AERONAUTICA MILITARE
COMANDO LOGISTICO

Direttiva per la gestione dell'accesso al servizio Internet in Aeronautica Militare

CL-3DV-017

BASE 21 LUGLIO 2014

PAGINA NON SCRITTA

AERONAUTICA MILITARE
COMANDO LOGISTICO

INDICE

ALLEGATI:

ELENCO DI DISTRIBUZIONE

PAGINA NON SCRITTA

V

AERONAUTICA MILITARE
COMANDO LOGISTICO

ATTO DI APPROVAZIONE

Approvo la "**Direttiva per la gestione dell'accesso al servizio Internet in Aeronautica Militare**" CLA-NL-3320-0002-00B00 (CL-3DV-017) BASE 21 LUGLIO 2014.

Roma, **08 LUG 2014**

IL COMANDANTE LOGISTICO
(Gen. S.A. Gabriele SALVESTRONI)

PAGINA NON SCRITTA

ELENCO DELLE AGGIUNTE E VARIANTI

PAGINA NON SCRITTA

RIFERIMENTI

- Legge n. 547 del 23 dicembre 1993, che modifica il Codice Penale introducendo i crimini informatici.
- Legge n. 675 del 31 dicembre 1996 “Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali”.
- D.P.R. 28 dicembre 2000, n. 445 “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”.
- Direttiva Difenet “Requisito Tecnico-Operativo per lo sviluppo, l’adeguamento e l’interconnessione delle reti Intranet per la trattazione delle informazioni del Ministero della Difesa”, approvata il 29/09/2000 dal C.S.M.D. d’intesa con il S.G.D./D.N.A..
- Decreto legislativo 30 giugno 2003 n. 196 “Codice in materia di protezione dei dati personali” e successivi aggiornamenti.
- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell’amministrazione digitale”.
- Direttiva PCDM n. 2/2009 del 26 maggio 2009.
- Direttiva SMD-I-019 “Politica di Sicurezza per i Sistemi di Telecomunicazione e Informatici Non Classificati della Difesa” Edizione 2009.
- Direttiva SMD-VI Reparto “Disposizioni per l’accesso ad Internet nelle reti non classificate della Difesa” Edizione 2011.
- Direttiva CL-3DV-014 “Compiti, attribuzioni e responsabilità CERT e CIRT”, CLA-NL-3320-0001-00B00 Edizione 2013.

PAGINA NON SCRITTA

XI

ENTI INTERESSATI

1. A livello centrale:
   - SMA e Alti Comandi: per opportuna conoscenza, ottemperanza e norma;
   - Divisioni/Servizi del Comando Logistico: per ottemperanza e norma.

2. A livello intermedio:
   Tutte le Articolazioni degli Enti Centrali AM: per ottemperanza e norma.

3. A livello periferico:
   Tutti gli Enti AM: per ottemperanza e norma.

PAGINA NON SCRITTA

PREMESSA, SCOPO E APPLICABILITÀ

La piena consapevolezza dei rischi elevatissimi per la sicurezza che derivano dalla esposizione della intranet di Forza Armata al mondo Internet, rende necessario prevedere un accesso ad Internet in modo selettivo.

Lo scopo della presente Direttiva è quello di disciplinare le modalità di accesso a Internet da parte degli utenti di FA, e normare l'interconnessione della intranet di FA (Aeronet) con il mondo Internet contenendo il rischio entro limiti accettabili e per quanto possibile conosciuti, e nel presupposto che l'obiettivo primario resti quello della salvaguardia della confidenzialità, dell'integrità e della disponibilità delle informazioni gestite e conservate nei sistemi informatici e di telecomunicazione della FA.

La presente direttiva si applica a tutti gli utenti ed a tutti i dispositivi (PC desktop, notebook, netbook, tablet, palmari, smartphone, etc.) in grado di connettersi ad Internet e che accedono alla stessa attraverso reti dell'Aeronautica Militare, siano essi dedicati a tale scopo o inseriti nel dominio Aeronet, e indipendentemente dalla tecnologia e dal tipo di trasporto e di protocollo utilizzati.

Capitolo I - GENERALITÀ

L'utilizzo delle tecnologie dell'informazione e della comunicazione (ICT) costituisce oggi un elemento cruciale per il conseguimento ed il mantenimento di elevati livelli di efficienza ed efficacia dello strumento militare. In tale ambito, parallelamente alla pluralità di servizi e funzionalità offerte dalla intranet di Forza Armata (Aeronet), il patrimonio informativo, i servizi e le funzionalità associate alla comunicazione disponibile su Internet, rappresentano una risorsa di importanza spesso fondamentale per il supporto logistico alle attività, il supporto decisionale e la capacità operativa. È pertanto imprescindibile garantire un adeguato livello di accesso a tale risorsa, sia attraverso risorse di rete dedicate a tale scopo, sia direttamente attraverso il dominio Aeronet.

Tuttavia è necessario che ciò avvenga in modo estremamente selettivo e nella piena maturità e consapevolezza dei rischi elevatissimi per la sicurezza che derivano dalla esposizione della intranet di Forza Armata al mondo Internet.

La riduzione del suddetto rischio a livelli accettabili comporta peraltro investimenti particolarmente ingenti da parte della FA in strumenti di sicurezza, tanto più elevati quanto più elevata è la diffusione del Servizio. La diffusione non disciplinata dell'accesso Internet, quando realizzato attraverso Aeronet, comporta inoltre la necessità di dover fronteggiare, come l'esperienza ha insegnato, l'ulteriore problematica generata dall'utenza inesperta e non formata, per la quale l'uso simultaneo sulla stessa postazione di lavoro di servizi Internet e intranet porta a "sfumare" il confine tra i due domini. Il rischio derivante assume in tale ambito livelli inaccettabili, solo limitatamente riducibili attraverso strumenti tecnologici, ma più spesso riguardanti la sfera della formazione ed educazione del singolo.

La Direttiva SMD-I-019 (Politica di Sicurezza per i Sistemi di Telecomunicazione ed Informatici non classificati della Difesa) delinea i principi generali in materia di disciplina dell'accesso a Internet, indica le misure di tipo tecnologico per la regolamentazione e protezione del servizio, e definisce le responsabilità a carico dell'Ente fornitore del Servizio Internet.

Nella suddetta Direttiva viene in particolare espressamente sottolineato come la minaccia ai sistemi informativi che costituiscono il patrimonio della Difesa, possa provenire sia dall'esterno, ossia da soggetti esterni all'Organizzazione Militare, sia dall'interno della stessa, con potenziale danno per l'Organizzazione militare nella sua interezza (Difesa) ed a livello di singolo dominio di Forza Armata. Ciò è tanto più vero in un contesto nel quale l'integrazione e reciproca interazione tra i sistemi informativi a livello Difesa è sempre più stretta, a cominciare dalla integrazione dei domini delle Forze Armate all'interno di una foresta unica.

In tale contesto la formazione ed educazione di tutto il personale ad un uso responsabile e consapevole dello strumento informativo, a cominciare dalla postazione di lavoro

assegnata per lo svolgimento della quotidiana attività lavorativa e della connessione Internet eventualmente resa disponibile, assume rilevanza strategica.

Capitolo II - PRINCIPI E VINCOLI

Tutti i soggetti autorizzati all'accesso e/o all'uso di risorse ICT della Difesa sono tenuti ad utilizzarle per le attività istituzionali. Potranno essere autorizzati eventuali usi discendenti da convenzioni o accordi approvati, purché l'utilizzo sia lecito e non in contrasto con la normale attività lavorativa e, per il personale militare, nel rispetto del Codice dell'Ordinamento Militare.

Il personale dell'Aeronautica Militare deve essere informato sulle proprie responsabilità in tema di sicurezza ICT, sensibilizzato al puntuale rispetto dei principi ed all'applicazione delle regole di sicurezza disposte, segnalando ogni comportamento non in linea con quanto definito.

L'Aeronautica Militare pone in essere tutte le azioni tecniche reputate necessarie alla garanzia e tutela dei sistemi informativi ed effettua i controlli sul personale per il corretto impiego degli strumenti telematici, in linea con le procedure previste dalla Direttiva SMD-I-019 Ed. 2009 "Politica di sicurezza per i sistemi di telecomunicazione ed informatici della Difesa".

Nell'esercizio di tali prerogative l'Aeronautica Militare garantisce che il trattamento dei dati personali di tutti gli utenti coinvolti a qualsiasi titolo sia conforme ai seguenti principi, in linea con quanto previsto dal D. Lgs. n. 196 del 2003:

1. principio di necessità:
   i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità;
2. principio di correttezza:
   le caratteristiche essenziali dei trattamenti devono essere rese note agli Utenti;
3. principio di pertinenza e non eccedenza:
   i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime, nella misura meno invasiva possibile, solo dai soggetti preposti, mirati sull'area di rischio, tenendo conto della normativa sulla protezione dei dati.

Capitolo III - MODALITÀ DI ACCESSO ALLA RETE INTERNET

Nel presente capitolo vengono disciplinate le modalità di accesso al servizio Internet e delle relative connessioni con la rete Aeronet, con il duplice obiettivo di assicurare la corretta fruibilità del servizio, garantendo al tempo stesso un livello di sicurezza adeguato, in funzione degli investimenti che la FA attua e potrà attuare nello specifico settore.

Il servizio Internet per gli utenti della Forza Armata può avvenire secondo le seguenti modalità:

1. **Servizio Internet attraverso Rete dedicata**

   In tale modalità l'accesso al servizio Internet è fornito localmente, presso ciascun Ente/Reparto della FA, da infrastrutture LAN dedicate e fisicamente separate dalla infrastruttura Aeronet, con client distinti per la navigazione Internet e intranet, in modo da evitare ogni interscambio tra le due reti e garantire al massimo livello la sicurezza della Aeronet.

   Tale soluzione comporta rilevanti oneri da un punto di vista realizzativo, per la necessità di duplicazione delle infrastrutture di rete necessarie, che solo in parte possono essere ridotti attraverso l'adozione di apposite VLAN sugli apparati attivi di rete. E' pertanto responsabilità di ciascun Comandante di Ente/Reparto valutare la effettiva necessità, nonché la portata ed estensione del servizio, che comunque in nessun caso potrà prevedere interconnessioni con la locale LAN Aeronet.

   Al Comandante di Ente/Reparto è altresì devoluta la responsabilità di disciplinare l'accesso al servizio Internet locale, previa implementazione di un adeguato sistema che, in linea con le disposizioni del presente documento, consenta:

   - l'identificazione univoca degli Utenti che accedono al servizio, tramite "*User Id*" e *password*;
   - la possibilità di *monitoring* degli accessi degli utenti così identificati;
   - la conservazione dei log di navigazione in accordo con la normativa vigente in continua evoluzione;
   - l'adeguata formazione/informazione degli utenti attraverso la sottoscrizione dei moduli di assunzione di responsabilità, di cui agli allegati "A" e "B" del presente documento e la conservazione degli stessi;
   - il filtraggio dei siti in linea con le restrizioni minime di cui all'allegato "C".

   Il Comandante provvede altresì alla nomina degli amministratori locali della rete dedicata al servizio Internet, che dovranno coincidere con l'organizzazione locale di sicurezza ICT – CIRT (Computer Incident Response Team), in aderenza alle direttive di settore (SMA-RGS-020, CL-3DV-014), inoltre cura l'indottrinamento e la formazione del personale dipendente al corretto impiego delle risorse ICT, facendo compilare e sottoscrivere apposito modulo di assunzione di responsabilità afferente

l'uso dello strumento informatico, comprensivo di specifiche indicazioni inerenti al servizio Internet, così come riportato in (Allegato "A").

Ciascun Ente/Reparto dovrà provvedere a comunicare al Comando Logistico 3ª Divisione le modalità di attuazione del servizio Internet locale con particolare riferimento ai sistemi di controllo adottati ed al provider individuato per la fornitura del servizio. Il Comando Logistico 3ª Divisione, per il tramite del dipendente Reparto Sistemi Informativi Automatizzati (ReSIA), fornisce supporto e consulenza specifica agli Enti/Reparti in materia di gestione del servizio Internet locale.

Ciascun Comando di Ente/Reparto, qualora si trovi nella impossibilità di porre in essere una infrastruttura come quella descritta, o che ravvisi particolari ragioni di opportunità, può formulare richiesta nei confronti del Comando Logistico 3ª Divisione di accesso al servizio Internet tramite la connettività commerciale disponibile presso Palazzo AM nell'ambito del Servizio Pubblica Connettività (SPC).

Tale modalità di accesso, benché sfrutti l'infrastruttura di trasporto di Aeronet per veicolare il traffico da e verso il punto di accesso Internet di Palazzo AM, non è da considerarsi un vero e proprio servizio di "*Internet over Aeronet*", disciplinato nel successivo paragrafo, in quanto deve comunque rispettare i suddetti criteri di separazione fisica e logica dal dominio Aeronet.

La gestione tecnica di tale modalità di accesso è affidata al ReSIA che provvede alla appropriata configurazione dei sistemi di sicurezza e dei proxy attraverso i quali essa viene realizzata. Il ReSIA ha facoltà di attuare, anche senza preavviso, limitazioni alla banda disponibile per il servizio e alle modalità di *web filtering*, in risposta a specifiche esigenze operative e di sicurezza, o su disposizione del Comando Logistico 3ª Divisione.

In questa modalità di accesso a Internet non è in nessun caso consentito richiedere al ReSIA personalizzazioni del livello di accesso e delle politiche di filtro, che sono riportate in allegato "C".

L'accesso al servizio Internet in tale modalità è basato sull'indirizzamento IP delle reti locali autorizzate, tassativamente differente da quello Aeronet, che il ReSIA provvede a standardizzare. Il Reparto/Ente che richiede l'accesso ad Internet deve assicurare la conservazione dei *log* di navigazione dei singoli utenti in aderenza alla normativa vigente ed è tenuto ad adottare le opportune soluzioni tecniche e/o procedurali necessarie a tale scopo.

Nell'assegnare tale accesso il Comandante, attraverso la sua articolazione a ciò deputata, avrà cura di indottrinare il personale interessato sull'uso dei Servizi, facendo sottoscrivere i previsti moduli di ammissione responsabilità di cui alla presente direttiva che dovranno essere conservati agli Atti dell'Ente.

Il ReSIA è responsabile della specifica disciplina delle modalità tecniche di accesso al Servizio in accordo alle linee di indirizzo del Comando Logistico 3ª Divisione e le attua attraverso l'emanazione di disposizioni di dettaglio nei riguardi degli amministratori di rete degli Enti/Reparti.

La vigilanza sul corretto e responsabile impiego del Servizio Internet è devoluta alla organizzazione locale di sicurezza (CIRT – Computer Incident Response Team) che dovrà segnalare ogni abuso secondo le procedure previste dalla Direttiva SMA-RGS-020 "Sicurezza per i sistemi di telecomunicazione ed informatici dell'Aeronautica Militare".

2. **Attraverso la rete Aeronet, per gli utenti in dominio aeronautica.difesa.dom, secondo procedure e livelli di accesso definiti**

L'accesso attraverso la rete Aeronet ha il vantaggio di consentire una gestione completamente centralizzata da parte della FA, ma espone il patrimonio informativo ed i relativi sistemi ICT a livelli di rischio molto elevati, nonché a limiti nella fruizione del servizio Internet dettati dalla disponibilità di banda.

La Direttiva SMD-I-019 "Politica di Sicurezza per i Sistemi di Telecomunicazione ed Informatici non classificati della Difesa", nel riconoscere il valore del patrimonio informativo disponibile sul *Web*, prevede la possibilità che il dominio Difesa possa essere interconnesso con domini *"untrusted"*, primo fra tutti quello Internet, ma subordina tale possibilità in primo luogo ad un rigoroso principio di necessità, poi alla adozione di idonee soluzioni tecnologiche, procedurali e di controllo tendenti a salvaguardare la sicurezza dei domini di ciascuna Forza Armata e, attraverso di essi, dell'intera foresta Difesa.

Nel presente paragrafo si intende pertanto descrivere le modalità di accesso degli utenti e delle postazioni di lavoro del dominio Aeronet al servizio Internet, che in questo senso è a tutti gli effetti da considerarsi un servizio "*Internet over Aeronet*".

La modalità standard di fruizione del servizio "*Internet over Aeronet*", definita "Accesso base", è quella che concede ad ogni titolare di una utenza del dominio *aeronautica.difesa.dom* ed assegnatario di una postazione di lavoro censita in tale dominio, l'accesso ad Internet attraverso il c.d. "proxy interoperabilità" che realizza la interconnessione dei servizi intranet di Forza Armata con i servizi intranet della Difesa.

Nell'ambito di questi ultimi servizi rientra infatti anche quello di accesso a Internet tramite connettività commerciale gestita dal Comando C4 Difesa.

Il Comando Logistico 3ª Divisione, attraverso il ReSIA, disciplina le politiche di accesso ai servizi intranet della Difesa da parte degli utenti di FA, ed in particolare per il servizio Internet stabilisce le modalità di gestione della quota di banda trasmissiva dedicata, le priorità ed i livelli di accesso.

Tale modalità di accesso, benché aperta in linea di principio a tutti gli utenti, attua una politica molto selettiva sulla navigazione *Web* rendendo disponibile un numero limitato di siti *web* espressamente autorizzati dal Comando Logistico 3ª Divisione sulla base dei seguenti criteri generali:

- rilevanza del sito *web* per le finalità di istituto della FA;

- carattere di interesse generale dei servizi e delle informazioni rilasciati dal sito *web*;
- sicurezza e reputazione del sito *web*;
- onerosità del sito richiesto in termini di banda trasmissiva necessaria alla fruizione dei relativi servizi e contenuti offerti.

Non è esclusa la possibilità di richiedere l'abilitazione via proxy interoperabilità di siti *web* aventi finalità istituzionali, ma di interesse limitato a ristretti ambiti di attività, sebbene ciò sia subordinato alla valutazione di opportunità da parte del Comando Logistico 3ª Divisione.

Le richieste di abilitazione di siti *web* attraverso tale modalità di accesso dovranno essere rispondenti ai suddetti criteri, ed inoltrate esclusivamente per il tramite degli amministratori di rete locali, alla casella di posta elettronica aeroresia.helpdesk@aeronautica.difesa.it. Sarà cura del ReSIA sottoporre alla valutazione del Comando Logistico 3ª Divisione le richieste di abilitazione in accordo ai processi interni stabiliti ed alle policy di F.A..

L'elenco dei siti autorizzati è riportato sul portale intranet del ReSIA, che ne cura il costante aggiornamento. Il ReSIA ha facoltà di attuare, anche senza preavviso, il blocco dei siti *web* autorizzati, e/o limitazioni alla banda assegnata per l'accesso ad Internet, in risposta a specifiche esigenze operative e di sicurezza, o su disposizione del Comando Logistico 3ª Divisione.

La seconda modalità di accesso al servizio "*Internet over Aeronet*", alternativa alla precedente, è costituita dall'impiego di un proxy di FA, denominato "Proxy Internet", che consente agli utenti in dominio *aeronautica.difesa.dom* l'accesso ad Internet attraverso la propria postazione di lavoro censita in dominio, utilizzando la connettività commerciale disponibile presso Palazzo AM nell'ambito del Servizio Pubblica Connettività (SPC).

Il Comando Logistico 3ª Divisione, di concerto con SMA, disciplina le politiche di sicurezza e di *web filtering* per tale tipologia di accesso, e le attua attraverso il ReSIA che cura la gestione tecnica del servizio.

Tale tipologia di accesso ad Internet, aperta esclusivamente ad utenti in dominio, deve essere caratterizzata da una elevatissima selettività, in ragione dei già citati potenziali rischi per la sicurezza, ed obbedisce ad una politica di *web filtering* chiusa, che suddivide i siti *web* in categorie e blocca quelle non previste, sulla base di criteri di sicurezza e di opportunità.

Gli strumenti tecnologici a disposizione della FA per l'attuazione delle politiche di *web filtering* consentono la completa personalizzazione del livello di accesso, fino alla autorizzazione per singolo sito e per singolo utente. Per tale ragione, ed ancora una volta al fine di contenere al massimo la superficie di esposizione al rischio per la sicurezza, è fondamentale che le richieste di accesso al servizio siano più circostanziate e dettagliate possibile.

Le richieste di abilitazione a tale modalità di accesso ad Internet, dovranno pervenire alla casella di posta elettronica aeroresia.helpdesk@aeronautica.difesa.it, esclusivamente da parte dell'amministratore di rete locale dell'Ente/Reparto richiedente, corredate dal modulo di assunzione di responsabilità riportato all'allegato "A", compilando anche il modulo aggiuntivo per la richiesta di accesso al servizio "*Internet over Aeronet*" debitamente controfirmato dal Comandante di Corpo che, con tale firma, autorizza abilitazione di accesso

Sarà cura del ReSIA sottoporre alla valutazione del Comando Logistico 3ª Divisione le richieste pervenute per la relativa autorizzazione, dopo averle valutate dal punto di vista tecnologico.

Il RESIA è responsabile della implementazione e gestione degli appropriati sistemi di autenticazione ed accesso al servizio, nonché della raccolta e conservazione dei *log* di navigazione riferiti ai singoli utenti, destinati ad essere resi disponibili alle autorità competenti ed in accordo alle vigenti normative in materia.

Capitolo IV – PROFILI DI ACCESSO UTENZA

Al fine di definire i livelli di servizio riservati all'utenza, nel presente Capitolo si individuano i diversi profili di accesso ad Internet, differenziati per qualifica/ruolo/funzione ricoperta.

1. Profilo di accesso base.

Come da capitolo III punto 3: il profilo base consente l'accesso ad Internet ad ogni titolare di una utenza del dominio *aeronautica.difesa.dom* ed assegnatario di una postazione di lavoro censita in tale dominio.

Tale modalità di accesso attua una politica molto selettiva sulla navigazione *web,* rendendo disponibile un numero limitato di siti espressamente autorizzati dal Comando Logistico 3ª Divisione sulla base dei seguenti criteri generali:

- rilevanza del sito *web* per le finalità di istituto della FA;
- carattere di interesse generale dei servizi e delle informazioni rilasciati dal sito *web*;
- sicurezza e reputazione del sito *web*;
- onerosità del sito richiesto in termini di banda trasmissiva necessaria alla fruizione dei relativi servizi e contenuti offerti.

Non è esclusa la possibilità di richiedere l'abilitazione di siti web aventi finalità istituzionali, ma di interesse limitato a ristretti ambiti di attività, sebbene ciò sia subordinato alla valutazione di opportunità da parte del Comando Logistico 3ª Divisione.

Le richieste di abilitazione di siti *web* attraverso tale modalità di accesso dovranno essere rispondenti ai suddetti criteri, ed inoltrate esclusivamente per il tramite degli amministratori di rete locali con l'approvazione dei Comandanti di corpo responsabili, alla casella e-mail aeroresia.helpdesk@aeronautica.difesa.it. Sarà cura del ReSIA sottoporre alla valutazione del Comando Logistico 3ª Divisione le richieste di abilitazione, in accordo ai processi interni stabiliti.

L'elenco dei siti autorizzati è riportato sul portale intranet del ReSIA, che ne cura il costante aggiornamento. Il ReSIA ha facoltà di attuare, anche senza preavviso, il blocco dei siti *web* autorizzati, e/o limitazioni alla banda assegnata per l'accesso ad Internet, in risposta a specifiche esigenze operative e di sicurezza, o su disposizione del Comando Logistico 3ª Divisione.

2. Classe di accesso per incarichi funzionali di Capo Sezione e Dirigenti (Capi Uffici e vice Capi Uffici o equivalenti)

Tale tipologia di accesso ad Internet è riservata al personale che ricopre l'incarico di Capo Sezione degli Enti Centrali o incarico corrispondente ed al personale dirigente di FA, ed obbedisce anch'essa ad una politica di *web filtering* chiusa, che suddivide i siti

web in categorie e blocca quelli non previsti, sulla base di criteri di sicurezza e di opportunità.

Il Comando Logistico 3ª Divisione disciplina le politiche di sicurezza e di *web filtering* per tale tipologia di accesso e le attua attraverso il ReSIA che cura la gestione tecnica del servizio**.**

Ove particolari esigenze di servizio lo richiedano, tale classe di accesso potrà essere concessa anche al personale non ricadente nelle qualifiche Capo Sezione/Dirigente (o equivalente), sulla base di richiesta motivata e sottoscritta da parte del Comandante di corpo dell'Ente/Articolazione a cui appartiene l'interessato, in cui siano evidenti le reali motivazioni che giustifichino l'accesso ad utenze di una classe di livello superiore a quelle standard previste per l'utente.

3. Classe di accesso per i Vertici di FA e Ufficiali Generali

Tale classe di accesso è riservata ai vertici della FA e viene gestita con le stesse modalità della precedente, ma è caratterizzata da minori restrizioni alla navigazione. Ove particolari esigenze di servizio lo richiedano, tale classe di accesso potrà essere concessa anche al personale di cui alla classe indicata al precedente punto 2, sulla base di richiesta motivata che sarà di volta in volta vagliata dal Comando Logistico 3^ Divisione. Nella eventuale richiesta dovranno essere indicate le reali motivazioni che giustifichino l'accesso alla classe superiore.

Capitolo V– RESPONSABILITÀ E COMPITI

Tutto il personale di FA utente delle postazioni informatiche connesse ad Internet, dovrà provvedere a compilare e sottoscrivere il modulo di assunzione di responsabilità in allegato "A" in cui deve prendere coscienza dei seguenti aspetti:

- potenziali rischi ai quali sta esponendo l'intera organizzazione;
- responsabilità personale di ogni conseguenza derivante dall'accesso ad Internet con il livello di abilitazione richiesto;
- accettazione dell'eventualità di essere sottoposto a controllo da parte del personale del ReSIA preposto alla tutela della sicurezza.

Tale attività, di cui è responsabile il Proprietario dei dati locale/Comandante dell'Ente, avverrà a cura del . Responsabile Operativo locale per la Sicurezza ICT (CL 3DIV 014 – Cap I, punto 3, comma e), che dovrà anche provvedere all'indottrinamento periodico del predetto personale, in analogia a quanto avviene per la trattazione della documentazione classificata, con strumenti e metodologie che verranno fornite e condivise dal CERT AM.

Le politiche di accesso, ad eccezione di Internet fornito da provider locali a cura dei singoli Comandanti, sono disciplinate dal Comando Logistico 3ª Divisione, attraverso il ReSIA, che, in particolare per il servizio Internet, stabilisce le modalità di gestione della quota di banda trasmissiva dedicata, le priorità ed i livelli di accesso.
I profili di utenza, così come regolamentati nel precedente capitolo, dovranno essere implementati, a cura dei comandanti responsabili, anche per le modalità di connessione al servizio Internet mediante l'uso della rete dedicata, di cui al precedente Capitolo III (provider locali).

E' responsabilità dei Comandanti di Corpo per casi eccezionali e solo per comprovate ed inderogabili esigenze di servizio, richiedere per le poche utenze che ne avranno necessità:

- abilitazioni in deroga per il personale non dirigente, che potrà essere abilitato soltanto ed esclusivamente alla classe di accesso per il personale dirigente;
- abilitazioni in deroga per il personale dirigente per l'uso della classe di accesso riservata ai vertici di FA .

di cui al precedente capitolo, punti 2 e 3.

La richiesta dovrà pervenire attraverso i canali ufficiali e completa delle opportune motivazioni al Comando Logistico 3ª Divisione, che esprimerà parere circostanziato per la possibile successiva autorizzazione in deroga per il tramite del ReSIA.

Per il personale che usufruisce delle abilitazioni con classe di accesso associata al servizi disciplinati ai punti "2." e "3." Del precedente capitolo, oltre al modulo in allegato "A", sarà obbligatoria la compilazione anche del modulo in allegato "B", con cui l'utente ed il proprio Comandante di Corpo prendono coscienza dei seguenti aspetti:

- potenziali rischi ai quali sta esponendo l'intera organizzazione;

- responsabilità personale di ogni conseguenza derivante dall'accesso ad Internet con il livello di abilitazione sottoscritto;
- accettazione dell'eventualità di essere sottoposto a controllo da parte del personale del ReSIA preposto alla tutela della sicurezza.

Per quanto attiene a responsabilità e compiti precipue delle Articolazioni di FA:

a. il 4° Reparto dello Stato Maggiore dell'Aeronautica:

Provvede a valutare le esigenze di aggiornamento tecnico e di evoluzione del servizio alla luce degli sviluppi del settore e delle Direttive Ministeriali, curando l'integrazione della componente A.M. (dominio Aeronet) nel contesto interforze (dominio Difenet) e nella Pubblica Amministrazione (Sistema Pubblico di Connettività) ed emanando i relativi indirizzi di policy del settore;

b. la 3ª Divisione del Comando Logistico:

- promuove l'ammodernamento, l'adeguamento tecnologico e la sicurezza dei sistemi ICT;
- emana le linee guida in materia di sicurezza informatica sulla base delle normative vigenti e delle direttive interforze (nei limiti specificati dalla direttiva PDCM n. 2/2009);
- è responsabile, tramite il ReSIA, del funzionamento della rete telematica AERONET e della relativa connessione alla intranet della Difesa (DIFENET);
- traduce gli indirizzi di policy dello Stato Maggiore AM in materia di gestione del servizio Internet in direttive attuative;
- valuta, avvalendosi del supporto tecnico del ReSIA, le esigenze di accesso ad Internet ed emana le relative autorizzazioni;
- garantisce la disponibilità di connettività per il servizio Internet attraverso il Servizio Pubblica Connettività – SPC;
- provvede, attraverso il ReSIA, alla gestione tecnica del servizio Internet in tutte le modalità, attuando quanto previsto dalla vigente normativa, ed attuando le misure tecnologiche e procedurali per la tutela della Sicurezza;
- dispone l'effettuazione di controlli, attraverso il ReSIA, da remoto o tramite attività di Audit in loco, circa lo stato di sicurezza delle reti, ivi comprese quelle localmente dedicate al servizio Internet;
- supervisiona le attività di formazione ed indottrinamento degli utenti del dominio Aeronet in materia di uso responsabile dei servizi ICT, ivi compreso Internet.

c. Il Reparto Sistemi Informativi Automatizzati

- è responsabile, dal punto di vista tecnico, del funzionamento della rete telematica AERONET e della relativa connessione alla intranet della Difesa (DIFENET);
- fornisce consulenza tecnica alla 3ª Divisione del Comando Logistico in materia di accesso ad Internet;
- provvede alla gestione tecnica del servizio Internet in tutte le modalità, attuando quanto previsto dalla vigente normativa ed attuando le misure tecnologiche e procedurali per la tutela della sicurezza;
- effettua attività di controllo, da remoto o direttamente in loco, circa lo stato di sicurezza delle reti, ivi comprese quelle localmente dedicate al servizio Internet.

d. Il Comandante dell'Ente/Reparto:

- è responsabile della gestione del servizio Internet attivato a livello locale, provvedendo a tutti gli adempimenti normativi ivi compresa la nomina degli amministratori delle reti dedicate;
- è responsabile del controllo sul personale abilitato, e della adozione degli opportuni provvedimenti derivanti da ogni abuso nell'impiego del servizio;
- è responsabile della segnalazione di ogni evento rilevante per la sicurezza secondo le modalità e procedure previste dalla SMA-RGS-020, ivi compresa la interconnessione fraudolenta della rete locale Aeronet con Internet;
- è responsabile della comunicazione alla 3ª Divisione del Comando Logistico della modalità di accesso ad Internet adottata a livello locale;
- è responsabile della conservazione dei log di navigazione in aderenza alla normativa vigente.

e. Amministratore di rete

- è responsabile del controllo di configurazione, dell'implementazione, dell'efficienza e della disponibilità della rete locale Aeronet;
- è responsabile del controllo di configurazione e dell'implementazione della rete locale dedicata ad Internet, avendo cura della sua separazione fisica dalla rete Aeronet;
- è l'unica interfaccia titolata da/verso il ReSIA per le richieste di assistenza in merito alla reti locali sotto la sua gestione;
- è responsabile dell'implementazione delle procedure di sicurezza previste dalla SMA-RGS-020.

f. Utente:

- è responsabile del corretto utilizzo del servizio Internet, astenendosi da qualunque comportamento che possa mettere a rischio le risorse ICT di FA;
- deve attenersi scrupolosamente a tutte le prescrizioni contenute nel “Modulo di assunzione di responsabilità” in allegato “A” e “B” (ove previsto);
- deve, soprattutto se titolare di privilegi estesi di accesso ad Internet, curare con particolare attenzione la custodia delle proprie credenziali utente;
- deve segnalare all’amministratore di rete o referente informatico del proprio Ente ogni evento o circostanza che possa rilevare per la sicurezza dei servizi ICT.

PAGINA NON SCRITTA

ALLEGATI

PAGINA NON SCRITTA

COMANDO ENTE

MODULO DI ASSUNZIONE DI RESPONSANBILITÀ

Con il presente modulo d'Assunzione di Responsabilità il sottoscritto (grado/qualifica cognome e nome) …… …… …… ……..
in servizio presso ……..
località……telefono ufficio …… assegnatario della casella di posta elettronica dell'Amministrazione Difesa ……..……..……*@aeronautica.difesa.it*.

dichiara di essere a conoscenza che:

a. il PC affidatogli dall'Amministrazione Difesa deve essere utilizzato esclusivamente per adempiere alle sole esigenze d'istituto a lui demandate. La possibilità d'uso di Internet è consentita unicamente per incrementare l'efficienza e la produttività del proprio lavoro e NON per scopi personali;

b. l'user-ID di dominio assegnato e la password di accesso devono essere custoditi e mantenuti strettamente riservati e non devono essere condivisi con altri utenti;

c. non è auspicabile detenere dati personali sul PC in dotazione;

d. l'indirizzo di posta elettronica (e-mail) assegnato, ancorché nella forma nome.cognome@am.difesa.it, non ha caratteristiche di privatezza ma costituisce normale strumento di lavoro e ne è vietato l'utilizzo per scopi personali. L'assegnatario è tenuto ad informare di tale caratteristica i terzi a cui comunica il citato indirizzo e-mail;

e. l'utilizzo di apparati di sicurezza (firewall IDS) e di filtraggio della posta indesiderata (firewall-antispam) devono inevitabilmente analizzare in modo autonomo ed automatico il traffico Internet e della posta elettronica per svolgere il loro compito;

f. deve essere data tempestiva comunicazione al proprio amministratore di rete/referente informatico o anche direttamente al ReSIA (tel. 06/783621 o 604.3001) dell'eventuale perdita di riservatezza delle proprie credenziali di dominio (user ID e password);

g. è vietato immettere, trasmettere, diffondere qualsiasi materiale che non può essere distribuito legalmente via rete telematica (vedi disposizioni di legge di seguito indicate);

h. è vietato modificare la configurazione del PC in dotazione. Le esigenze di impiego di software diverso da quello in dotazione, qualora non disponibile in apposito catalogo di FA per il download automatico, devono essere rappresentate al proprio amministratore di rete/referente informatico;

i. le disposizioni legislative sulla tutela giuridica del software considerano i programmi per elaboratore alla stregua di opere letterarie protette dalle vigenti leggi in materia;

j. la riproduzione permanente/temporanea, totale/parziale di software acquisito dal commercio o prodotto dall'Amministrazione Difesa deve essere autorizzata dai titolari dei diritti di proprietà sullo stesso;

k. chiunque abusivamente duplica software per uso su elaboratori o sapendo o, avendo motivo di sapere che si tratta di copie non autorizzate, lo distribuisce, lo vende, lo detiene a scopi commerciali/personali, è soggetto

alla pena prevista dalla vigente legislazione. Alla stessa pena è soggetto chi mette in atto sistemi tendenti a facilitare la rimozione arbitraria e l'elusione funzionale dei dispositivi applicati a protezione dei software per uso su elaboratori;

l. lo scarico dalla rete (download) di opere protette dal copyright (musiche, filmati, programmi etc. etc.) non è consentito a nessun titolo ed è soggetto a sanzione in conformità dalle vigenti leggi;

m. la detenzione sul proprio elaboratore di contenuti pedo-pornografici è vietata e soggetta a sanzione in conformità alle vigenti leggi;

n. non sono consentite azioni tendenti a nascondere la propria identità, a molestare o arrecare danno all'attività degli elaboratori di altri utenti o ad acquisire dati/informazioni/privilegi a cui non si ha diritto.

Qualsiasi inadempienza a quanto dichiarato nel presente documento costituirà infrazione al regolamento di disciplina, salvo più grave infrazione alle leggi e regolamenti esistenti e provocherà quanto meno l'immediata sospensione del servizio rete Internet. Il Comando Logistico 3ª Divisione - Reparto Sistemi Informativi Automatizzati può interrompere il servizio prestato al sottoscritto anche solo per palese violazione del codice di buon comportamento.

L'amministratore di rete locale/referente informatico provvederà a fornire adeguato supporto e consulenza specifica in materia di gestione della postazione di lavoro e di accesso al servizio Internet.
Si riportano per opportuna informazione le normative che regolano l'argomento oggetto del presente modulo:

- Netiquette, "galateo di internet";
- D.P.R. n.144 in data 27/07/2005 "Misure urgenti per il contrasto del terrorismo internazionale";
- D.Lgs. 196 in data 30/06/2003, "Codice di protezione dei dati personali";
- D.P.R. n. 513 in data 10/11/1997, "Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'art. 15, comma 2 della Legge in data 15/03/1997 n. 59";
- Legge n. 633 in data 22/04/1941 in materia di disposizioni sul diritto di autore, come modificato dalla legge n.2 del 09/01/2008;
- Art. 615-ter del Codice Penale in merito all'accesso abusivo ad un sistema informatico o telematico;
- Legge 23 dicembre 1993 n. 547 "Modificazioni ed integrazioni delle norme del Codice Penale e del codice di procedura penale in tema di criminalità informatica".
- Codice dell'Amministrazione Digitale (CAD) in vigore a decorrere dal 1 gennaio 2006
- Direttiva n. 2/2009 della presidenza del Consiglio dei Ministri – Dipartimento della Funzione Pubblica.

I dati di questo modulo saranno utilizzati dal Comando, titolare del trattamento degli stessi, nel rispetto del D.Lgs. 196 in data 30/06/2003.

Firma per accettazione

_____

Località, _____

COMANDO ENTE

MODULO AGGIUNTIVO PER CLASSI DI ACCESSO AL SERVIZIO INTERNET "CAPI SEZIONE, DIRIGENTI" E "VERTICI DI FA"

Con il presente modulo d'assunzione di Responsabilità il sottoscritto (grado/qualifica cognome e nome) …… …… ……
in servizio presso ……
località……. telefono ufficio ……. assegnatario della casella di posta elettronica dell'Amministrazione Difesa ……. *@aeronautica.difesa.it.*

DICHIARA:

- di essere consapevole che l'utilizzo della classe di accesso per (barrare la classe di utilizzo):
  ☐ Capi Sezione/Dirigenti;
  ☐ Vertici
  comporta maggiori rischi per la sicurezza del patrimonio informativo –della FA e pertanto ai fini della presente richiesta, di aver al riguardo ricevuto adeguato indottrinamento da parte della organizzazione locale preposta alla Sicurezza ICT;
- di utilizzare l'utenza Internet esclusivamente per esigenze legate alla propria attività di servizio, nell'impossibilità di poterla altrimenti soddisfare;
- di impegnarsi ad attuare un comportamento particolarmente responsabile nell'uso del servizio e nella custodia delle proprie credenziali di accesso;
- di essere informato e di accettare tutti i controlli da parte della organizzazione locale preposta alla Sicurezza ICT e dal ReSIA, nei limiti previsti dalla "*Direttiva per la gestione dell'accesso al servizio Internet in Aeronautica Militare"*.

Firma per accettazione

Località, _____ _____

Visto per approvazione
(Il Comandante di Corpo)

_____

PAGINA NON SCRITTA

CATEGORIZZAZIONE SITI WEB PROXY ACCESSO INTERNET SU SERVIZIO SPC

Porte TCP/UDP aperte: 80 (http) 443 (https)

Le seguenti categorie web sono interdette:
ADULT
ADVERTISEMENT
CRIMINAL ACTIVITY
HACKING
INTOLERANCE AND HATING
VIOLENCE
SPYWARE
PHISHING
ILLEGAL DRUGS
CHAT
RINGTONES
PEER TO PEER
PROXYES
PERSONALS AND DATING
ENTERTAINMENT
GAMES
STREAMING MEDIA

Le seguenti categorie di applicativi sono interdette:

PEER TO PEER
BYPASS PROXYES AND TUNNELS
APPLICATIVI FACEBOOK (CHAT, GAMES ET SIMILIA)

PAGINA NON SCRITTA

ELENCO DI DISTRIBUZIONE

1. **ENTI CENTRALI DELLA DIFESA**

- STAMADIFESA	ROMA
- SEGREDIFESA	ROMA
- BILANDIFE	ROMA
- ISPEDIFE	ROMA
- COMMISERVIZI	ROMA
- ARMAEREO	ROMA
. UTARM	MILANO
. UTARM	TORINO
. UTARM	NAPOLI
- DUTARM	BRINDISI
- GENIODIFE	ROMA
- NAVARM	ROMA
- TERRARM	ROMA
- TELEDIFE	ROMA
- PERSOMIL	ROMA
- PREVIMIL	ROMA
- PERSOCIV	SEDE
- DIFESAN	ROMA

2. **ENTI DELL'AERONAUTICA MILITARE**

- STATAEREO	SEDE
- AEROSQUADRA	ROMA
- AEROSCUOLE/AEROREGIONE 3	BARI
- DIPMA	SEDE
- ISPAVIAMAR	ROMA
- AEROSICURVOLO	SEDE
- AEROREGIONE PRIMA	MILANO
- AEROCOMANDO	CENTOCELLE
- AEROSQUADRA COA	POGGIO RENATICO
- AEROFORCOMBAT	MILANO
- COMMOBSUP	ROMA
- 1^ AEROBRIGATA	ROMA
- AEROSCIENZE	FIRENZE
- AEROACCADEMIA	POZZUOLI
- 46^ AEROBRIGATA	PISA
- SPERINTER	PERDASDEFOGU
- 4° AERORTM	BORGO PIAVE
- AEROISTME	MILANO
- AEROISTME	ROMA
- 2° AEROSTORMO	RIVOLTO
- 3° AEROSTORMO	VILLAFRANCA
- 4° AEROSTORMO	GROSSETO
- 6° AEROSTORMO	GHEDI
- 9° AEROSTORMO	GRAZZANISE
- 14° AEROSTORMO	PRATICA DI MARE
- 15° AEROSTORMO	CERVIA
- 16° AEROSTORMO	MARTINA FRANCA
- 17° AEROSTORMO INCURSORI	FURBARA
- 31° AEROSTORMO	CIAMPINO
- 32° AEROSTORMO	AMENDOLA
- 36° AEROSTORMO	GIOIA DEL COLLE
- 37° AEROSTORMO	TRAPANI

- 41° AEROSTORMO	SIGONELLA
- 50° AEROSTORMO	PIACENZA
- 51° AEROSTORMO	ISTRANA
- 61° AEROSTORMO	LECCE
- 70° AEROSTORMO	LATINA
- 72° AEROSTORMO	FROSINONE
- AEROCAT	DECIMOMANNU
- AERORESTOGE	PRATICA DI MARE
- AEROCENTRO GRAM	POGGIO RENATICO
- 1° AEROREMAVELI	CAMERI
- 3° AEROREMAVELI	TREVISO
- 10° AEROREMAVELI	LECCE
- 11° AEROREMAVELI	SIGONELLA
- 6° AEROREMAELI	PRATICA DI MARE
- AEROP	PRATICA DI MARE
- AEROP	AVIANO
- AEROP	CAMERI
- AEROP	CAPODICHINO
- AEROP	GUIDONIA
- AEROP	VIGNA DI VALLE
- AEROP QG 1^ R.A.	LINATE
- AEROP QG COMAER	CENTOCELLE
AEROCOMSEV	ROMA
- AEROSCUOLE/AEROREGIONE 3 QG	PALESE
- AEROREPASSG	POGGIO RENATICO
- AEROMARESCIALLI	VITERBO
- AEROSPECIALISTI	CASERTA
- AEROVOLONTARI	TARANTO
- AEROLINGUE	LORETO
- AEROSCUOLA DOUHET	FIRENZE
- AEROASSIVOLO	PRATICA DI MARE
- AEROGEO	PRATICA DI MARE
- AEROSELEZIONE	GUIDONIA
- AEROCENTRORIF	FIUMICINO
- AERORESIA	ACQUASANTA
- AEROCENTROSANITARIO	ROMA
- 1° AERORTC	LINATE
- 2° AERORTC	PALESE MACCHIE
- 2° AEROREMAMISSILI	PADOVA
- 1° AEROGENIO	VILLAFRANCA
- 2° AEROGENIO	CIAMPINO
- 3° AEROGENIO	PALESE MACCHIE
- AEROINFERM	BARI
- AEROINFERM	MILANO
- AEROINFERM	PRATICA DI MARE
- AEROINFERM	ROMA
- AEROINFERM	VILLAFRANCA
- AEROINFERM POLIFUNZIONALE	POZZUOLI
- 313° AEROGRUPPO	RIVOLTO
- 21° AERORADAR	POGGIO BALLONE
- 22° AERORADAR	LICOLA
- AEROREP C2M	PALESE MACCHIE
- AEROREGISCC	PRATICA DI MARE
- AEROSUPERVISIONERETI	MONTECAVO
- 1° AERORISMI	VEVERI
- 5° GRUMAVELI	CAPODICHINO
- 2° AEROGRUMAUTO	FORLI’
- 3° AEROGRUMAUTO	MUNGIVACCA
- AEROCENTROLOG	GUIDONIA
- 2° AERODEP	GALLARATE

- 11° AERODEP	ORTE
- 64° AERODEPOTER	PORTO SANTO STEFANO
- 65° AERODEPOTER	TARANTO
- AERODEP RETE POL	PARMA
- RAMI – EAG	HIGH WYCOMBE (GBR)
- RAMI – IWSSC	HALLBERGMOOS (GER)
- RAMI – AM-X	BRASILIA (BRA)
- RAMI – TLP	ALBACETE (SPA)
- RAMI – ENJJPT	SHEPPARD (USA)
- RAMI – NTFC	MOOSE JAW (CAN)
- RAMI – CDAOA	TAVERNY-PARIGI (FRA)
- RAMI – NAEW	GEILENKIRCHEN (GER)
- RAMI – EF2000	TORREJON DE ARDOZ (SPA)
- RAMI – B767 T/T	WICHITA (USA)
- RAMI – ACCS “NATEX” PRESSO NACMA	BRUXELLES (BEL)
- RAMI – C130J	DAYTON (USA)
- RAMI – ACCS – “PMREP” PRESSO NACMA	BRUXELI ES (BEL)
- RAMI – F16	HILL (USA)
- RAMI – DDE HELIOS	ISSY LES MOULINEAUX (FRA)
- RAMI – AJETS	CAZAUX (FRA)
- RAMI – PA200-EF2000	BICESTER (GBR)
- RAMI – MRCA-EF2000	ERDING (GER)
- RAMI – IAFFT	MADRID (SPA)
- RAMI – IAFFT	WARTON (GBR)
- RAMI – SCUOLA EPNER	ISTRES CODEX (FRA)
- RAMI – BASE AEREA	KALAMATA (GRE)
- AEROPDIST	BRINDISI
- AEROPDIST	ELMAS
- AEROPDIST	ALGHERO
- AEROPDIST	DOBBIACO
- AEROPDIST	PANTELLERIA
- AEROCENTRO LOGISTICO	CADIMARE
- AERODIST	JACOTENENTE
- AERODIST	MONTESCURO
- AERODIST	TERMINILLO
- AERODIST	OTRANTO
- AERODIST	SIRACUSA
- AERODIST	CAPO MELE
- AERODIST	LAMPEDUSA
- AERODIST	LUNI SARZANA
- DISTASPERINTER	CAPO SAN LORENZO
- AEROMAGA	GUIDONIA
- 112° AEROSUDEP	SANGUINETTO
- 114° AEROSUDEP	FRANCAVILLA FONTANA
- 1° AEROSTD	CASELLE
- 2° AEROSTD	TORINO
- 3° AEROSTD	FINALE LIGURE
- 4° AEROSTD	CASCINA COSTA
- 6° AEROSTD	VENGONO SUPERIORE
- 7° AEROSTD	MILANO
- 8° AEROSTD	FIRENZE
- 9° AEROSTD	FOLIGNO
- 10° AEROSTD	POMEZIA
- 11° AEROSTD	FROSINONE
- 12° AEROSTD	NAPOLI
- 13° AEROSTD	BRINDISI
- 1° AEROLAB	PADOVA
- 2° AEROLAB	FIUMICINO
- 3° AEROLAB	MUNGIVACCA
- 4° AEROLAB	PARMA

- 5° AEROLAB	DECIMOMANNU
- 6° AEROLAB	TRAPANI
- 112 AEROSQUADRIGLIA RADAR	MORTARA
- 113 AEROSQUADRIGLIA RADAR	LAME
- 114 AEROSQUADRIGLIA RADAR	POTENZA PICENA
- 115 AEROSQUADRIGLIA RADAR	CAPO MELE
- 123 AEROSQUADRIGLIA RADAR	CAPO FRASCA
- 131 AEROSQUADRIGLIA RADAR	JACOTENENTE
- 132 AEROSQUADRIGLIA RADAR	CROTONE
- 133 AEROSQUADRIGLIA RADAR	CHIETI
- 134 AEROSQUADRIGLIA RADAR	LAMPEDUSA
- 135 AEROSQUADRIGLIA RADAR	MARSALA
- 136 AEROSQUADRIGLIA RADAR	OTRANTO
- 137 AEROSQUADRIGLIA RADAR	MEZZOGREGORIO
- JOINT AIR TASK FORCE	HERAT
- TASK FORCE AIR	AL BATEEN
- SCUOLA AEROCOOPERAZIONE	GUIDONIA

3. **DISTRIBUZIONE INTERNA**

- 1^DIVISIONE CSV AEROLOG	PRATICA DI MARE
- 2^ DIVISIONE AEROLOG	SEDE
- 3^ DIVISIONE AEROLOG	SEDE
- SERVIZIO DEI SUPPORTI AEROLOG	SEDE
- SERVIZIO DI COMMISSARIATO E AMMINISTRAZIONE AEROLOG	SEDE
- SERVIZIO INFRASTRUTTURE AEROLOG	SEDE
- SERVIZIO SANITARIO AEROLOG	SEDE
- AEROLOG UFFICIO CERTIFICAZIONE	SEDE
- AEROLOG UCL – SEZIONE COMANDO	SEDE
- AEROLOG UCL – SEZIONE PERSONALE	SEDE
- AEROLOG UCL – SEZIONE SICUREZZA	SEDE
- AEROLOG S.M. 1° UFFICIO	SEDE
- AEROLOG S.M. 3° UFFICIO	SEDE
- AEROLOG S.M. 4° UFFICIO	SEDE
- AEROLOG S.M. 5° UFFICIO	SEDE