ANNESSO A – CHECK-LIST ATTIVITA' ART. 34/35 Reg.2916/679/UE

Periodo di riferimento: ***Gen-Giu 2018***
a cura di ADS/DBA e RDT ext secondo nomine e designazioni del TDT

Doc. di riferimento: RO-3201, DB-PG679, IO-DB01, RV-DB01

- Assegnato vari ruoli e accessi nella Active directory, quindi le persone sono state limitate ad accedere a particolari cartelle e documenti. Il supervisore Privacy @Sara Borelli detiene copia del documento completo dove è specificata la toponomastica dei diritti e dei gradi di accesso risorse LAN

- Sistemato armadio tecnico liberando lo spazio e ottimizzando la disposizione delle apparecchiature. In accordo alle nuove policies di DP/679, tutti i dispositivi non identificabili, non attribuibili ad alcuna funzione/ utilizzo sono stati rimossi. Dove la rimozione fisica non è stata valutata praticabile e/o sostenibile, gli apparati sono stati isolati dalla alimentazione elettrica.

- La chiave dell'armadio è stata rimossa e consegnata secondo ruolo di responsabilità e/o custodia indicato nelle politiche di Sicurezza Informatiche del Disciplinare Interno della Azienda.

- Una nuova postazione NAS è stata installata in aggiunta agli apparati ICT nei *racks* dell'armadio tecnico. Successivamente al Setup dell'alloggiamento fisico si sono intraprese le sessioni di configurazione che
    - centralizzano nel SysOP embedded del dispositivo la gestione del Server sysLOG,
    - replicano alberature logiche degli Shared Folders della LAN
    - lanciano gli automatismi di *backup* e stoccaggio dati (sia immagini che repertori files)
    - lanciano gli automastismi di replica FTPS su area Cloud

- Abbiamo inserito un UPS nell'armadio (e al momento stiamo cercando le batterie in modo da sostituirle e mettere in funzione il dispositivo)

- Un nuovo Firewall viene montato nell'armadio tecnico. Il modello della ZyXel USG-60 è stato acquistato sulla base del dimensionamento di due flussi di connettività bilanciati. Dal lato WAN è stata attuata una toponomastica di sezionamenti coerente con le politiche di Sicurezza adottate in ambito ICT. A sua volta le segregazioni in classe C/IPV4 della LAN seguono le divisioni di ruolo/funzioni aziendali delle diverse categorie di trattamenti dei Soggetti Autorizzati secondo nomine/designazioni e/o deleghe del TDT.

- Un precedente apparato NAS in simmetria Mirror, presente nell'armadio tecnico ma non più identificabile, viene formattato secondo Secure Erasure Procedure (HD wiping). Il proposito è quello di un riutilizzo come unità di storage cifrato addizionale esterno (firewire/eSATA) del nuovo apparato NAS.

- Tutte le password/chiavi del network Wi-Fi sono state registrate dagli ADS e protette a mezzo sistema di VAULT digitale. Il sistema credenziali è distinto per ogni punto di accesso (incluso *dongle*-USB se utilizzati). Architetturalmente, una copertura di rete WI-FI distinta è stata implementata per gli ospiti/visitatori. A meno di incidenti di violazione informatica, le credenziali di tutti gli apparati WI-FI sono modificate/aggiornate e pertanto ri-registrate e ri-conservate con frequenza semestrale. Le prassi/procedure necessarie a questi adempimenti sono formalizzate nel Disciplinare Tecnico dell'azienda.

- È stato formattato un addizionale Server quale misura di sicurezza nel caso di un Backup di Dominio (DNS/LAN ed eventualmente stazione di test/sviluppo prodotto.

- Tutti i dispositivi obsoleti, come ad esempio una unità di lettura cassette, sono stati rimossi e regolarmente smaltiti dopo le procedure di Secure Erasure in accordo allo standard NIST.

- I ripetitori WI-FI di locali adiacenti alle aree del sito produttivo R&S, sono stati classificati e integrati alla rete LAN con separato sezionamento di masking. Anche queste credenziali sono mantenute e conosciute agli ADS e al TDT.

- In merito all’apparato VOIP aziendale, il controllo alla IDE/WEB della console di configurazione deve essere revisionata con il gestore TIM. Più precisamente si deve definire se contrattualmente il Provider incumbent ha la proprietà e quindi il totale controllo sul dispositivo **Cisco**. La nostra azienda potrebbe negoziare, se del caso, per una formula di sola connettività e in questo caso sarà considerato l’acquisto di un proprio HW VOIP. Più di tutto però va chiarito se, in caso di conferma del controllo TIM, questa dovrà sottoscrivere un documento di SLA/PLA, ovvero recepire la nomina di Responsabile Esterno del Trattamento.