>	4. Non esistono	

Tick: apporre l'indicazione (✓) di effettuazione del passo suggerito e del tipo di considerazione

Val.: apporre la cifra (1, 2, 3 o 4) corrispondente al rating valutato più opportuno

Amministrazione della Sicurezza

Obiettivo: L'Organizzazione della Funzione Sicurezza Informatica dovrebbe avere un adeguato numero di *Professionalità* con il compito di amministrare la sicurezza informatica

Tick	Passi suggeriti	Commenti
<input type="checkbox"/>	Intervistare gli amministratori della sicurezza: funzioni, background, attività, ecc....	
<input type="checkbox"/>	Valutare la copertura delle posizioni rispetto a quantità e qualità	
<input type="checkbox"/>	Valutare la coerenza delle attività svolte rispetto alla missione	
<input type="checkbox"/>	Valutare i ruoli aziendali coinvolti e l'interazione tra di essi	

Tick	Considerazioni di valutazione	Commenti
<input type="checkbox"/>	Sono individuati chiaramente i ruoli interni/esterni (utenti) e le relazioni tra i due ?	
<input type="checkbox"/>	Esistono regole chiare e conosciute sulla richiesta, modifica, attivazione ed estinzione delle abilitazioni ?	
<input type="checkbox"/>	Esistono e sono implementati adeguati strumenti per la configurazione centralizzata delle utenze/privilegi ?	
<input type="checkbox"/>	Esistono e sono configurati sistemi di controllo accessi alle risorse ?	
<input type="checkbox"/>	Esistono e sono aggiornati sistemi di gestione antivirus	
<input type="checkbox"/>	Esistono e sono operativi sistemi di gestione del back-up e recovery	
<input type="checkbox"/>	Esistono e sono operative strutture di gestione degli incidenti (gruppi di risposta)	

Val.	Conclusioni	Commenti
<input type="checkbox"/>	1. L'amministrazione della sicurezza risulta ben presidiata e operativamente efficiente	
<input type="checkbox"/>	2. L'amministr.ne è impropriamente presidiata ma appare essere oper.ente efficiente	
<input type="checkbox"/>	3. Le responsabilità sono assegnate ma la funzione è solo parzialmente efficiente	
<input type="checkbox"/>	4. L'amministrazione è inefficiente	

Tick: apporre l'indicazione (✓) di effettuazione del passo suggerito e del tipo di considerazione

Val.: apporre la cifra (1, 2, 3 o 4) corrispondente al rating valutato più opportuno

Analisi del Rischio

Obiettivo: Ci dovrebbe essere un efficace e tempestiva analisi delle minacce potenziali e del loro impatto sulla sicurezza delle informazioni critiche

Tick	Passi suggeriti	Commenti
<input type="checkbox"/>	Identificare e rivedere le analisi del rischio più recenti	
<input type="checkbox"/>	Considerare il livello e l'impatto dei rischi individuali	
<input type="checkbox"/>	Discutere le procedure di analisi e valutazione del rischio utilizzate	
<input type="checkbox"/>	Valutare i piani d'azione generati dall'analisi	

Tick	Considerazioni di valutazione	Commenti
<input type="checkbox"/>	L'analisi del rischio copre tutte le risorse informatiche ?	
<input type="checkbox"/>	L'analisi considera tutte le minacce ragionevolmente probabili ?	
<input type="checkbox"/>	Il personale della sicurezza informatica e i Referenti applicativi sono coinvolti ?	
<input type="checkbox"/>	Sono stimati gli impatti sul business ?	
<input type="checkbox"/>	Sono valutati i costi/benefici delle contromisure suggerite ?	
<input type="checkbox"/>	E' valutata la riduzione di rischio conseguente ?	

Val.	Conclusioni	Commenti
<input type="checkbox"/>	1. Le analisi del rischio sono periodicamente eseguite	
<input type="checkbox"/>	2. Le analisi del rischio sono eseguite ma sono superate ed hanno un obiettivo ristretto	
<input type="checkbox"/>	3. Il rischio è stato informalmente considerato	
<input type="checkbox"/>	4. Non c'è analisi del rischio	

Tick: apporre l'indicazione (✓) di effettuazione del passo suggerito e del tipo di considerazione

Val.: apporre la cifra (1, 2, 3 o 4) corrispondente al rating valutato più opportuno

Sensibilizzazione e Formazione

Obiettivo: Consapevolezza e sensibilizzazione sulla sicurezza dovrebbero essere sviluppati attraverso efficaci programmi di formazione a tutti i livelli dell'Organizzazione

Tick	Passi suggeriti	Commenti
<input type="checkbox"/>	Intervistare alcuni Responsabili per determinare se viene fornito uno specifico training sulla sicurezza	
<input type="checkbox"/>	Rivedere il materiale di training	
<input type="checkbox"/>	Rivedere i programmi e le procedure di formazione	

Tick	Considerazioni di valutazione	Commenti
<input type="checkbox"/>	E' richiesto al personale di firmare un accordo di riservatezza sulle informazioni ?	
<input type="checkbox"/>	Il personale riceve periodicamente un bollettino sulla sicurezza o altro materiale ?	
<input type="checkbox"/>	Esistono programmi di sensibilizzazione e formazione ?	
<input type="checkbox"/>	La consapevolezza sulla sicurezza sembra ragionevolmente diffusa ?	

Val.	Conclusioni	Commenti
<input type="checkbox"/>	1. Sono impiegati programmi di sensibilizzazione e formazione	
<input type="checkbox"/>	2. Il materiale disponibile può essere sensibilmente migliorato	
<input type="checkbox"/>	3. Non c'è un programma di training ma esiste una certa consapevolezza	
<input type="checkbox"/>	4. Non esiste consapevolezza	

Tick: apporre l'indicazione (✓) di effettuazione del passo suggerito e del tipo di considerazione

Val.: apporre la cifra (1, 2, 3 o 4) corrispondente al rating valutato più opportuno

Quadro di Valutazione

Esempio

SECURITY MANAGEMENT	CONCLUSIONI			
	Adeguato ←			→ Non adeguato
1. POLICY	1	2	3	4
2. RUOLI/RESPONSABILITA'	1	2	3	4
3. NORME/PROCEDURE	1	2	3	4
4. AMMINISTRAZIONE	1	2	3	4
5. ANALISI DEL RISCHIO	1	2	3	4
6. SENSIBILIZZAZIONE E FORMAZIONE	1	2	3	4