1. **Aspetti inerenti le comunicazioni e la sicurezza**
2. **Comunicazioni “non classificate”**

L’attuale dislocazione del **CDO** di **MIASIT** all’interno di una struttura alberghiera a **TRI** e l’attuale configurazione della maglia C4I di **MIS** non consentono di rispettare i corretti canoni di “sicurezza fisica” e ha indotto la Missione a utilizzare sistemi di rete “non classificati” e *network* commerciali locali, senza possibilità di poter disporre di sistemi di telefonia di forza armata (tipo SOTRIN). Il riferimento per le misure di sicurezza delle informazioni da applicare e per l’utilizzo consapevole delle postazioni e dei servizi *internet* a disposizione del contingente **ITA** sono contenute nella [**DP 14-2021**](CARTELLA%208/DP%2014-2021%20Misure%20di%20sicurezza%20delle%20informzazioni%20(25.04.2021)/20210425%20-%20DP_14-2021_SICUREZZA_DELLE_INFORMAZIONI_protocollata.pdf). Le principali comunicazioni con i Comandi di vertice per entrambi i contingenti, quindi, avvengono attraverso sistemi “non classificati” tramite apposita piattaforma “virtual.difesa”, da cui è possibile accedere ai servizi “webmail” (gestione delle *email* funzionali), “citrix” (gestione intranet/skype/archiviazione documenti/pacchetto *office*) e “webex” (gestione **VTC**). In particolare:

* l’accesso a “virtual.difesa” avviene attraverso criteri con riconoscimento a doppio fattore (*password* statica e *password* dinamica fornita da *token*);
  + Per **TRI**: con indirizzi del tipo “[nome.cognome@smdnc.difesa.dom](mailto:nome.cognome@smdnc.difesa.dom)”, con annessa *email* funzionale (es.: [miasit.com@smd.difesa.it](mailto:miasit.com@smd.difesa.it), [miasit.ma@smd.difesa.it](mailto:miasit.ma@smd.difesa.it),) e con criteri di accesso a doppio fattore di autenticazione (gli stessi utilizzati per l’accesso alla piattaforma “virtual.difesa”);

La gestione e archiviazione dei dati non classificati avviene tramite *Local Area Network* (**LAN**) attivata a partire dal secondo semestre del 2020, su un’unità di rete *Network Attached Storage* (**NAS**), accessibile da tutte le postazioni con criteri differenziati in base alla funzione/incarico dell’utente. Parallelamente è disponibile un sistema di *backup* giornaliero su altri archivi di massa.

Le sedi di **TRI** e **MIS** hanno un sistema di protocollo e gestione documentale **ADHOC** collegato alla casella di PEC dell’Area Organizzazitva Omogenea (**AOO**) “TF IPPOCRATE”[[1]](#footnote-1) ([Annesso **6.c.1**](CARTELLA%206/ANN%206.c.1%20Richiesta%20di%20attivazione%20sistema%20@DhOC%20(13.05.2020).pdf)). La gestione della piattaforma **ADHOC** avviene, su postazione dedicata, tramite *Virtual Private Network* (**VPN**) assegnata dal **CDO** C4I dell’**EI**, su specifica richiesta.

Sono inoltre attivate le comunicazioni GSM attraverso l’impiego di telefoni cellulari (consegnati a tutte le figure chiave degli *staff* e registrati presso uno specifico registro in cura alle rispettive cellule **J6**) tramite l’utilizzo di SIM CARD ricaricabili dell’operatore locale “ALMADAAN”.

**(2) Comunicazioni “classificate”**

La gestione dei flussi documentali classificati avviene, allo stato attuale, unicamente attraverso la Nave della **MM** in supporto a **OMS**, ormeggiata presso il porto militare di **TRI** (Abu Sittah), che rappresenta il Punto Controllodella Missione. Infatti a causa del *retrograde* della **TF-I** a **MIS**, a partire dal 05.08.2022, sono cessati i servizi classificati a **MIS** che erano di supporto anche per lo *staff* di **TRI**. Attualmente **MIS** dispone di una postazione con *Personal Computer* (**PC**) “*stand alone* R” per trattare documenti con classifica fino a livello “riservato”. Mentre, per inviare i documenti tramite *email*, è impiegato il sistema *Enciphering Deciphering Code* (**EDC**) che utilizza un algoritmo di cifratura per criptare i file e inviarli tramite *email* funzionale con un **PC** non classificato “UNCLASS”. Nel futuro, si prevede che il **CDO MIASIT** presso Hotel **SULTAN** abbia idonee strutture e spazi che rispettino i canoni di “sicurezza fisica” e possa quindi implementare reti/servizi classificati canonici*.* Attualmente le comunicazioni sicure possono essere effettuate attraverso la telefonia GSM con comunicazioni criptate (fino a RISERVATO -NATO RESTRICTED): a **TRI** con cellulare SAMSUNG GT-19300 (n.tel: +39 335-7375960) – oggetto di **P/C** tra titolari ([Annesso **6.c.2**](CARTELLA%206/ANN%206.c.2%20Ricevuta%20Assegnazione%20Cellulare%20Sicuro%20(14.08.2022).pdf)) – e a **MIS** con cellulare SAMSUNG GT-19300 (n.tel: +39 335-1205299).

1. La richiesta **MIASIT** di attivazione di una nuova **AOO** in data 07.05.2020 non ha avuto seguito esecutivo. [↑](#footnote-ref-1)