MINISTERO DELLA DIFESA
AGENZIA INDUSTRIE DIFESA
DIREZIONE GENERALE

Piazza della Marina, 4 – 00196 ROMA
Posta elettronica: aid@aid.difesa.it
Posta elettronica certificata: aid@postacert.difesa.it

Tel: 06/36804457 – Fax: 06/36803921
P.I. 07281771001 – C.F. 97254170588

Atto Organizzativo 6/2020

Direttiva sull'applicazione dell'istituto del "Lavoro agile" (*Smartworking*) presso la Direzione Generale e le Unità Produttive di Agenzia Industrie Difesa durante la fase transitoria e a regime a seguito delle misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19 .

IL DIRETTORE GENERALE

VISTA la delibera del Consiglio dei Ministri del 31 gennaio 2020 "Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili", che dichiara per 6 mesi lo stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili;

VISTO il DL 23 febbraio 2020, n. 6, recante "Misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19", in particolare l'art. 3, "Applicazione del lavoro agile";

VISTO il D.P.C.M. 23 febbraio 2020 recante "Disposizioni attuative del decreto-legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19", in particolare l'art. 3"Applicazione del lavoro agile";

VISTA la circolare n.1/2020 del 04/03/2020 della Presidenza del Consiglio dei Ministri recante "Misure incentivanti per il ricorso a modalità flessibili di svolgimento della prestazione lavorativa";

VISTA la direttiva prot. n. M-D GSGDNA REG2020 0017383 del 5 marzo 2020 emanata da SGD I Reparto relativa a "Misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19. Accesso alle attività di istituto tramite modalità di *smart working*".

VISTO il DPCM 8 marzo 2020 "Ulteriori disposizioni attuative del decreto-legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19", in particolare l'art. 2, co. 1) lett. r);

Digitally signed by GIAN CARLO ANSELMINO
Date: 2020.03.11 15:16:10 CET

VISTO il DPCM 9 marzo 2020 “Ulteriori disposizioni attuative del decreto-legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19, applicabili sull’intero territorio nazionale”, che estende le previsioni dell’art. 1 del DPCM 8 marzo 2020 a tutto il territorio nazionale;

VISTA la direttiva prot. n. M-D GSGDNA REG2020 0018289 del 9 marzo 2020 emanata da SGD I Reparto relativa a “Misure urgenti in materia di contenimento e gestione dell’emergenza epidemiologica da COVID-19. Accesso alle attività di istituto tramite modalità di *smart* w*orking*” che estende le previsioni della precedente direttiva anche al personale militare;

VISTA altresì, la legge 22 maggio 2017, n. 81 recante “Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato”, in particolare il Capo II, Lavoro agile, artt. 18-23;

VISTO l’Atto Organizzativo n. 5/2020 emanato dal Direttore Generale di AID in data 10 marzo 2020 recante “Applicazione delle misure urgenti in materia di contenimento e gestione dell’emergenza epidemiologica da COVID-19 presso la Direzione Generale e le Unità Produttive dell’Agenzia Industrie Difesa e avvio dell’applicazione dell’istituto del “Lavoro agile” (*Smart working*).”

PRESO ATTO, in considerazione dell’emergenza epidemiologica in atto, della necessità di avviare l’istituto del lavoro agile (*smart working*) in tempi brevi e anche in forma transitoria in attesa dell’ultimazione delle attività di predisposizione degli strumenti informatici necessari da parte dell’Area strategica ICT della Direzione Generale, allo scopo di implementare le misure più idonee ad evitare la diffusione del contagio, salvaguardando la salute dei soggetti a rischio e, allo stesso tempo, di continuare lo svolgimento delle attività lavorative, con particolare attenzione a quelle finalizzate alla produzione, che si svolgono presso gli Stabilimenti Militari;

ATTESO CHE presso le Unità Produttive si svolgono, sotto la direzione del Direttore di ciascuna UP, attività lavorative di diversa natura e tipologia finalizzate a garantire produzioni di beni e servizi caratterizzate da specifiche peculiarità;

CONSIDERATO inoltre che non tutte le attività sopradescritte sono idonee all’applicazione dell’istituto del lavoro agile;

DISPONE

l’attivazione dello *smart working*, previa individuazione dei destinatari da parte del Direttore Generale/Dirigenti responsabili per il personale della Direzione Generale e Direttori di Stabilimento per il personale delle Unità Produttive, per tutto il periodo di emergenza dichiarato dal Consiglio dei Ministri con delibera del 31 gennaio 2020 e salvo eventuali proroghe, secondo le indicazioni di dettaglio qui di seguito fornite.

Premessa

E’ necessario prendere atto, preliminarmente, che l’istituto del lavoro agile (*smart working*) non è per sua natura applicabile a tutte le attività che si svolgono presso Agenzia Industrie Difesa, in

special modo alle attività produttive che si svolgono presso le Unità Produttive, in relazione alle quali si fa rinvio a quanto già previsto nell'A.O. n. 5/2020 in relazione alle misure di sicurezza e alla limitazione dei rischi legate allo svolgimento delle attività presso la sede di servizio e agli istituti che permettono l'assenza del lavoratore, soprattutto con riferimento al personale "a rischio" in ragione dell'età e in particolari condizioni personali/familiari come individuate dalla circolare 1/2020 del 4 marzo 2020.
Nei casi in cui è possibile applicare lo *smart working*, a giudizio del dirigente responsabile presso la Direzione Generale e del Direttore di ogni UP ad esso deve essere data pronta applicazione secondo le indicazioni qui di seguito riportate.

Applicazione dell'istituto

- Il personale, civile e militare, individuato da ciascun dirigente responsabile della DG e dal Direttore di ciascuna UP ai fini dell'applicazione dello *smart working* dovrà svolgere le attività lavorative esclusivamente presso l'indirizzo di residenza o domicilio, se non coincidente, da indicarsi nella comunicazione di attivazione dello *smart working* di cui si allega fac-simile (*allegato 1*);

- Nel caso di necessità di svolgimento dello *smart working* presso altri siti, ammissibile solo nei casi strettamente indispensabili, il personale dovrà essere espressamente autorizzato dal Direttore UP/dirigente responsabile, e sempre nel rispetto delle indicazioni di sicurezza sanitaria e distanziamento sociale e di tutte le disposizioni in vigore relative allo spostamento sul territorio nazionale;

- La prestazione di lavoro agile (*smart working)* potrà svolgersi con i mezzi forniti dall'amministrazione e, qualora non fossero disponibili, anche attraverso l'uso di strumenti personali, nel rispetto dei principi di riservatezza e sicurezza delle reti e delle informazioni, da attestarsi, in entrambi i casi, con apposita autocertificazione di assunzione di responsabilità come da fac-simile in allegato (*allegato 2*);

- La prestazione di lavoro agile si svolgeranno tenendo conto delle possibilità di accesso alle risorse di software e hardware garantite dal C4 e dall'ICT e che saranno comunicate a mezzo di apposite circolari;

- L'istituto del lavoro agile dovrà essere attivato in via prioritaria a favore dei lavoratori portatori di patologie che li rendono maggiormente esposti al contagio, dei lavoratori che si avvalgono di servizi pubblici di trasporto per raggiungere la sede lavorativa, e quelli sui quali grava la cura dei figli a seguito della contrazione dei servizi di asilo nido e della scuola dell'infanzia;

- Nell'ambito delle attività individuate dal Direttore/Dirigenti responsabili in cui è possibile l'attivazione dello *smart working* allo stesso deve essere data la più ampia applicazione possibile nei limiti di compatibilità con la continuità dello svolgimento dei servizi. Qualora, anche nell'ambito di queste attività, debba essere garantita una presenza minima del personale presso la sede, si potrà individuare un'alternanza di presenza in sede e di *smart working* per il personale interessato idonea a garantire l'osservanza delle misure di sicurezza e la funzionalità rispetto all'efficienza dei servizi, per le quali il dirigente responsabile o soggetto individuato dal Direttore dell'UP fornirà una programmazione utile agli aspetti di gestione del personale e della sicurezza.

- Lo *smart working* si svolge sotto la diretta responsabilità del Dirigente di riferimento o del soggetto coordinatore/responsabile individuato dal Direttore di ciascuna UP nell'ambito della

configurazione dell'assetto organizzativo di ogni Stabilimento o di altro assetto individuato dallo stesso Direttore ai sensi di quanto disposto nell'A.O. n. 5-2020. Il dirigente di riferimento o il soggetto coordinatore/responsabile dovrà coordinare e seguire il lavoro assegnato a ciascun lavoratore e attestarlo al fine della rendicontazione mensile delle presenze e anche ai fini dell'applicazione del sistema di misurazione e valutazione del personale in vigore presso l'Agenzia per il personale civile e per gli aspetti connessi alla valutazione del personale militare.

- Il personale civile delle aree funzionali e il personale militare cui si applica lo *smart working* dovrà garantire una fascia di attività e di reperibilità pari all'orario di lavoro previsto rispettivamente nel CCNL per il personale civile e nei vigenti DPR per il personale militare.

- L'attività di *smart working* dovrà avvenire nel rispetto della normativa sulla Privacy in particolare del GDPR e della normativa sulla documentazione classificata e/o riservata;

- L'ufficio del personale di ciascuna UP/DG procederà alle comunicazioni relative all'obbligo di informativa di cui all'art. 22 della legge 22 maggio 2017, n. 81 da assolvere in via telematica anche ricorrendo alla documentazione resa disponibile sul sito dell'Istituto nazionale assicurazione infortuni sul lavoro.

Per ulteriori informazioni utili relative all'applicazione dell'istituto del lavoro agile (*smart working*) è possibile far riferimento alla Direttiva del Presidente del Consiglio dei Ministri n. 3/2017.

Disposizioni sulla sicurezza dei lavoratori (Par. 6 Direttiva n. 3/2017 della PCDM-Dip. Funzione Pubblica, linee guida in materia di promozione della conciliazione dei tempi di vita e di lavoro)

- Preventivamente all'avvio dello *smart working* il datore di lavoro consegna al lavoratore un'informativa scritta, che il lavoratore firmerà per ricevuta, nella quale sono individuati i rischi generali e specifici connessi alla particolare modalità di esecuzione del lavoro (fac-simile in allegato 3).

Trattamento economico durante l'applicazione dello *smart working*.

- Il trattamento economico durante il periodo di applicazione dello *smart* working non subisce alcuna decurtazione né penalizzazione con riferimento alle progressioni economiche.

- Non è riconosciuto né trattamento di trasferta, né lavoro straordinario, non sono riconosciute altre protrazioni orarie, né permessi brevi o altri istituti che comportino riduzioni di orario.

- Nel caso di malattia, di permessi di cui alla l. 104 o di impossibilità di svolgere l'attività lavorativa per evenienze straordinarie il lavoratore in *smart working* dovrà prontamente comunicare per iscritto la circostanza impeditiva al dirigente responsabile/coordinatore e all'indirizzo mail indicato dall'Ente di appartenenza (per la Direzione Generale all'indirizzo ammpers.aid@aid.difesa.it).

Personale somministrato

- Per il personale in somministrazione per il quale il dirigente responsabile attesta la possibilità di lavoro in *smart working* deve essere effettuata apposita segnalazione alla soc. Osmosi a cura del responsabile dell'esecuzione contrattuale (DEC) di ciascuna UP/DG con riferimento

al periodo, alla residenza o domicilio presso il quale si svolge l'attività lavorativa e alle fasce orarie di svolgimento, al fine dell'attivazione di tutte le attività di competenza del datore di lavoro tra cui l'attivazione dell'assicurazione.

Disposizioni relative ai tirocini in corso presso la Direzione Generale e le Unità Produttive

Con riferimento ai tirocini in corso presso l'Agenzia per i quali è possibile al tirocinante, su espressa dichiarazione del Tutor di riferimento, completare il progetto formativo utilizzando modalità di comunicazione digitali, il periodo formativo potrà essere concluso permettendo al tirocinante di rimanere presso il proprio domicilio.

In tutti gli altri casi in cui il tirocinante debba necessariamente essere presente presso la sede della Direzione Generale e delle Unità Produttive i tirocini debbono essere sospesi con effetto immediato in ragione delle situazioni di emergenza in atto e fino al termine della stessa.

Fase transitoria

- In via eccezionale e transitoria, dovuta alla situazione di emergenza e di urgenza epidemiologica in atto, l'istituto dello *smart working* **potrà essere applicato fin da subito**, ***nel rispetto di tutte le condizioni sopra elencate*****,** nelle more di realizzazione delle attività di accesso completo alle risorse informatiche cui sta provvedendo l'Area strategica ICT della Direzione Generale.

- In questa fase ai lavoratori potranno essere assegnati dei compiti da poter svolgere presso la propria residenza/domicilio con i propri mezzi informatici e di comunicazione e, per consentire un collegamento con il Dirigente responsabile/soggetto coordinatore individuato dal Direttore dello Stabilimento *si potrà far uso anche della mail privata*, nel rispetto della normativa Privacy e nel rispetto dei limiti di trattamento dei dati classificati/riservati. Peraltro, con comunicazioni pervenuta in data 10 marzo da parte del Comando C4, l'accesso alla mail aid.difesa.it è possibile fin d'ora attraverso il portale "*webmail.difesa,it*" con l'avvertenza che l'accesso è da attivare preventivamente presso la sede di servizio di ciascun lavoratore, in quanto non è possibile l'attivazione da remoto. Si allega comunicazione C4 e relative istruzioni di attivazione (allegato 4).

IL DIRETTORE GENERALE
Ing. Gian Carlo ANSELMINO

COMUNICAZIONE DI AVVIO DI PRESTAZIONE LAVORATIVA IN LAVORO AGILE AI SENSI DEL D.L. 6/2020 E SUCCESSIVE DISPOSIZIONI ATTUATIVE.

1. In considerazione delle misure di emergenza previste dal decreto-legge n. 6/2020 e dei conseguenti decreti attuativi, DPCM 8 marzo 2020 e 9 marzo 2020, considerata la necessità di agevolare l'applicazione del lavoro agile (c.d. *smart working*) di cui agli artt. 18 e seguenti della legge 22 maggio 2017, n. 81, allo scopo di contrastare e contenere l'emergenza epidemiologica in atto a livello internazionale, come evidenziato dal Segretariato Generale della Difesa con note n. M_D GSGDNA REG2020 0017383 in data 5.3.2020 e M-D GSGDNA REG2020 0018289 del 9 marzo 2020, tenuto conto di quanto previsto dalla Direttiva n. 1/2020 della Presidenza del Consiglio dei Ministri – Ministro per la pubblica amministrazione e dalla Circolare n. 1/2020 della predetta Presidenza del Consiglio, nonché dell'Atto Organizzativo n. 5/2020 di Agenzia Industrie Difesa, si comunica che la S.V. *(indicare nominativo, profilo professionale, incarico),* a decorrere dal *(indicare la data),* svolgerà la propria prestazione lavorativa con le modalità del lavoro agile secondo le prescrizioni di seguito indicate.
2. L'attività cha la S.V. è tenuta ad effettuare in modalità di lavoro agile è la seguente:

   (descrizione sintetica dell'attività a cura del dirigente/responsabile individuato dal Direttore UP alle cui dirette dipendenze l'interessato presta servizio)

3. La predetta attività verrà svolta nel periodo di vigenza della legislazione di emergenza *(indicare la durata in relazione all'evolversi della situazione emergenziale ed alle esigenze del lavoratore)* ed avrà la seguente articolazione: *(indicare se giorni continuativi o giorni a settimana, agevolando chi rientra nelle categorie indicate nella circolare n. 1/2020 del Ministro della pubblica amministrazione, secondo le valutazioni del dirigente).*

4. La S.V. svolge la prestazione lavorativa in modalità di lavoro agile fuori dalla sede di servizio esclusivamente presso la propria residenza o il proprio domicilio, se non coincidenti, qui di seguito indicato (*indicare indirizzo e numero di telefono*) rendendosi inoltre disponibile ad essere contattato dall'Ufficio di appartenenza nelle seguenti fasce orarie *(indicare periodi di contattabilità).*

5. Nel caso di malattia, di permessi di cui alla l. 104 o di impossibilità di svolgere l'attività lavorativa per evenienze straordinarie il lavoratore in *smart working* dovrà prontamente comunicare per iscritto la circostanza impeditiva al dirigente responsabile/coordinatore e all'indirizzo mail indicato dall'Ente di appartenenza (per la Direzione Generale all'indirizzo ammpers.aid@aid.difesa.it – *indicare altro indirizzo o contatto di riferimento di ciascuna UP*).

6. Nel caso in cui la strumentazione informatica non venga fornita dall'amministrazione o sia insufficiente, la S.V. è autorizzata ad utilizzare propri dispositivi informatici, secondo i principi già fissati nel Regolamento del Ministero della difesa in materia di sperimentazione dello *smart working*, adottato in data 8 ottobre 2018, garantendo adeguati livelli di sicurezza e protezione della rete come da dichiarazione di assunzione di responsabilità *(v. allegato 2)*

Digitally signed by GIAN CARLO ANSELMINO
Date: 2020.03.11 15:16:10 CET

e da successive disposizioni dei responsabili ICT e C4-Difesa, ai sensi di quanto previsto dalla Circolare n. 1/2020 della Presidenza del Consiglio dei Ministri sopra menzionata.

7. Il lavoro agile di cui al presente atto viene svolto in ottemperanza alle norme vigenti in materia e nel rispetto della disciplina contenuta nel CCNL Comparto Funzioni Centrali 12.2.2018, del d.P.R. 16 aprile 2013, n. 62, "Regolamento recante codice di comportamento dei dipendenti pubblici" e del d.M. 29.1.2014, recante "Codice di comportamento dei dipendenti del Ministero della Difesa". Pertanto, ogni condotta contraria alle disposizioni testé richiamate o in contrasto con le prescrizioni di cui al presente atto, determina la revoca dell'autorizzazione allo svolgimento della prestazione lavorativa in modalità lavoro agile ed il conseguente ripristino degli obblighi di espletamento della prestazione medesima nella sede di servizio. Per il personale militare valgono le analoghe disposizioni contenute nei vigenti regolamenti in materia.

8. La S.V. non subisce alcuna decurtazione sul trattamento economico spettante nei giorni/periodi di lavoro prestato in modalità di lavoro agile, né penalizzazioni con riguardo alle progressioni economiche. In relazione allo svolgimento del lavoro agile, non è riconosciuto il trattamento di trasferta e non sono configurabili prestazioni di lavoro straordinario, protrazioni dell'orario di lavoro aggiuntive né permessi brevi ed altri istituti che comportino riduzioni di orario. Nelle giornate di attività svolte in lavoro agile non viene altresì erogato il buono pasto.

9. Durante il periodo di lavoro agile, la S.V. deve custodire con diligenza dati e strumenti informatici eventualmente messi a disposizione dall'Amministrazione ed è tenuto al rispetto degli obblighi di riservatezza di cui al d.PR n. 62/2013 e al d.M. 29.1.2014 sopra citati nella trattazione della documentazione di cui viene in possesso in ragione dell'attività svolta.

10. Per quanto concerne l'osservanza delle disposizioni in materia di sicurezza sul luogo di lavoro la S.V. è invitata a prendere piena cognizione dell'informativa in materia che le viene consegnata contestualmente alla firma per accettazione della presente comunicazione e, per tutto quanto non espressamente previsto in essa e nel presente atto, si rinvia alla comunicazione pubblicata dall'Istituto Nazionale Assicurazioni e Infortuni sul Lavoro (INAIL) sul proprio portale telematico.

11. La S.V. autorizza al trattamento dei propri dati personali ai sensi del D.Lgs. n. 196/2003, come modificato e integrato dal D.lgs. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679", per le finalità connesse all'espletamento dell'attività di lavoro agile ai sensi del presente atto.

Luogo e data, IL DIRETTORE GENERALE/IL DIRETTORE DELLA UP

Per accettazione:
IL LAVORATORE

Allegato C

_____**Timbro Lineare**

MODULO DI ASSUNZIONE DI RESPONSABILITÀ

Il sottoscritto[1] ..... n servizio presso _____,[2]
con l'incarico di ……., telefono ufficio…… , assegnatario della casella di posta elettronica dell'Amministrazione Difesa[3]……@_____.difesa.it

dichiara di essere a conoscenza che:

a) i privilegi di amministrazione del PC affidatogli dall'A.D. sono detenuti dall'A.D. stessa che, per esercitarli, può assegnare specifiche credenziali di amministrazione ad un Referente Informatico Locale od amministratore locale. Come tale, questi può, pertanto, aver accesso ai file prodotti/archiviati sul PC;
b) il PC affidatogli dall'A.D. 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;
c) le credenziali (*username* e *password*) di accesso devono essere custodite e mantenute strettamente riservate e non devono essere condivise con altri utenti;
d) non è consentito detenere dati personali sui dispositivi in dotazione;
e) l'indirizzo di posta elettronica (*e-mail*) assegnatogli, ancorché possa essere articolato sulla base del nome e del cognome dell'utente, non ha caratteristiche di privatezza, ma costituisce strumento di lavoro finalizzato esclusivamente all'assolvimento dei compiti istituzionali; ne è, pertanto, vietato l'utilizzo per scopi personali[4]. L'assegnatario è tenuto ad informare di tale caratteristica i terzi a cui comunica il citato indirizzo *e-mail*;
f) gli apparati di sicurezza (ad es. i *firewall* ed IDS) e di filtraggio della posta indesiderata (ad es. *firewall-antispam*) analizzano costantemente ed in modo autonomo ed automatico il traffico *internet* e della posta elettronica per garantire la sicurezza perimetrale dei sistemi;
g) deve dare comunicazione immediata all'Ente Tecnico che ha rilasciato le credenziali, dell'eventuale perdita di riservatezza della *password* e al Capo Ufficio/Servizio della eventuale cessazione di utilizzo della rete;
h) è vietato immettere, trasmettere, diffondere qualsiasi materiale che non può essere distribuito legalmente via rete telematica (**vedere disposizioni di legge di seguito indicate**);
i) è vietato modificare la configurazione del PC in dotazione. Qualsiasi esigenza particolare dovrà essere rappresentata con comunicazione formale secondo le procedure in vigore;
j) le disposizioni legislative sulla tutela giuridica del *software* considerano i programmi per elaboratore alla stregua di opere letterarie protette dalle vigenti leggi in materia;
k) 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;

Firma per accettazione[5]

_____

[1] Grado/qualifica, cognome e nome.
[2] Ufficio dove si presta servizio.
[3] Indicare l'indirizzo di posta elettronica funzionale di reparto.
[4] è vietato, pertanto, utilizzare le caselle di posta elettronica istituzionali (personali e funzionali) ed i relativi indirizzi *e-mail*, per registrarsi su siti/servizi *Internet* (fra cui i *Social Network*, i servizi *e-commerce*, etc.) non erogati dall'A.D., ovvero da *providers* di servizi (pubblici o privati) che eserciscono i medesimi per conto della stessa A.D., a meno di eventuali deroghe concesse per esigenze esclusivamente legate ad attività di istituto.
[5] Da apporre anche sulla seconda pagina.

Digitally signed by GIAN CARLO ANSELMINO
Date: 2020.03.11 15:16:10 CET

l) chiunque duplichi abusivamente *software* protetto da *copyright* e lo venda/distribuisca per scopi commerciali, è soggetto alla pena prevista dalla vigente legislazione. Quanto detto vale anche per 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;
m) il prelevamento dalla rete (*download*) di opere protette dal *copyright* (musiche, filmati, programmi,…) non è consentito a nessun titolo ed è soggetto a sanzione in conformità dalle vigenti leggi;
n) la detenzione sul proprio elaboratore di contenuti pedo-pornografici è vietata e soggetta a sanzione in conformità alle vigenti leggi;
o) non sono consentite azioni tendenti a nascondere la propria identità, a molestare o arrecare danno sull'attività degli elaboratori di altri utenti o ad acquisire dati/informazioni/privilegi a cui non si ha diritto;
p) è fatto assoluto divieto di trattare informazioni classificate con materiali o attrezzature ICT che non siano configurate in accordo al Capo VII "Sicurezza dei Communication and Information System – CIS" del DPCM 6 novembre 2015 "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva (Decreto 5/2015)".
q) nel caso di utilizzo di mezzi propri in applicazione dello smart working il sottoscritto si atterrà alle stesse disposizioni di cui alle lettere precedenti.

Qualsiasi inadempienza a quanto dichiarato nel presente documento provocherà l'immediata sospensione del servizio rete *internet*. L'Ente Tecnico può interrompere il servizio prestato al sottoscritto anche solo per palese violazione del *"Disciplinare interno all'Amministrazione Difesa sull'utilizzo dei servizi informatici non classificati erogati in ambito Difesa, quali i servizi di POSTA ELETTRONICA, ISTANT MESSAGING, ed accesso ad INTERNET"*.

Si riportano per opportuna informazione, le normative che regolano l'argomento oggetto del presente modulo:

- Netiquette, "galateo di *internet*";
- D.L. 27 luglio 2005, n. 144, convertito con modificazioni dalla L. 31 luglio 2005, n. 155, recante: "*Misure urgenti per il contrasto del terrorismo internazionale*";
- D.L. 196 in data 30/06/2003, codice di protezione dei dati personali;
- D.P.R. 28 dicembre 2000, n. 445 recante: "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*";
- Legge 22 aprile 1941, n. 633 recante: "*Protezione del diritto di autore e di altri diritti connessi al suo esercizio*", con particolare riferimento all'art. 1, comma 1-bis da ultimo modificato con D.Lgs. 6 maggio 1999, n. 169;
- Decreto legislativo 10 febbraio 225, n. 30 recante: "Codice della proprietà industriale, a norma dell'articolo 15 della legge 12 dicembre 2002, n. 273";
- Art, 615 *ter* e seguenti del Codice Penale in merito all'accesso abusivo ad un sistema informatico o telematico;
- Decreto legislativo 7 marzo 2005, n. 82 recante: "Codice dell'Amministrazione Digitale" (CAD)";
- Provvedimento del Garante per la protezione dei dati personali 27 novembre 2008, "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", modificato con provvedimento del 25 giugno 2009, "*Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento"*;
- DPCM 6 novembre 2015 n 15 recante: "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva.

I dati riportati in questo modulo saranno utilizzati dall'EDR, titolare del trattamento degli stessi, nel rispetto del D.Lgs. 30/06/2003 n. 196.

Roma _____

Firma per accettazione

_____

Informativa per l'anno 2020 su salute e sicurezza nel lavoro agile

ai sensi dell'art. 22, comma 1, L. n. 81/2017 e ai sensi Par. 6 Direttiva n. 3/2017 della PCM-Dip. Funzione Pubblica, "Linee guida in materia di promozione della conciliazione dei tempi di vita e di lavoro.

• Ragione sociale dell'impresa: AID - CCNL applicato:_____

• Nome e cognome del lavoratore:

• Accordo del: …… - (eventuale) Policy per la gestione del lavoro agile del:

• Nome e cognome dell'RLS: …….

• Nome e cognome dell'RSPP: Enrico Romano

Si specifica il lavoro agile è inteso come modalità di esecuzione del rapporto di lavoro subordinato:

• stabilito mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro;

• con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa;

• eseguita, in parte all'interno di locali dell'amministrazione e in parte all'esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva

Rischi generali

In relazione alle attrezzature consegnate si evidenziano i seguenti rischi:

✓ Rischio elettrico

✓ Rischio incendio

✓ Radiazione ottiche non ionizzanti

Assicurarsi visivamente del buono stato della presa e dei cavi che si utilizzano.

Non mangiare né bere nei pressi della postazione della macchina. Utilizzare solo materiali elettrici marchiati CE. Non manomettere il PC. Non aprire il PC né modificarne la configurazione Hardware. Non utilizzare pennette USB/Storage Disk che non siano stati previamente autorizzati. Segnalare ogni anomalia del PC, sia hardware che software. Se possibile avvalersi di una unità di continuità omologata.

In caso di incendio DIVIETO ASSOLUTO DI UTILIZZARE L'ACQUA. Se a disposizione, utilizzare **un estintore a polvere** se addestrati e formati per tale attività. In caso contrario o se non si riuscisse ad estinguere comporre il numero telefonico 115 per contattare i VV.FF.

Nell'uso del videoterminale, rispettare almeno le prescrizioni e/o le limitazioni imposte dal Medico Competente per (es. pause frequenti, lenti in uso…). Tenere a disposizione i manuali di uso delle macchine anche eventualmente in formato digitale.

Digitally signed by GIAN CARLO ANSELMINO
Date: 2020.03.11 15:16:10 CET

Il Lavoro Agile sarà svolto con macchine marchiate CE, conformi al Titolo III del d.lgs. 81/2008 nonché alle specifiche disposizioni legislative e regolamentari di recepimento delle Direttive comunitarie di prodotto, connesse con la rete della Difesa o con macchine di proprietà dei lavoratori **(modalità per cui comunque si applicano le misure di tutela di cui all'articolo 15 del d.lgs. 81/2008**).

Le macchine (pc portatili) che saranno consegnate, o che sono già state consegnate, saranno previamente configurate secondo le policy di cyber-sicurezza del C4S e da esse sarà possibile connettersi alla VPN Citrix per accedere ai servizi richiesti. Le macchine registreranno gli orari di accesso e disconnessione dell'utente per la verifica della presenza e relativo computo della prestazione in termini di ore lavorate.

Data la riservatezza dei dati trattati e in relazione obblighi normativi emessi dalla Presidenza del Consiglio dei Ministri in relazione all'emergenza COVID 19, è OBBLIGATORIO svolgere l'attività di lavoro agile **DA CASA**. Almeno fino al termine della richiamata emergenza, è fatto espresso divieto del lavoro outdoor.

Rischi specifici connessi alla particolare modalità di esecuzione del rapporto di lavoro

In relazione alle modalità esecutiva da remoto i rischi connessi all'espletamento della mansione di Videoterminalista con le attrezzature descritte sono connessi a:

✓ Radiazioni elettromagnetiche

✓ Microclima

✓ Posture incongrue

✓ Layout e postazione di lavoro

✓ Illuminazione

• Rischi legati ai comportamenti: adottare comportamenti adeguati rispetto alla mansione lavorativa da compiere in modalità agile, rispettare procedure e istruzioni: evitare il disordine e le distrazioni, fare le pause dall'uso del PC dopo 2 ore lavorative continuate, adottare una postura corretta, non dondolarsi sulla sedia;

• Scelta da parte del lavoratore del luogo idoneo per la prestazione lavorativa secondo i criteri illustrati nei corsi di formazione erogati al personale e comunque rispondenti ai criteri delle postazioni (es. scegliere luoghi con illuminazione adeguata, evitare i riflessi sul monitor, scegliere luoghi con clima, livello di umidità e ricambio d'aria adeguati, evitare sbalzi termici ecc.) come anche da opuscolo INAIL allegato;

• Rischi legati all'uso di strumenti ed attrezzature di lavoro di comunicazione: in funzione di come si

realizza la connessione si può essere esposti a radiazioni elettromagnetiche:

La valutazione del rischio risulta in ogni caso bassa come da seguente tabella:

	Probabilità	Danno	Rischio grezzo	Azioni di Prevenzione e Protezione	Rischio Residuo
Cavo + Router/Modem	1	1	1	Materiale marcato CE Informativa	1
Wireless + Router/Modem	2	1	2	Materiale marchiato CE Informativa	1
Wireless + Hotspot telefono	2	2	4	Materiale marchiato CE Informativa	2
Wireless + Saponetta	2	2	4	Materiale marchiato CE Informativa	2

Data di consegna:

Modalità di consegna dell'informativa definita dall'azienda: cartacea o mail.

Il lavoratore dichiara di ricevere la presente informativa ai sensi di legge, di attenersi diligentemente ai comportamenti indicati nella stessa nonché nell'accordo sottoscritto e di cooperare, secondo quando impartito nell'ambito del corso di formazione frequentato, all'attuazione delle misure di prevenzione predisposte dal datore di lavoro, anche secondo quanto disposto dall'art. 20 del D.Lgs. n. 81/2008.

Firma del ricevente

Nominativo:

_____

M_D GAID REG2020 0002682 11-03-2020

Da: c4info
Inviato: martedì 10 marzo 2020 12:14
Oggetto: Piattaforma CITRIX
Allegati: ATT00001.bin; documentazione_otp.pdf

LABOR OMNIA VINCIT

Gentile utente,
per consentire le attività di Smart Working previste dal DPCM n. 59 dell'8 marzo 2020 è necessario che l'utenza applichi le seguenti modalità d'accesso:

- per consultare le e-mail, digitare https://webmail.difesa.it direttamente nella barra indirizzi del browser del proprio PC / tablet / smartphone (non è necessario accedere alla piattaforma Citrix, evitare di avanzare richieste di accesso alla piattaforma in titolo se l'esigenza è solamente questa);
- per consultare Adhoc, è necessario accedere a https://virtual.difesa.it, previa autorizzazione all'uso della piattaforma Citrix;
- per chi fosse sprovvisto di Token di autenticazione, si allega la procedura per la creazione dello stesso (utilizzabile per entrambe le piattaforme);
- inoltre è stata inibita la "navigazione Open" da piattaforma Citrix ai client che si presentino da collegamento commerciale domestico nazionale.

Si stanno ponendo in essere tutte le attività atte a potenziare il servizio in oggetto e minimizzare i disagi che il massiccio ricorso allo stesso sta provocando.

Digitally signed by GIAN CARLO ANSELMINO
Date: 2020.03.11 15:16:10 CET

Si prega di non rispondere a questa e-mail ma in caso di necessità contattare il Call Desk ai seguenti recapiti:

Please, do not reply to this mail. In case of emergency, contact the helpdesk at:

(Mil: 2024444)

(Civ: 0646914444)

Il testo e gli eventuali documenti trasmessi contengono informazioni riservate al destinatario indicato. La seguente email è confidenziale e la sua riservatezza è tutelata legalmente dalla legge 196/03. La lettura, copia od altro uso non autorizzato o qualsiasi altra azione derivante dalla conoscenza di queste informazioni sono rigorosamente vietate. Se pensi di non essere il destinatario di questa mail, o se hai ricevuto questa mail per errore, sei pregato di darne immediata comunicazione al mittente e di provvedere immediatamente alla sua distruzione. Questo messaggio rappresenta l'opinione del mittente e non necessariamente l'opinione dell'Amministrazione Difesa.

This E-mail is confidential and is intended for the exclusive attention of the addressees indicated. If you are not the intended recipient, this E-mail should not be read or disclosed to any other person. Please notify the sender immediately and delete this E-mail from your computer system. Although this E-mail has been checked for viruses and other defects, no responsibility can be accepted for any loss or damage arising from its receipt or use.

Prima di stampare questa comunicazione consideratene l'impatto ambientale.

COMANDO C4 DIFESA

Guida all'utente per la creazione del Token One Time Password (OTP) e all'accesso WEBMAIL

INDICE

1. PREMESSA pag. 3
2. INSTALLAZIONE DEL GENERATORE DI CODICI pag. 4
3. ATTIVAZIONE TOKEN pag. 5
4. ACQUISIZIONE QR Code pag. 7
5. CREAZIONE PIN pag. 8
6. CANCELLAZIONE TOKEN pag. 9
7. RESET/CAMBIO PIN pag. 9
8. ACCESSO AL SERVIZIO WEBMAIL CON OTP pag. 10

1. PREMESSA

a. Sicurezza e comodità: significato e funzionalità del codice OTP

Riuscire a garantire la massima sicurezza di accesso oggi è diventata una priorità, non solo per l'uso delle carte di credito, o la gestione dei conti correnti tramite home banking, ma anche per la posta elettronica. Per questo motivo il Comando C4 Difesa per consentire l'utilizzo di Outlook Web Access (OWA) in modo sicuro ha introdotto un secondo fattore di autenticazione (codice OTP), ovvero un codice alfanumerico, generato da un algoritmo che crea una serie casuale di numeri, utilizzabili solo dal titolare dell'utenza opportunamente registrato.

b. Come funziona il codice?

L'acronimo OTP sta a indicare la One Time Password, ovvero una password usa e getta, dove il codice viene generato "al bisogno" dall'apposita App messa a disposizione sul Play Store di Google o App Store di Apple.

La presente guida ha lo scopo di seguire l'utente passo dopo passo nella fase di *Enrollment* (registrazione) del Token Software sul proprio dispositivo Mobile con sistema operativo Android o IOS (non disponibile per Windows Phone).

2. INSTALLAZIONE DEL GENERATORE DI CODICI

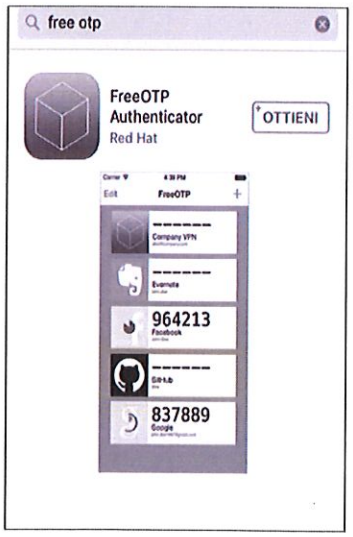
E' necessario installare l'App FreeOTP Authenticator qualora non già presente sul dispositivo mobile.

a. Dispositivi Android

Collegarsi al PLAY STORE inserire nel campo di ricerca il testo "FreeOTP Authenticator" ed installare l'App.

b. Dispositivi IOS

Collegarsi al APPLE STORE inserire nel campo di ricerca il testo "FreeOTP Authenticator" e installare l'App.

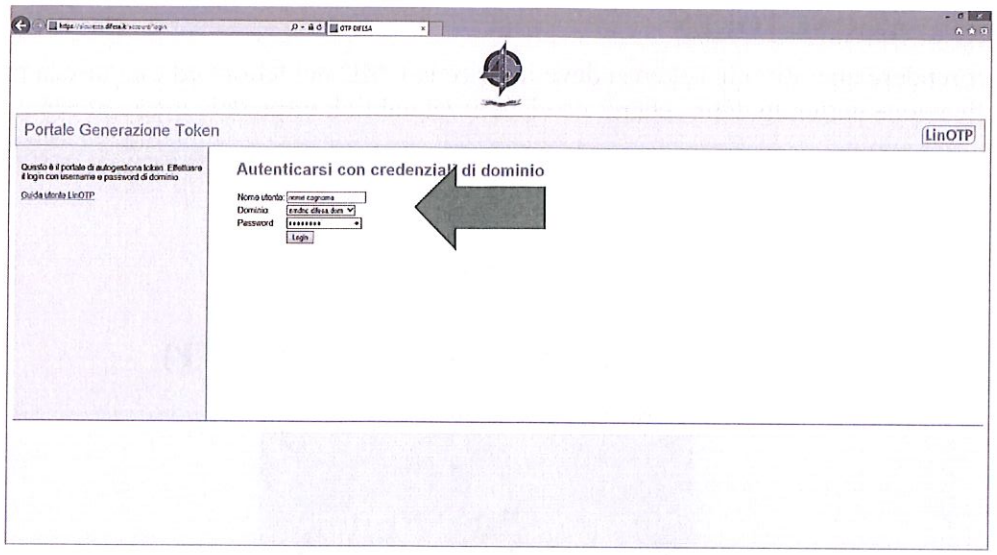


3. ATTIVAZIONE TOKEN

Per rendere operativo il Token si deve inserire la CMD nel lettore ed eseguire la procedura di attivazione partendo dalla schermata visualizzata al link **https://sicurezza.difesa.it**:

a. cliccare su **Log-In;**

b. inserire il **PIN Carta** della propria CMD e cliccare su OK;

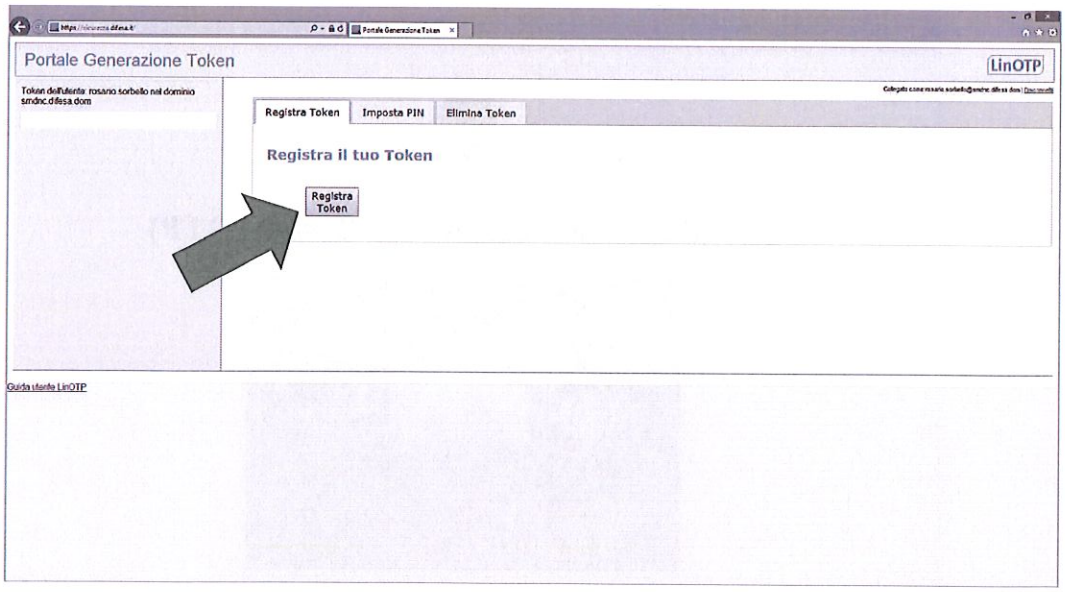


c. inserire le proprie credenziali nome utente e password di dominio nei seguenti campi:

- **nome utente:** inserire il nome utente con cui si accede alla webmail (es. nome.cognome);
- **dominio: selezionare il dominio di appartenenza;**
- **password: inserire la** propria password;

d. cliccare su **Login**;

e. si aprirà la seguente pagina dove sarà possibile generare il QR Code



f. cliccare su **Registra Token**;

g. verrà visualizzato il QR Code, ovvero un'immagine del seguente tipo contenente le specifiche del token che dovrà essere acquisito dal proprio dispositivo Mobile.

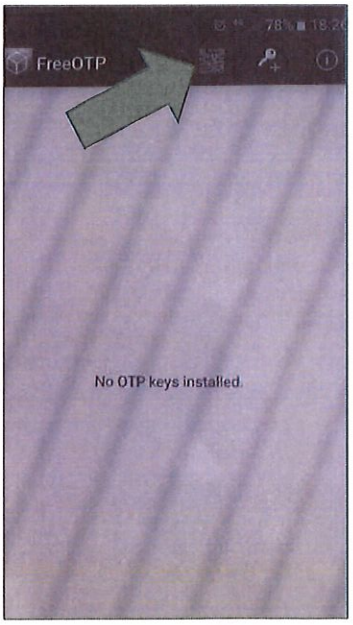
4. ACQUISIZIONE QR Code

Per acquisire il QR Code è necessario utilizzare FreeOTP Authenticator.

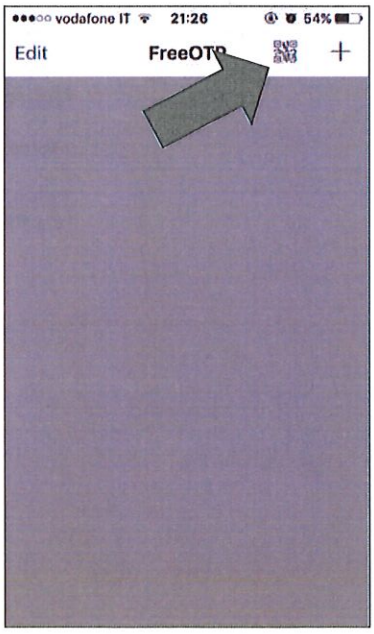
Nota: per acquisire il QR Code sui dispositivi Android, se richiesto dal dispositivo, è necessario consentire all'App di accedere alla fotocamera.

(1) Avviare l'App;

(2) cliccare sull'icona con l'immagine del QR Code;



(S.O. Android)



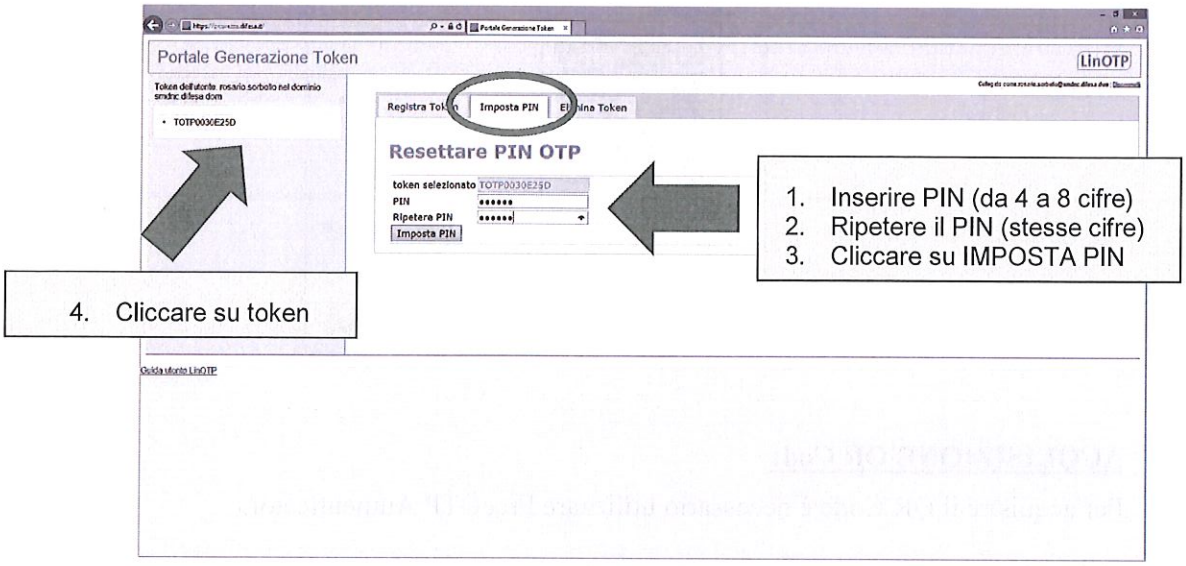
(S.O. IOS)

(3) inquadrare con il dispositivo il QR Code visualizzato e attendere acquisizione.

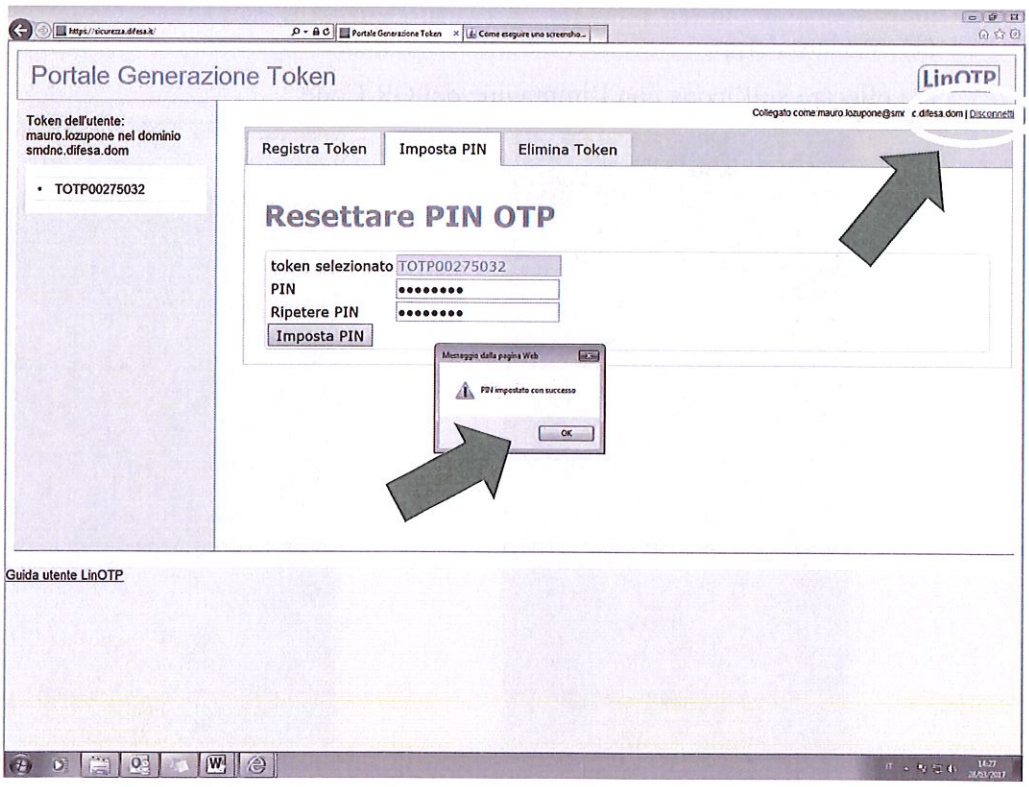
5. CREAZIONE PIN

Per poter accedere al servizio di posta elettronica via web è necessario impostare un PIN seguendo le seguenti procedure:

a. Cliccare su **Imposta PIN** (vds. ellisse color rosso) e si aprirà la seguente schermata e procedere come indicato:



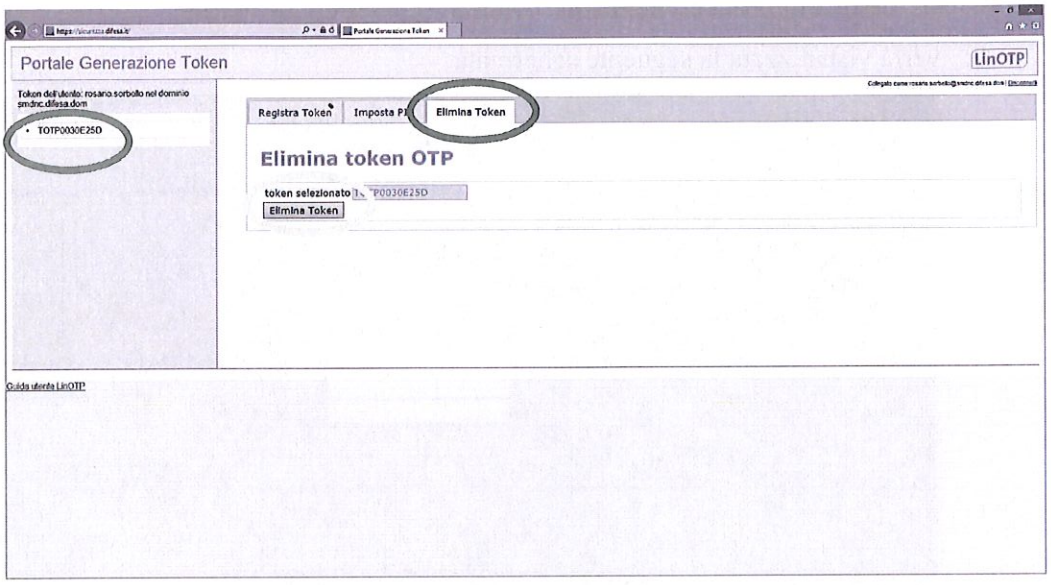
b. Al termine cliccare su **OK** e successivamente per uscire dal "portale LinOtp" cliccare **DISCONNETTI** (vds. ellissi gialla).



6. CANCELLAZIONE TOKEN

Qualora per qualsiasi motivo (es. processo di creazione non portato a termine, cancellazione involontaria dell'app, etc..) si vuole eliminare il token dal portale, si deve procedere con la seguente procedura:

a. inserire la propria CMD nel lettore Smart Card e ripetere la procedura da a.-d del paragrafo 3;



b. cliccare su **Elimina Token** (vds. ellisse color rosso);

c. cliccare sul **token** che si trova in alto a sinistra (vds. ellisse color verde) e lo stesso sarà visualizzato in **Token selezionato;**

d. cliccare su **Elimina Token** (vds. ellisse color giallo).

7. RESET/CAMBIO PIN

Qualora sia necessario cambiare il PIN del token, seguire la seguente procedura:

a. inserire la propria CMD nel lettore Smart Card e ripetere la procedura del paragrafo 3. dal sottopara. a. al d.;

b. cliccare su **Imposta PIN** e ripetere la stessa procedura utilizzata al paragrafo 5.

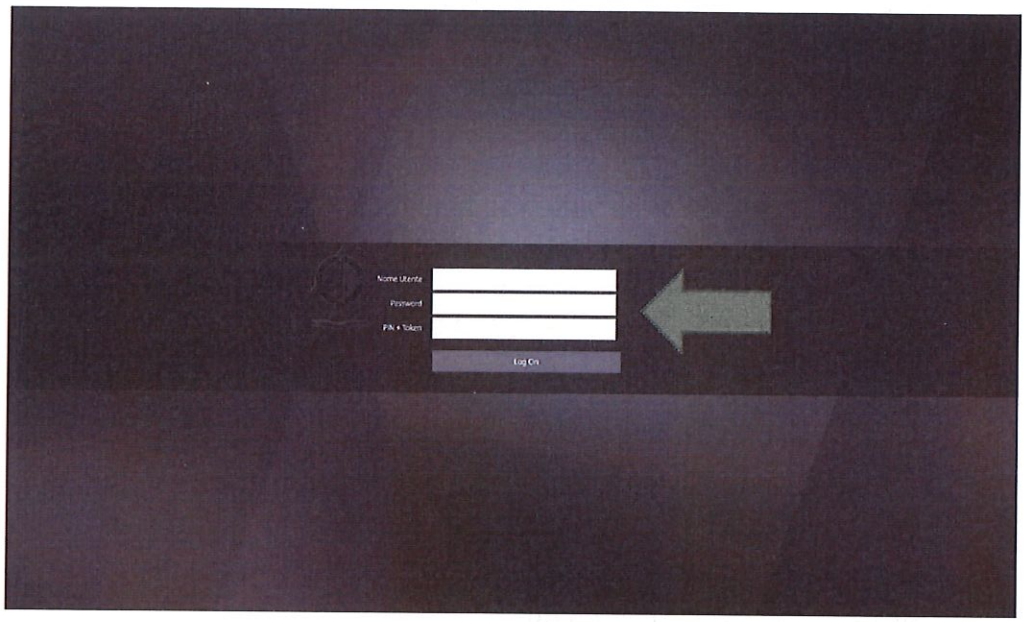
8. ACCESSO AL SERVIZIO WEBMAIL con OTP

Per accedere alla posta elettronica via web seguire le seguenti procedure:

a. avviare il browser e digitare l'indirizzo:

- casella di posta istituzionale: **https://webmail.servizi.difesa.it**;
- casella di posta civile: **https://webmail.persociv.difesa.it**;

b. verrà visualizzata la seguente schermata



c. inserire le credenziali dell'utente come di seguito indicato:

- **nome utente:** inserire il nome utente con cui si accede alla webmail seguito dal dominio (es. nome.cognome@domini.difesa.dom);
- **password:** inserire la password;
- **PIN+TOKEN:** inserire il PIN (creato con procedura al para. 5) seguito dalle cifre visualizzate sull'App FreeOtp.