

## INFORMAZIONI AGGIUNTIVE QUESTIONARIO CYBER RISKS SOGEI SPA

- **Sezione 1 -MFA:** non si richiede la multi factor authentication per tutti gli accessi da remoto (molti mercati utilizzano questo step all'entrata per la valutazione di qualunque rischio); **E' un errore visto che per tutti gli accessi c'è la MFA.**
- **Sezione 2 - EDR:** bassa la percentuale di device mobili su cui vi sono gli antimalware e che siano regolarmente patchati; possiamo a tal proposito fornire dettagli in merito a qualche remediation alternativa? Vi è in progetto un maggior controllo dei device stessi? **C'è un progetto di utilizzo del MAM entro luglio 2024.**
- **Sezione 4 - PAM:** mancanza di un PAM. Inoltre nella sezione opzionale "External partner accompaniments" non sono quantificati il numero di service account e i loro privilegi amministrativi. Inseriamo in allegato una definizione per meglio chiarire il tema. È possibile avere un approfondimento in tal senso? Sarebbe ottimale il completamento della tabella excel che inseriamo in allegato per dare un quadro completo del tema ai mercati. **Il PAM è una soluzione standard utilizzata su 11.000 server. Ulteriori informazione nella tabella Excel "Service account".**
- **Sezione 8- Cyber security awareness:** non vi è obbligatorietà nei corsi di formazione per i dipendenti; questo sarà sicuramente un punto critico nell'interrogazione dei mercati. Avete in pipeline un cambiamento in tal senso? **Abbiamo in programma di erogare un corso di cyber security awareness nei prossimi mesi (anche se non abbiamo ancora un contratto ma materiale sì), però l'obbligatorietà non deriva da una scelta nostra ma da un mandato di HR. Essendo ora la stessa direzione generale potremmo impegnarci in tal senso. In ambito sicurezza e continuità operativa nel corso del 2022 sono state erogate complessivamente 989 gg di formazione mentre nel 2023 le giornate sono state 1137. Al momento non è previsto un obbligo ma di sicuro la sicurezza è un tema all'attenzione e credo i numeri indicati ne siano una evidenza incontrovertibile.**
- **Sezione 11 - Sistemi End of life:** la mancata segregazione dei sistemi end of life è un altro tema rilevante. Anche in questo caso sarebbe necessario argomentare maggiormente in merito. **Per i sistemi in EOL abbiamo creato due nuovi ambienti denominati blue e green in cui spostiamo le applicazioni sanando le obsolescenze: nell'area blu ci vanno le applicazioni su sistemi non obsolete il cui porting non necessita di re-engineering, nell'area green ci vanno le nuove applicazioni o quelle ingegnerizzate ex-novo.**