Consiglio regionale della Calabria

Disciplinare per l’utilizzo dei servizi e degli strumenti informatici

SOMMARIO

Introduzione

Il presente disciplinare mira a definire, da un lato, procedure per l'assegnazione degli strumenti e per l'erogazione dei servizi informatici messi a disposizione dal Consiglio regionale della Calabria, dall'altro, principi e disposizioni per un migliore utilizzo degli stessi da parte dell'utente, che ne diventa custode e responsabile.

Ciò, soprattutto, per prevenire usi arbitrari degli strumenti informatici o comportamenti inconsapevoli che possano mettere a rischio la sicurezza dei sistemi e dei dati trattati, nel rispetto, però, dei limiti posti della vigente disciplina in materia di riservatezza (D.lgs. 196/2003 e Regolamento UE 2016/679) e di controllo sul lavoratore da parte dei soggetti pubblici (art. 4, secondo comma, dello Statuto dei lavoratori).

Il suo ambito di applicazione risulta particolarmente esteso, essendo sottoposti alle sue prescrizioni tutti i soggetti autorizzati, a qualsiasi titolo, all'utilizzo degli strumenti e all'accesso ai servizi informatici messi a disposizione dal Consiglio.

Si fa riferimento, a titolo meramente esemplificativo e non esaustivo, non solo ai dipendenti pubblici in servizio presso l'Ente, ma pure al presidente del Consiglio, ai consiglieri, agli assessori, a svariate figure istituzionali, al personale in forza presso le strutture speciali consiliari e presso i gruppi politici, ai dipendenti della società in house, ai fornitori e loro dipendenti e, in definitiva, a tutti i soggetti che utilizzano strumenti e servizi informatici comunque assegnati e/o erogati dal Consiglio regionale della Calabria.

Si tratta, quindi, di un documento di fondamentale importanza per il funzionamento della macchina amministrativa consiliare, che tutti gli utenti, per quanto di rispettiva competenza, sono tenuti a rispettare e a fare rispettare.

Contesto normativo

La redazione del disciplinare è avvenuta sulla base dei principali riferimenti normativi di seguito indicati:

- Codice penale (Regio decreto 19 ottobre 1930, n. 1398), con particolare riferimento ai reati informatici
- Codice civile e, in particolare, articoli 2086, 2087 e 2104, in tema di poteri del datore di lavoro sulla verifica della corretta prestazione lavorativa e sull'utilizzo degli strumenti di lavoro
- Costituzione italiana e, in particolare, articoli 2 e 15, in tema, rispettivamente, di inviolabilità dei diritti dell'uomo e di libertà, nonché di segretezza della corrispondenza e di ogni altra forma di comunicazione;
- L. 300/1970 (Statuto dei lavoratori) e, in particolare, articoli 4, 7 e 8;
- D. lgs. 165/2001 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche) e, in particolare, il suo Titolo IV;
- D. lgs. 196/2003 (Codice in materia di protezione dei dati personali);
- D. lgs. 82/2005 (Codice dell'amministrazione digitale);
- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento:
  - Lavoro: le linee guida del Garante per posta elettronica e internet;

- Rifiuti di apparecchiature elettriche ed elettroniche (RAAE) e misure di sicurezza dei dati personali - 13 ottobre 2008;
- Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori;

- D. lgs. 81/2008 (Testo unico sulla sicurezza);
- Direttiva n. 2/2009 della Presidenza del Consiglio dei ministri sul corretto utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro;
- D.P.R. 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione);
- Regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014;
- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR);
- Circolare AgID 18 aprile 2017, n. 2/2017 "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».".

Il disciplinare è stato redatto, altresì, in ossequio a:

- Codice calabrese del buon governo, approvato con deliberazione del Consiglio regionale n. 49 del 6 dicembre 2005;
- Regolamento consiliare per il trattamento dei dati personali sensibili e giudiziari;
- Codice disciplinare personale Dirigente del Comparto Regioni e Autonomie locali;
- Codice disciplinare personale non Dirigente del Comparto Funzioni locali;
- Disciplinare per lo svolgimento dell'attività lavorativa in modalità agile, sottoscritto in sede di delegazione trattante in data 27 gennaio 2022 e, in particolare, da pag. 210 a pag. 215;
- CCNL Funzioni locali, sottoscritto il 16 novembre 2022;
- Social Media policy, approvata con deliberazione dell'Ufficio di Presidenza n. 85 del 19 dicembre 2022;
- Codice di comportamento dei dipendenti del Consiglio regionale della Calabria, approvato con deliberazione dell'Ufficio di Presidenza del Consiglio regionale n. 93 del 29 dicembre 2022.

TITOLO I
Disposizioni generali

Art. 1
(Finalità)

1. Il Consiglio regionale della Calabria, nell'espletamento della sua attività istituzionale, opera prestando la massima attenzione alla sicurezza del proprio sistema informativo e adottando adeguate misure tecnologiche e organizzative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni, sia a proteggere le informazioni gestite.

2. Per le finalità di cui al comma 1, il presente disciplinare definisce:

a) le regole per l'accesso e l'utilizzo dei servizi e degli strumenti informatici del Consiglio regionale della Calabria, onde garantire disponibilità, integrità e riservatezza dei dati e dei documenti, da parte dei dipendenti pubblici e di tutti i soggetti che, in virtù di un rapporto di lavoro a qualsiasi titolo, li utilizzano, di seguito denominati utenti;
b) le procedure di attivazione, gestione e disattivazione delle credenziali per l'accesso ai sistemi informatici e ai servizi informatici erogati dall'Ente;
c) l'ambito, le modalità e i limiti del monitoraggio e dei controlli attuabili dall'Ente nel rispetto della normativa vigente;
d) le responsabilità degli utenti in caso di inosservanza di regole e prescrizioni.

Art. 2
(Principi generali)

1. Gli strumenti informatici sono assegnati agli utenti al solo fine dello svolgimento dell'attività lavorativa e/o istituzionale e delle attività comunque autorizzate dall'Ente. Essi devono essere utilizzati con le modalità prescritte dal presente disciplinare, anche nel rispetto del Codice di comportamento dei dipendenti della pubblica amministrazione e della normativa vigente in materia.

2. Gli utenti, pertanto, sono sottoposti ai seguenti obblighi generali:

a) custodire con diligenza gli strumenti informatici loro affidati, segnalando tempestivamente alle strutture preposte, secondo le modalità previste, ogni danneggiamento, smarrimento o furto;
b) non consentire l'utilizzo degli strumenti informatici in custodia a soggetti estranei alle attività dell'Ente, salvo che non siano autorizzati, a qualsiasi titolo, dallo stesso;
c) mantenere la riservatezza sulle informazioni e sui dati personali di cui vengono a conoscenza durante lo svolgimento della propria attività, anche dopo la cessazione del rapporto con l'Ente;
d) adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati e ogni altro pregiudizio per l'amministrazione;
e) garantire la corretta custodia di atti e documenti.

3. Non è consentito all'utente l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere alle incombenze personali, salvo che l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

Art. 3
(Definizioni)

1. Ai sensi del presente disciplinare, si intende per:

a) **Strumenti informatici**: personal computer fissi o portatili, stampanti locali o di rete, programmi e prodotti software, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc.);
b) **Servizi informatici:** servizi necessari all'utilizzo degli strumenti informatici (es.: connettività, internet, linee telefoniche, servizi di assistenza, posta elettronica, servizi di firma digitale, etc.);
c) **Sistema informativo:** l'insieme degli strumenti e dei servizi informatici;
d) **Utente:** soggetto autorizzato a qualsiasi titolo all'utilizzo degli strumenti e all'accesso ai servizi informatici messi a disposizione dall'Ente (personale dipendente, personale comandato da altre pubbliche amministrazioni, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni, ospiti, etc.);
e) **Utenza istituzionale**: insieme delle informazioni di profilazione (identificativo, credenziali di autenticazione, autorizzazioni, etc.) associate ad articolazioni organizzative (es.: settore.risorseumane@consrc.it), organi (es.: presidente@consrc.it, etc.) e organismi consiliari, nonché alle diverse figure istituzionali presenti nel Consiglio regionale (es.: garante.infanzia@consrc.it);
f) **Postazione di lavoro (PDL):** personal computer (desktop o portatile) e periferiche a corredo (es.: scanner, stampante, casse, cuffie, mouse, tastiera e monitor, pendrive, hard disk esterni, etc.) messi a disposizione dell'utente dall'Ente per l'espletamento dell'attività lavorativa e/o istituzionale;
g) **Postazione remota di lavoro:** ogni PDL collocata al di fuori delle sedi istituzionali consiliari (es.: notebook utilizzato per il lavoro agile, etc.);
h) **Amministratore di sistema**: figura professionale incaricata della gestione e della manutenzione dei sistemi informatici o di loro componenti. Rientrano, altresì, nella definizione di amministratore di sistema le figure equiparabili, quali l'amministratore di basi di dati, l'amministratore di rete e di apparati di sicurezza e l'amministratore di sistemi software complessi, individuate in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", come modificato dal provvedimento del 25 giugno 2009;
i) **Casella di posta elettronica personale/casella PEC personale:** casella assegnata a un utente per lo svolgimento dell'attività lavorativa o istituzionale, associata strettamente alla sua persona, il cui indirizzo è del tipo nome.cognome@consrc.it;
j) **Casella di posta elettronica condivisa/casella PEC condivisa:** casella associata a un ufficio o altra articolazione organizzativa, un organo o un organismo consiliare, una figura istituzionale, per lo svolgimento delle relative attività (settore.risorseumane@consrc.it, presidente@consrc.it, etc.);
k) **Dispositivi di memorizzazione rimovibili**: supporti per la memorizzazione di file non collegati stabilmente alla postazione di lavoro (CD, DVD, pendrive, schede di memoria, hard disk rimovibili, etc.);
l) **File di log**: registrazione sequenziale e cronologica delle operazioni effettuate da un sistema o da un servizio informatico;

m) **Servizi di comunicazione e collaborazione:** posta elettronica, chat, telefonia, videoconferenza, spazi condivisi di archiviazione;
n) **Software di produttività:** software utilizzati per lo svolgimento delle comuni attività d'ufficio quali, ad esempio, la stesura di documenti (software di video-scrittura, foglio elettronico, software per la manipolazione di immagini e video, software per la gestione della posta elettronica, etc.);
o) **Software gestionali:** gli applicativi informatici utilizzati dall'Ente per la gestione informatizzata delle attività istituzionali (sistema di gestione informatica dei documenti, sistema per la gestione contabile, sistema per la gestione delle risorse umane, etc.);
p) **Spazio condiviso di archiviazione dati:** ogni servizio o dispositivo idoneo alla memorizzazione di dati di proprietà del Consiglio regionale, destinato a custodire quelli relativi a utenze istituzionali (cartelle condivise su server aziendali, spazio cloud, etc.);
q) **Spazio personale di archiviazione dati:** ogni servizio o dispositivo idoneo alla memorizzazione di dati di proprietà del Consiglio regionale, assegnato specificamente ad un utente (cartella desktop/documenti, pendrive, spazio cloud associati a un account personale, etc.).

TITOLO II
Regole per l'utilizzo dei sistemi informatici dell'Ente

Art. 4
(Credenziali di accesso)

1. L'accesso alle applicazioni del sistema informativo consiliare avviene attraverso credenziali di autenticazione rilasciate dall'Ente.

2. Le credenziali di autenticazione, da gestire nel rispetto delle regole stabilite, sono strettamente personali e non devono essere comunicate, né rese disponibili ad altri soggetti.

3. In caso di diffusione accidentale delle credenziali di autenticazione, anche solo presunta, le password devono essere immediatamente modificate e l'incidente deve essere tempestivamente segnalato all'unità organizzativa che le ha rilasciate.

4. Sono stabilite le seguenti regole per quanto riguarda l'accesso al sistema informativo:

a) composizione di password complesse, con una lunghezza minima stabilita e una sequenza di caratteri normali, speciali e/o numerici;
b) modifica della password al primo utilizzo;
c) impostazione di una validità minima e massima della password;
d) impossibilità di riuso delle ultime password utilizzate;
e) blocco dell'utenza dopo un determinato numero di tentativi falliti di inserimento della password;
f) reinizializzazione (reset) della password e riattivazione dell'utenza disabilitata, secondo le procedure in vigore.

5. I dettagli dei requisiti richiesti sull'utilizzo delle password sono riportati nell'Allegato 1 - Password.

6. In ogni caso, l'utente è tenuto all'utilizzo di password complesse, anche nel caso in cui il sistema non lo richiede espressamente e accetta l'immissione di password semplici.

7. Al fine di garantire un adeguato livello di sicurezza, l'Ente, per alcuni servizi, implementa un sistema di autenticazione a più fattori (Multi Factor Authentication - MFA), richiedendo all'utente di dimostrare la propria identità anche attraverso più forme di verifica al momento dell'accesso a un'applicazione, con le modalità riportate nell'Allegato 2 - Autenticazione a più fattori.

8. Il rilascio delle credenziali di accesso e ogni operazione di modifica delle stesse (reset password) e dei profili sono richiesti per iscritto all'ufficio competente. Gli utenti impossibilitati a recarsi presso gli uffici per la consegna delle credenziali indicano, nella richiesta, un contatto telefonico o un recapito di posta elettronica ove riceverle.

9. In caso di violazione delle credenziali di accesso a qualunque sistema o servizio, si applica la disposizione di cui all'Art. 14
(Furto, smarrimento, violazione).

10. Alla sospensione e/o cessazione del rapporto con l'Ente, le credenziali personali di accesso ai sistemi sono disabilitate tempestivamente, e, comunque, non oltre 7 giorni solari.

11. Le credenziali personali e i dati a essi collegati (es.: posta elettronica, spazio personale di archiviazione, contenuto delle cartelle sui PC personali) sono definitivamente cancellati entro 30 giorni solari dal venir meno del rapporto con l'Ente.

Art. 5
(Software)

1. Il Settore Informatico e Flussi informativi del Consiglio regionale cura l'aggiornamento dell'elenco dei software gestionali e di produttività autorizzati, di cui all'Allegato 3 - Elenco software autorizzati (PDL), secondo le indicazioni della Circolare AgID n. 2 del 18 aprile 2017 e successive e, in particolare, dell'elenco dei software autorizzati e non autorizzati.

2. È vietata l'installazione di qualunque software, anche libero, non fornito o autorizzato dal Settore Informatico e Flussi informativi.

3. È vietata l'esecuzione di software, anche se non richiede installazione, non fornito o autorizzato dal Settore informatico e Flussi informativi.

4. A richiesta dell'utente, per ragioni di servizio, il personale autorizzato installa i software di cui all'Allegato 3 - Elenco software autorizzati (PDL).

5. L'installazione di software non inclusi nell'elenco di cui all'Allegato 3 - Elenco software autorizzati (PDL) può avvenire esclusivamente su richiesta motivata da ragioni di servizio del responsabile di riferimento dell'utente.

Art. 6
(Software gestionali)

1. Per la particolare criticità delle informazioni trattate, l'utilizzo dei software gestionali è consentito esclusivamente per lo svolgimento delle attività lavorative, previa autenticazione e profilazione, nei limiti delle funzioni e dei compiti specificatamente assegnati a ciascun utente.

2. Ciascun responsabile provvede a segnalare tempestivamente agli amministratori del software gestionale la necessità di creare, aggiornare o cancellare i profili utente associati al personale assegnato o a coloro che a qualsiasi titolo trattano i dati di competenza dell'ufficio amministrativo di riferimento.

3. L'utente è tenuto a dare tempestiva comunicazione agli amministratori del software della presenza di eventuali errori nelle impostazioni associate al proprio profilo di utilizzatore. È comunque vietato ogni trattamento di informazioni il cui accesso discende da una "profilazione utente" non aggiornata o errata.

4. È vietato ogni trattamento dati non inerente all'attività lavorativa con la correlata responsabilità dell'utente in ogni caso di uso illecito.

Art. 7
(Disposizioni in caso di assenza programmata)

1. In caso di assenza dal servizio per un periodo superiore a 15 giorni solari, il dipendente che svolge mansioni rilevanti verso l'esterno è tenuto ad attivare il servizio di risposta automatica sulla propria casella di posta elettronica, per segnalare ai mittenti la durata dell'assenza dal servizio e la necessità di inoltrare ogni comunicazione urgente, all'Ufficio competente o alla persona delegata.

2. Se l'assenza programmata è superiore a 30 giorni solari, l'Ente, per ragioni di sicurezza, si riservala facoltà di disattivare temporaneamente le credenziali di accesso del dipendente ai sistemi informatici, a eccezione della posta elettronica e dello spazio personale di archiviazione.

Art. 8
(Posta elettronica e PEC)

1. Gli utenti sono dotati di una casella di posta elettronica personale sul dominio consrc.it, da utilizzare per l'esercizio della propria attività lavorativa e/o istituzionale.

2. Agli uffici, organi e organismi consiliari, nonché alle diverse figure istituzionali è assegnata una casella di posta elettronica e/o di PEC. Il responsabile pro tempore di tale casella è il dirigente, nonché il titolare delle relative funzioni istituzionali.

3. Il responsabile della casella di posta elettronica condivisa può autorizzare l'accesso ad altri utenti, richiedendo agli amministratori di sistema le necessarie modifiche dei profili autorizzativi.

4. Al venir meno della titolarità della funzione, l'accesso alla casella condivisa è tempestivamente precluso al responsabile cessato. Per garantire la continuità amministrativa viene comunque mantenuto l'accesso ai collaboratori già autorizzati. Nel caso di casella PEC, gli amministratori di sistema provvedono tempestivamente ai necessari adempimenti.

5. Anche in ossequio all'articolo 11 bis, commi 3 e 5, del dpr 62/2013, ogni utilizzatore del servizio di posta elettronica o di PEC è responsabile del contenuto dei messaggi inviati.

6. È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, oltraggiosi, discriminatori o che possono essere, in qualunque modo, fonte di responsabilità per l'amministrazione.

7. Nell'utilizzo del servizio, l'utente ha l'obbligo di:

a) proteggere il diritto di riservatezza dell'interlocutore evitando, se non necessario, di inoltrare messaggi altrui senza il previo consenso dell'interessato;
b) inviare le e-mail dalle caselle di posta elettronica esclusivamente a nome proprio;
c) evitare l'invio o l'inoltro di messaggi estranei al contesto lavorativo a un numero elevato di indirizzi o a liste di distribuzione interne al Consiglio regionale;
d) prestare la massima attenzione nell'apertura di link e di file allegati ai messaggi di posta elettronica ricevuti. In particolare, va evitata l'apertura e la lettura di messaggi di posta elettronica provenienti da mittenti di cui non si conosce l'identità o che contengono allegati potenzialmente dannosi (es. .EXE, .COM, .VBS, .HTM/HTML, .SCR, .BAT, .JS, .PIF, etc.).

8. L'utilizzatore si uniforma alle modalità di firma individuate dal Consiglio regionale nell'Allegato 6 - Galateo della comunicazione digitale.

Art. 9
(Servizi sincroni di comunicazione e collaborazione)

1. I servizi sincroni di comunicazione e collaborazione sono utilizzati esclusivamente per finalità istituzionali o strettamente collegate all'attività lavorativa; essi consentono di inviare messaggi, effettuare videoconferenze, telefonare e registrare.

2. Gli utenti accedono al sistema di videoconferenza a mezzo di specifiche credenziali ovvero identificandosi con nome e cognome per esteso.

3. La riunione è convocata a mezzo di apposito invito che reca l'elenco di tutti i partecipanti.

4. La registrazione delle riunioni in video conferenza è consentita solo se gli utenti sono stati preventivamente avvisati. L'eventuale successiva diffusione in favore di soggetti estranei al Consiglio regionale della Calabria della registrazione audio/video deve essere espressamente autorizzata per iscritto da tutti i soggetti che compaiono nelle immagini video o che hanno preso la parola.

5. Sono vietate le comunicazioni, all'interno o all'esterno dell'amministrazione, oltraggiose, discriminatorie o che possano essere in qualunque modo fonte di responsabilità per il Consiglio regionale; è opportuno attenersi a quanto indicato nell' nell'Allegato 6 - Galateo della comunicazione digitale per una corretta comunicazione in internet e nelle mail.

6. Il telefono fisso assegnato all'utente è uno strumento da utilizzare esclusivamente per lo svolgimento dell'attività lavorativa; le comunicazioni a carattere personale sono eccezionalmente tollerate in caso di effettiva necessità e/o emergenza, per comunicazioni di breve durata.

Art. 10
(Spazi di archiviazione)

1. Gli spazi di archiviazione devono essere utilizzati per la memorizzazione di file a uso strettamente lavorativo.

2. I dati di proprietà del Consiglio regionale devono essere memorizzati unicamente negli spazi di archiviazione, personali e condivisi, gestiti dall'Ente. È vietato agli utenti l'utilizzo di spazi di archiviazione non gestiti dall'Ente (es. Dropbox, Google Drive, Microsoft OneDrive, Apple iCloud, etc.) per memorizzare dati personali.

3. Gli atti, i provvedimenti e i documenti definitivi devono essere memorizzati nell'apposito spazio condiviso di archiviazione, messo a disposizione del Consiglio regionale (cartelle condivise, spazio cloud gestito dall'Ente), per minimizzare il rischio di perdita di dati dell'Ente a seguito di guasti alle PDL.

4. Il responsabile di ciascuna struttura organizzativa può individuare i collaboratori autorizzati ad accedere a partizioni dello spazio condiviso di archiviazione organizzate, per minimizzare l'accesso ai dati personali ivi custoditi.

5. Al venir meno della titolarità della funzione di responsabile della struttura, l'accesso agli spazi condivisi di archiviazione è tempestivamente precluso al responsabile cessato. Per garantire la continuità amministrativa viene comunque mantenuto l'accesso dei collaboratori già autorizzati.

6. In caso di necessità e/o comprovato pericolo per la sicurezza dei sistemi, il Consiglio regionale può procedere, anche senza preavviso, alla rimozione di file e/o applicazioni presenti negli spazi di archiviazione degli utenti, dandone tempestiva comunicazione agli interessati e, comunque, non oltre 15 giorni solari dalla rimozione.

7. Al fine di scongiurare la perdita irreversibile, dipendente da qualsiasi causa (es. malfunzionamenti hardware/software, malware, attacchi informatici, furto, smarrimento, etc.), dei dati inerenti all'attività lavorativa, gli utenti sono tenuti a memorizzarli negli spazi condivisi di archiviazione e/o nello spazio cloud associato al proprio account personale.

Art. 11
(Postazione di lavoro)

1. Il responsabile dell'unità organizzativa assegna in uso esclusivo a ciascun utente le PDL, per lo svolgimento della propria attività lavorativa. È vietato qualsiasi utilizzo che deturpa o rovina la PDL e gli accessori/periferiche in assegnazione.

2. La modifica alle configurazioni della PDL deve essere richiesta dal responsabile dell'unità organizzativa di riferimento al Settore Informatico e Flussi informativi e può essere effettuata esclusivamente da personale autorizzato.

3. A ciascun utente è associato un profilo per l'accesso alla PDL adeguato all'attività lavorativa e/o istituzionale di competenza.

4. La PDL è provvista di software di sicurezza (software antivirus, personal firewall, etc.) e software base autorizzato dal Consiglio regionale. L'installazione di ulteriori software è richiesta dal responsabile dell'unità organizzativa al Settore Informatico e Flussi informativi, che ne valuta i soli aspetti tecnici (prestazioni, sicurezza informatica, etc.).

5. L'utente deve adottare ogni precauzione per impedire l'accesso alla PdL a soggetti non autorizzati; essa, pertanto, in caso di suo temporaneo allontanamento, deve essere bloccata, mentre, al termine della giornata lavorativa, per motivi di sicurezza e di risparmio energetico e sostenibilità, deve essere spenta.

6. Alla cessazione dell'utilizzo di qualunque dispositivo e comunque prima dell'eventuale assegnazione ad altro utente o della sua dismissione, l'unità organizzativa competente procede alla cancellazione sicura (wiping) dei dati ivi contenuti. I supporti rimovibili, non destinati al riutilizzo e contenenti dati personali, devono essere fisicamente resi inaccessibili mediante distruzione.

7. In caso di furto e/o smarrimento degli strumenti o violazione dei dati, si applica l'Art. 14 (Furto, smarrimento, violazione).

Art. 12
(Postazione remota di lavoro)

1. Le postazioni remote di lavoro sono manutenute dall'Ente per l'installazione di aggiornamenti e per ogni altra attività necessaria a garantirne la sicurezza. In caso di significativo rischio di compromissione o/e sicurezza, il Settore Informatico e Flussi informativi può richiedere all'utente lo spegnimento della PDL fino all'effettuazione della verifica, ovvero bloccare il dispositivo da remoto.

2. Le attrezzature assegnate all'utente per l'attività di lavoro agile o altre attività istituzionali sono strumenti di lavoro appartenenti al patrimonio dell'Ente e, pertanto:

a) devono essere utilizzati esclusivamente per l'attività lavorativa;
b) devono essere custoditi con cura e diligenza, adottando ogni precauzione necessaria per evitare danni o sottrazioni;
c) devono essere utilizzati esclusivamente dall'assegnatario e non possono essere ceduti, neppure temporaneamente, a terzi, né a titolo gratuito né a titolo oneroso;
d) per la connessione alla rete Internet, devono essere utilizzate unicamente reti istituzionali (es.: WiFi del Consiglio regionale o di altri enti pubblici) o private (domestiche), purché sia implementato il protocollo di sicurezza WPA2 o standard di sicurezza superiori; è, invece, vietato connettere i dispositivi di servizio a hot-spot WiFi pubblici (es.: ristoranti, hotel, aeroporti, etc.);
e) devono essere usati soltanto i software installati e autorizzati dall'Ente ed è vietato disinstallarli o disattivarli;
f) gli utenti, prima della riconsegna, devono rimuovere dai notebook eventuali file elaborati e utilizzati. I file non rimossi dall'utente sono eliminati irreversibilmente prima dell'utilizzo da parte di un utente diverso.

3. È fatto divieto di:

a) utilizzare dispositivi (notebook, tablet, etc.) diversi da quelli all'uopo assegnati;
b) custodire le credenziali per l'accesso assieme al dispositivo assegnato;
c) apportare qualsiasi modifica hardware o connettere ai notebook dispositivi esterni non autorizzati;
d) utilizzare memorie esterne USB non assegnate dall'Ente.

4. Per tutto quanto non espressamente disciplinato, si applicano le disposizioni di legge vigenti in materia e quelle del presente disciplinare.

Art. 13
(Dispositivi di memorizzazione rimovibili)

1. L'utente deve utilizzare esclusivamente dispositivi di memorizzazione rimovibili assegnati dall'Ente e rivolgersi al Settore Informatico e Flussi informativi per le opportune configurazioni di sicurezza e/o crittografia del dispositivo, in caso di trattamento di dati personali.

2. L'assegnazione dei dispositivi è strettamente personale.

3. L'utente deve custodirli con la massima diligenza, cautela e riservatezza e utilizzarli esclusivamente per le attività lavorative svolte su PDL gestite dall'Ente.

3. È vietato cedere a chiunque, anche temporaneamente, dispositivi già utilizzati per la memorizzazione di informazioni o di dati personali, anche se cancellati, per scongiurare il rischio di recupero dei file eliminati da parte di soggetti malintenzionati.

4. In caso di furto e/o smarrimento, si applica l'Art. 14
(Furto, smarrimento, violazione).

Art. 14
(Furto, smarrimento, violazione)

1. In caso di violazione delle credenziali di accesso a qualunque sistema o servizio, l'utente deve avvisare tempestivamente il responsabile di riferimento e l'unità organizzativa che le ha rilasciate. Analogo adempimento è richiesto all'utente nei casi di furto o smarrimento delle strumentazioni informatiche.

2. In caso di possibile violazione di dati, l'utente ne dà tempestivo avviso, oltre che ai soggetti di cui al comma 1, anche al Responsabile della protezione dati.

3. Restano fermi gli obblighi di denuncia alle autorità competenti di qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso.

Art. 15
(Firma digitale)

1. Il kit di firma digitale è assegnato all'utente per esigenze di servizio, su richiesta del dirigente di riferimento indirizzata al Settore informatico e Flussi informativi.

2. L'uso del kit di firma digitale, anche remota, è strettamente personale, non cedibile a terzi e finalizzato esclusivamente all'attività lavorativa e istituzionale.

3. Per prevenire disservizi, l'utente richiede al Settore informatico e Flussi informativi il rinnovo del certificato di firma almeno 30 giorni solari prima della scadenza dello stesso.

4. In caso di furto e/o smarrimento degli strumenti o violazione dei dati, si applica l'Art. 14
(Furto, smarrimento, violazione).

Art. 16
(Altri dispositivi)

1. Con riferimento alle smart card utilizzate per l'identificazione dei partecipanti alle sedute informatizzate, si applicano, per quanto compatibili, gli articoli 4 e 14.

2. Con riferimento ad altri dispositivi (fotocopiatori multifunzione di rete, stampanti, scanner, webcam ecc.), si applicano le norme del presente disciplinare e, in particolare, per quanto compatibile, l'articolo 14.

Art. 17
(Navigazione Internet)

1. L'Ente mette a disposizione degli utenti il servizio di navigazione Internet esclusivamente per lo svolgimento della prestazione lavorativa, fatto salvo quanto previsto all'Art. 2 (Principi generali), comma 3.

2. L'utente è responsabile di qualsiasi operazione effettuata.

3. Fermo restando quanto previsto per i pubblici dipendenti dagli articoli 11-bis e 11-ter del dpr 62/2013, l'utente, ha i seguenti doveri:

a) tenere un comportamento diligente, lecito e tale da non compromettere le attività e l'immagine dell'Ente.
b) navigare in Internet in modalità trasparente e non anonima;
c) astenersi da qualsiasi comportamento di natura oltraggiosa e/o discriminatoria verso terzi;
d) trasferire sulla propria PDL solo file da siti web verificati e affidabili, prestando la massima attenzione per non incorrere in violazioni di diritti di proprietà intellettuale o in infezioni da malware;
e) non utilizzare social network, forum, chat e simili per scambiare dati e informazioni riservati o lesivi dell'immagine del Consiglio regionale e di quella dei suoi dipendenti e/o utenti.

4. Per prevenire l'accesso a siti web e risorse Internet potenzialmente nocivi, il Consiglio regionale può adottare soluzioni di sicurezza basate su filtri e decriptazione delle informazioni della navigazione Internet, anche attraverso il blocco dei siti potenzialmente nocivi.

5. Per prevenire il download di file o pagine web contenenti codici malevoli, l'Ente adotta soluzioni di sicurezza basate su tecnologie antivirus e antimalware, che effettuano la scansione dei contenuti della navigazione Internet e bloccano il download del contenuto in caso di rilevazione di codice malevolo.

TITOLO III
Sicurezza e prestazioni

Art. 18
(Controlli e monitoraggi)

1. Il Consiglio regionale effettua controlli e monitoraggi sui sistemi informatici messi a disposizione per lo svolgimento dell'attività lavorativa e istituzionale nel rispetto della normativa vigente e sul presupposto di un utilizzo responsabile da parte degli utenti, adottando, in ogni caso, soluzioni tecnologiche idonee a garantire adeguati standard di sicurezza dei sistemi stessi e dei dati gestiti.

2. Per i fini di cui al comma 1, i sistemi informatici implementano i cosiddetti "file di log", effettuando il tracciamento delle operazioni per rilevare eventuali anomalie o minacce informatiche potenzialmente dannose per la funzionalità e la sicurezza degli apparati e delle informazioni ivi contenute.

3. L'amministratore di sistema, se rileva anomalie o configurazioni non corrette delle PDL, a salvaguardia della sicurezza e dell'integrità dei sistemi informativi, può isolare l'origine dell'anomalia o del malfunzionamento anche senza preavvisare l'utente, comunicando successivamente le ragioni dell'intervento.

4. Le attività di cui al presente articolo sono svolte nel rispetto della normativa vigente e in ossequio ai principi di gradualità, pertinenza e non eccedenza stabiliti dal Garante per la protezione dei dati personali, nonché dei diritti e delle libertà fondamentali degli utenti.

Art. 19
(Amministratori di sistema)

1. Gli amministratori di sistema svolgono le attività necessarie per garantire l'efficienza e la sicurezza dei sistemi informativi e delle applicazioni in conformità con quanto stabilito dal presente disciplinare e nel rispetto della normativa vigente, anche relativa alla protezione dei dati personali.

2. L'Ente assegna agli amministratori di sistema le funzioni e/o le mansioni connesse all'erogazione dei servizi informatici al fin di perseguire un adeguato livello di efficienza e un grado di sicurezza commisurato al rischio.

3. Rientrano tra i compiti degli amministratori di sistema:

a) la gestione tecnica delle dotazioni informatiche (hardware e software) dell'Ente;
b) la creazione, l'attivazione, la disattivazione, tutte le relative attività amministrative di profilazione degli account di accesso ai sistemi e alle risorse;
c) il monitoraggio del corretto funzionamento delle risorse di rete, dei computer e degli applicativi affidati agli utenti, per finalità di manutenzione, gestione della sicurezza e protezione dei dati;
d) ogni attività necessaria a garantire la sicurezza informatica dei sistemi informativi dell'Ente;
e) in caso di prolungata assenza, irreperibilità o impedimento dell'utente e previa motivata richiesta del suo responsabile di riferimento, l'accesso, anche da remoto, ai dati o alle applicazioni di proprietà dell'Ente, nei limiti di legge vigenti in materia

4. Gli amministratori di sistema effettuano l'accesso ai sistemi informatici utilizzando le credenziali associate al profilo specifico solo per lo svolgimento delle operazioni che richiedono privilegi elevati. Negli altri casi, l'accesso ai sistemi deve avvenire con l'utilizzo di credenziali da utente semplice.

5. In caso di necessità di accesso a cartelle, file o archivi di altri utenti, gli amministratori di sistema limitano il proprio intervento a quanto strettamente indispensabile; in ogni caso, non possono esercitare alcun controllo a distanza dell'attività dei lavoratori.

TITOLO IV
(Disposizioni finali)

Art. 20
(Responsabilità e sanzioni)

1. Salvo che non costituisca fatto più grave, la violazione degli obblighi e dei divieti previsti dal presente disciplinare da parte dell'utente – dipendente pubblico in servizio presso il Consiglio regionale, comporta l'applicazione delle sanzioni disciplinari di cui al decreto legislativo 30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche), ai contratti collettivi, al D.P.R. 16 aprile 2013, n. 62 (Codice di comportamento dei dipendenti della pubblica amministrazione) e ai Codici disciplinari del personale del relativo Comparto (dirigente e non).

2. Restano ferme le responsabilità civili, penali e contabili di ogni utente per fatti illeciti e/o danni derivanti da usi non consentiti o poco diligenti dei servizi e degli strumenti informatici di proprietà e/o messi a disposizione dall'Ente, anche alla luce di quanto previsto dal presente disciplinare.

Allegati

Per garantire la costante sicurezza del sistema informativo del Consiglio regionale e, dunque, recepire tempestivamente le eventuali modificazioni normative ovvero rispondere a esigenze contingenti e/o emergenziali, i successivi allegati, recanti disposizioni tecnico-operative, sono aggiornati, revisionati o, comunque, modificati con provvedimento del dirigente del Settore Informatico e Flussi informativi.

Allegato 1 - Password

Si elencano, di seguito, i criteri di sicurezza per le password:

- La lunghezza minima di una password deve essere di 8 caratteri (14 per le utenze amministrative).
- La password deve includere una combinazione di lettere maiuscole, lettere minuscole, numeri e simboli.
- La password non deve contenere parole di senso compiuto, nomi, marchi, sigle, etc.
- Non utilizzare il nome utente (o parti di esso) come password.
- Non utilizzare password che possano essere legate alla persona, ai familiari, ai nomi di animali domestici, alle date di nascita, a numeri telefonici.
- Non utilizzare password corrispondenti a sequenze di lettere o numeri come aaabbb, qwerty, 123321, etc.
- La password deve essere significativamente diversa dalle precedenti; vanno evitate, in particolare, le sequenze del tipo Password1, Password2, Password3.
- La password non deve essere utilizzata per più di sei mesi e non deve essere riutilizzata.
- Utilizzare una password diversa per ciascun servizio.
- Le password del "profilo amministrativo" e del "profilo user" assegnati allo stesso utente devono essere significativamente differenti.
- Non comunicare a terzi le proprie password (neppure agli amministratori di sistema).
- Non appuntare le proprie password su foglietti volanti o incollati al PC/monitor.
- Non riportare le password in file memorizzati su PC oppure online (es. file di testo, documenti Word oppure Excel, etc.) senza previa crittografia degli stessi con password lunghe e complesse. Piuttosto, utilizzare dei software gratuiti di gestione delle password ("password manager") con funzionalità di crittografia integrate.
- Non rivelare le password in messaggi e-mail, chat o altre comunicazioni elettroniche.
- Prestare attenzione affinché altri non carpiscano la password durante la digitazione.

Se sussiste il sospetto che una password sia stata compromessa, occorre cambiarla immediatamente ed informare tempestivamente il proprio responsabile.

Allegato 2 - Autenticazione a più fattori

Il Consiglio regionale della Calabria implementa l'autenticazione a due fattori mediante l'app Microsoft Authenticator.

L'installazione e la configurazione sono effettuate in autonomia dagli utenti, secondo i passaggi di seguito illustrati:

- **aprire l'app Microsoft Authenticator sul proprio dispositivo mobile;**
- **in alto a destra, fare tap sui tre puntini e scegliere "Aggiungi account" (Figura 1 Aggiunta account);**
- **selezionare quindi "Account aziendale o dell'istituto di istruzione" (Figura 2 selezione tipologia account istituzionale);**
- **scegliere il metodo "Esegui la scansione di un codice a matrice" (Figura 3 Scelta del metodo di aggiunta);**
- **inquadrare il QRcode apparso sullo schermo del PC (Figura 4 Approvazione accesso);**
- **terminare la procedura approvando la richiesta di accesso (Figura 5 Conclusione dell'autenticazione).**

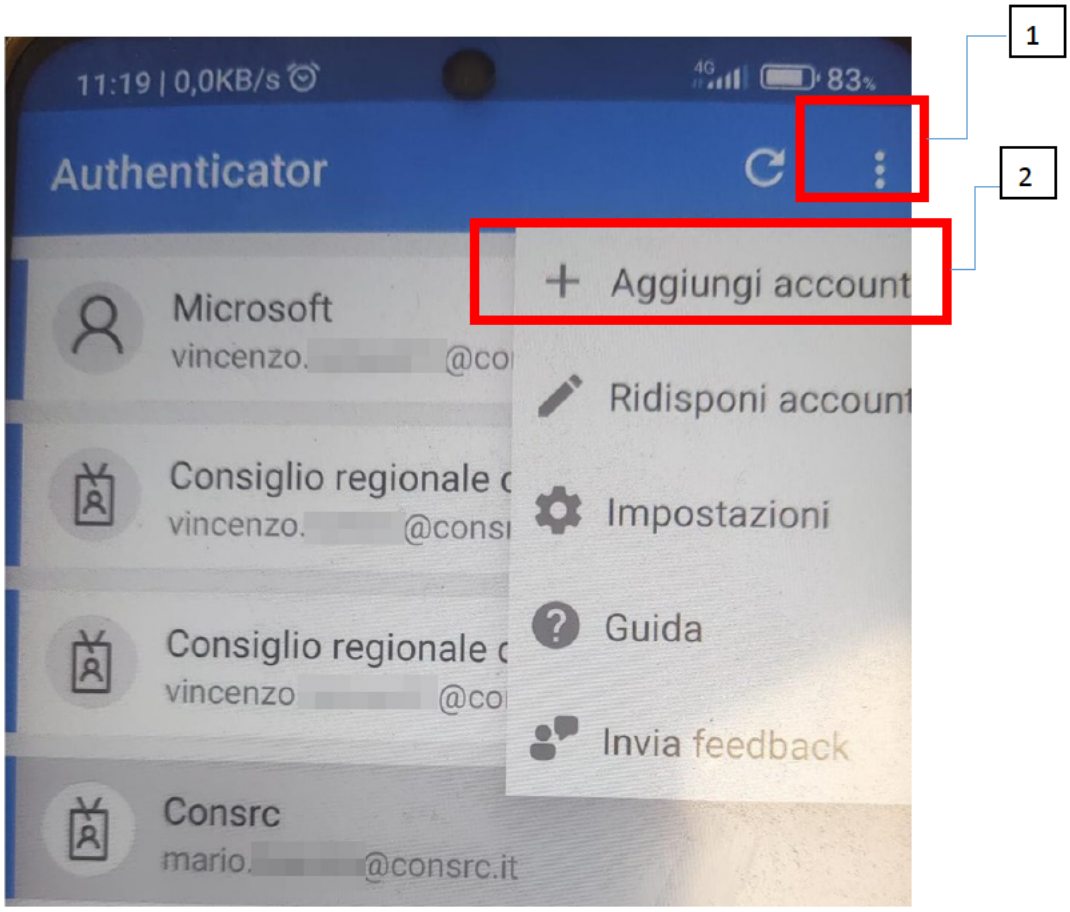

Figura 1: Aggiunta account

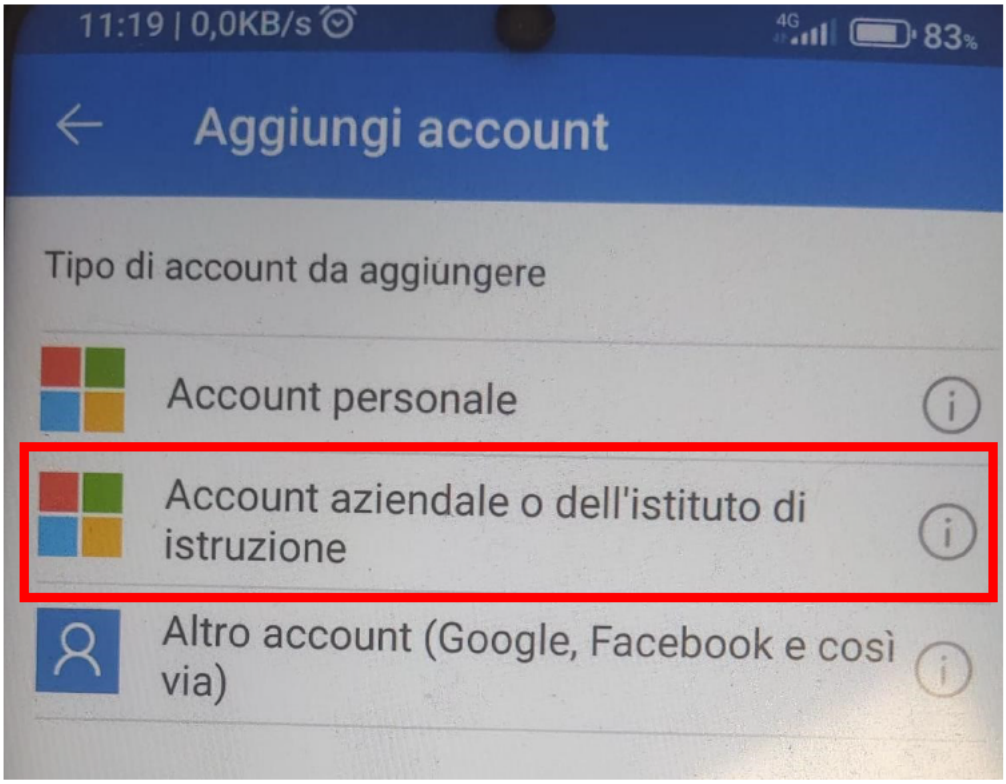

Figura 2 Selezione tipologia account istituzionale

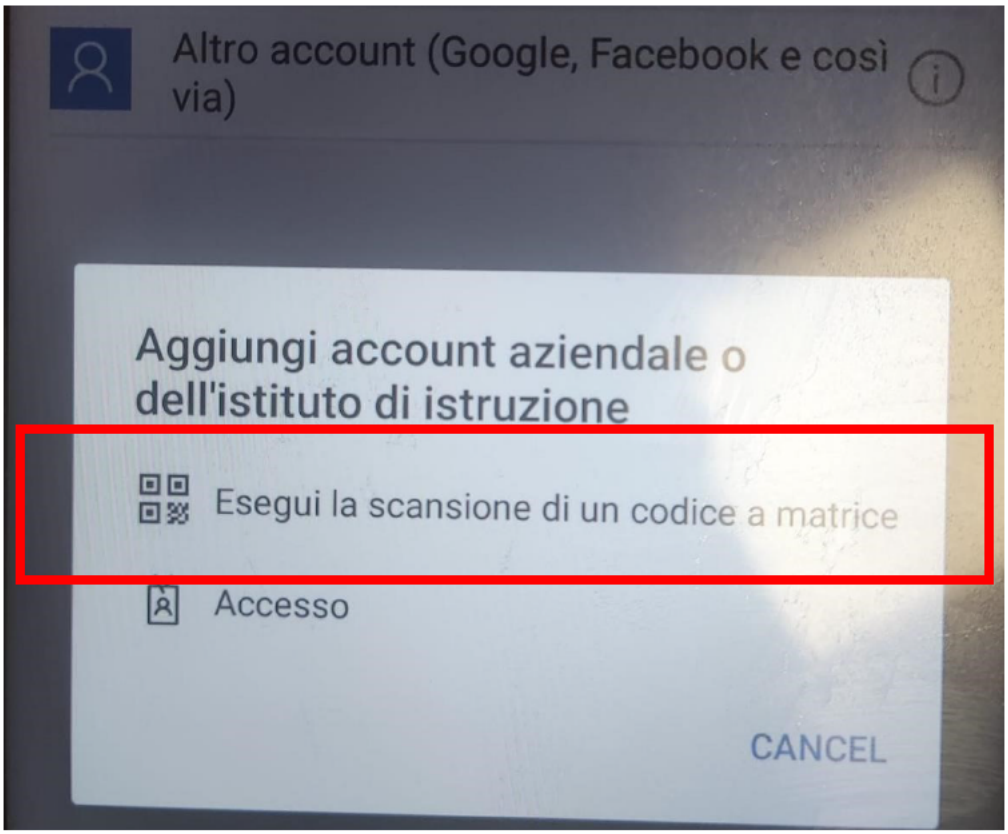

Figura 3 Scelta del metodo di aggiunta

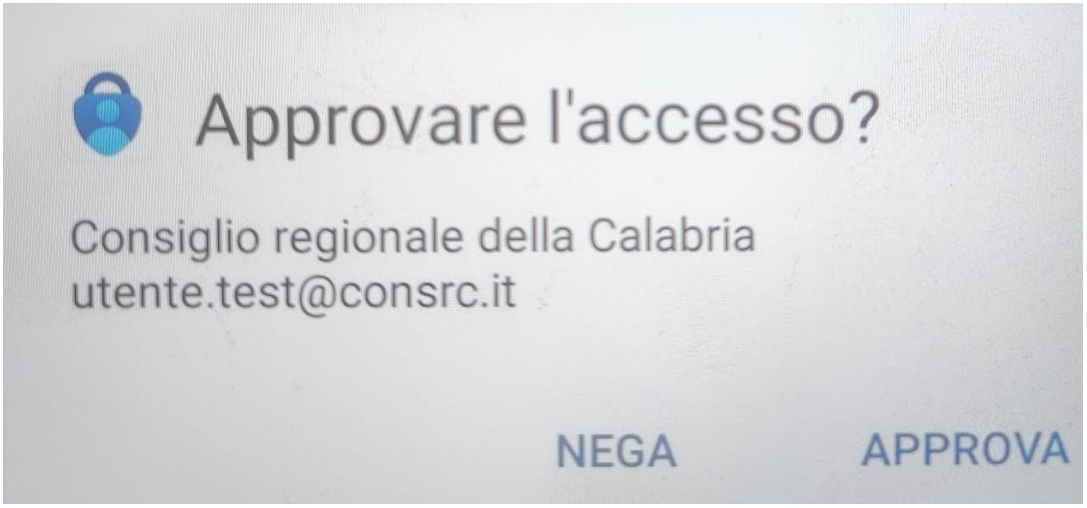

Figura 4 Approvazione accesso

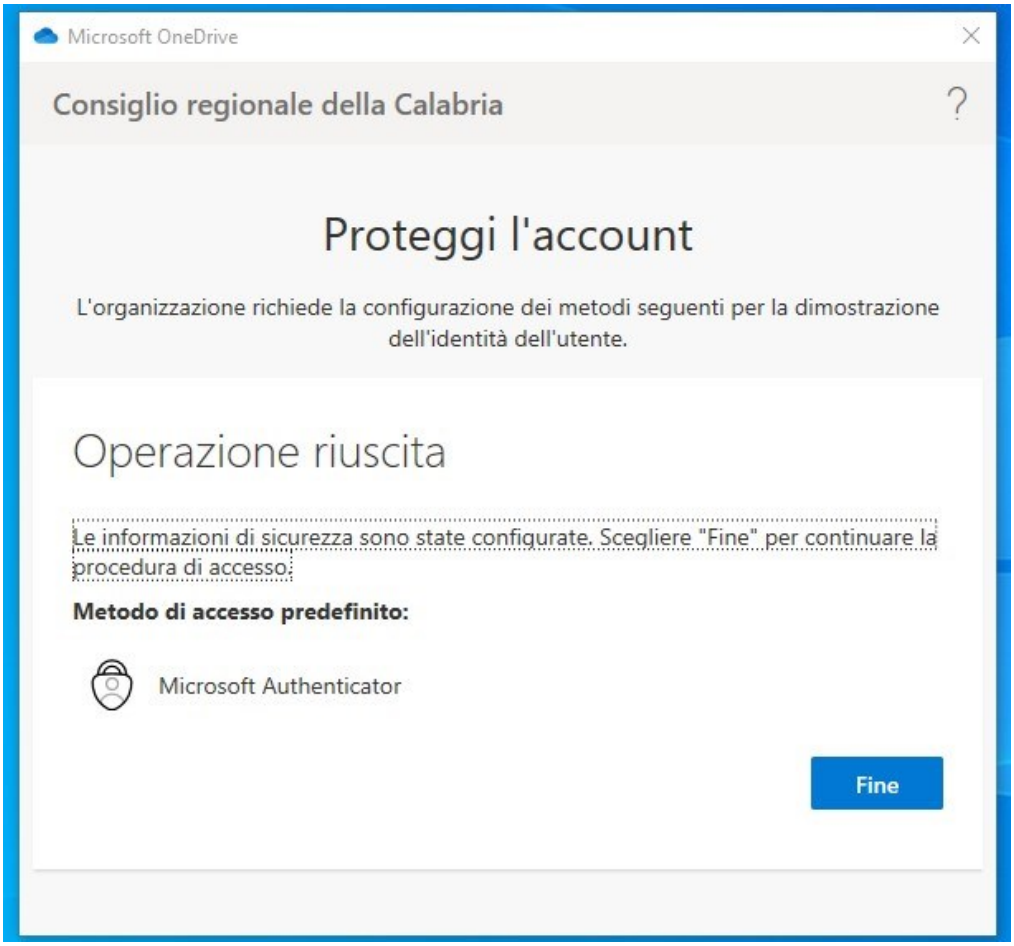

Figura 5 Conclusione dell'autenticazione

Allegato 3 - Elenco software autorizzati (PDL)

Di seguito uno stralcio, relativo alle sole PDL, dell'elenco di software autorizzati, stilato in applicazione della Circolare Agid n. 2 del 18 aprile 2017 (ABSC_ID 2.1.1.)

Categoria	Descrizione
Antivirus/Antimalware	Malwarebytes Anti-Malware versione
Antivirus/Antimalware	Microsoft Security Essentials
Antivirus/Antimalware	Symantec Endpoint Protection
Asset management	Microsoft Configuration Manager Client
Browser	Google Chrome
Browser	Mozilla Firefox
Browser	Safari
Browser	Windows Internet Explorer
Cloud	Microsoft OneDrive
Collaboration	Microsoft Skype for Business MUI (Italian)
Collaboration	Microsoft Windows Live Essentials
Collaboration	Microsoft Windows Live Mail
Collaboration	Microsoft Windows Live Messenger
Collaboration	Skype™
Collaboration	Microsoft Teams
DBMS	Firebird
DBMS	Pegasus MultiMedia DataBase
FTP client	FileZilla Client
Gestionale	Gestione Contabile
Gestionale	Serpico
Gestionale	Gestione Settore Tecnico, Provveditorato
Gestionale	Golem Time SQL
Gestionale	Modello 730
Gestionale	Paghe_2
Grafica	AutoCAD
Grafica	AutoCAD 2016 - Italiano
Grafica	GIMP
Grafica	ImagXpress
Grafica	Picasa
Multimedia	Adobe Creative Suite Master Collection
Multimedia	CDBurnerXP
Multimedia	CyberLink Power2Go
Multimedia	CyberLink PowerDVD
Multimedia	DolbyFile
Multimedia	ImgBurn
Multimedia	Movie Maker
Multimedia	NeroBurningROM
Multimedia	Network ScanGear Ver.2.21
Multimedia	PowerDVD
Multimedia	PowerDVD Create
Multimedia	QuickTime
Multimedia	VLC media player

Categoria	Descrizione
Office automation	ABBYY FineReader 6.0 Sprint
Office automation	Adobe Acrobat
Office automation	Adobe Acrobat 9 Pro - Italiano, Español, Nederlands, Português
Office automation	Adobe Acrobat Reader DC - Italiano
Office automation	Adobe Acrobat X Pro - Italiano, Español, Nederlands, Português
Office automation	Adobe AIR
Office automation	Adobe Refresh Manager
Office automation	CutePDF Writer
Office automation	Arubasign
Office automation	DiKe
Office automation	Document Capture Pro
Office automation	LibreOffice
Office automation	Microsoft Office 2007
Office automation	Microsoft Office 2010 Proof (Italian)
Office automation	Microsoft Office 2013 Professional Plus
Office automation	Microsoft Office 2016 Professional Plus
Office automation	Microsoft Office 2016 Standard
Office automation	Microsoft Office 365
Office automation	Nitro Pro
Office automation	Nuance OmniPage
Office automation	OpenOffice
Office automation	PaperPort Image Printer
Office automation	PDF Architect
Office automation	PDF24 Creator
Office automation	PDFCreator
Office automation	Presto! PageManager
Office automation	ScanSnap
Plugin	Adobe Flash Player 10 ActiveX
Plugin	Adobe Flash Player 26 ActiveX
Plugin	Microsoft Silverlight
Sistema operativo	Microsoft Windows 7 Pro
Framework	Microsoft .NET Framework
Framework	Microsoft .NET Framework 4 Client Profile
Framework	Microsoft Visual C++ 2005 Redistributable
Framework	Microsoft Visual C++ 2008 Redistributable - x86
Framework	Microsoft Visual C++ 2010 x64 Redistributable
Framework	Microsoft Visual C++ 2010 x86 Redistributable
Framework	Microsoft Visual C++ 2012 Redistributable (x64) -
Framework	Microsoft Visual C++ 2013 Redistributable (x86) -
Framework	Microsoft Visual C++ 2015 Redistributable (x86) -
IDE	Microsoft Visual Studio
IDE	Python
IDE	Pycharm
Uso tecnologia assistiva	JAWS
Uso tecnologia assistiva	NVDA
Tools	7-Zip
Tools	Adobe Shockwave Player
Tools	CCleaner

Categoria	Descrizione
Tools	Cobian Backup
Tools	DAEMON Tools Lite
Tools	Forefront TMG Client
Tools	Google Earth
Tools	GoToMeeting
Tools	Hardcopy
Tools	iTunes
Tools	Java
Tools	Microsoft Security Client
Tools	MySQL Connector/ODBC
Tools	Notepad++
Tools	PowerISO
Tools	Recuva
Tools	Samsung Kies3
Tools	TeamViewer
Tools	WhatsApp
Tools	WinRAR
Tools	WinZip
Tools	XStandard
Tools	Connettore PiTre
Tools	WebmailConnector
Tools	AnyDesk
Tools	ForticlientVPN
Sistema operativo	Microsoft Windows XP
Sistema operativo	Microsoft Windows Vista
Sistema operativo	Microsoft Windows 7
Sistema operativo	Microsoft Windows 8
Sistema operativo	Microsoft Windows 8.1
Sistema operativo	Microsoft Windows 10
Sistema operativo	Microsoft Windows 11

Allegato 4 - File di Log

I file di log contengono la registrazione sequenziale e cronologica delle operazioni effettuate in un sistema informatico.

Tali registrazioni possono includere: il riferimento alla postazione di lavoro utilizzata (indirizzo IP, nome computer, sistema operativo e/o altro software utilizzato, etc.); il riferimento al sistema che eroga un dato servizio (indirizzo IP, nome computer, sistema operativo e/o altro software utilizzato, etc.); il riferimento all'utente (ID, username, etc.); altri parametri propri dell'operazione (ID operazione, ID informazioni trattate, esito, codici di errore, data e ora dell'operazione, etc.).

Grazie a queste informazioni è possibile ricostruire la sequenza delle operazioni che si sono succedute nel sistema informativo e dunque analizzare i malfunzionamenti e le anomalie, individuare le minacce e gli attacchi informatici, garantire la sicurezza dei dati e il controllo sul loro corretto utilizzo.

Ai sensi dell'articolo 14 del Regolamento (UE) 2016/679 (General Data Protection Regulation - GDPR), si forniscono le seguenti informazioni:

1) **Titolare del trattamento dati.** Il titolare del trattamento è il Consiglio regionale della Calabria, Via Cardinale Portanova snc, 89123 Reggio Calabria (RC), e-mail: titolaretrattamentodati@consrc.it, PEC: consiglioregionale@pec.consrc.it.
2) **Dati di contatto del Responsabile della protezione dei dati:** e-mail: rpd@consrc.it, PEC: rpd@pec.consrc.it.
3) **Finalità del trattamento.** I log sono raccolti e conservati da parte del Consiglio regionale della Calabria esclusivamente per il perseguimento delle seguenti finalità:
   - conformità alle normative vigenti e applicabili;
   - monitoraggio della sicurezza del sistema informatico al fine di rilevare eventuali attacchi e svolgere le dovute analisi post-incidente;
   - garanzia di continuità dei servizi erogati mediante la rilevazione e la risoluzione di anomalie di funzionamento;
   - adempimenti contrattuali, laddove applicabile.
4) **Base giuridica del trattamento.** Le basi giuridiche del trattamento traggono origine dal:
   - l'articolo 24, paragrafo 1, del GDPR, che, in ossequio al principio di accountability (responsabilizzazione), pone in capo al titolare del trattamento l'onere di mettere in atto misure tecniche e organizzative adeguate a garantire, essendo in grado di dimostrarlo, che il trattamento effettuato è conforme al regolamento stesso;
   - l'articolo 32 del medesimo GDPR, che impone al titolare del trattamento il compito di individuare, implementare ed aggiornare un sistema di misure di sicurezza tecniche ed organizzative idonee a proteggere i dati personali da potenziali rischi quali la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso, accidentale o illegale, ai dati personali.
5) **Categorie di dati raccolti.** Possono essere raccolti i seguenti dati:
   - data/ora dell'evento;
   - informazioni sull'utente (id, username, etc.);
   - identificativo della postazione di lavoro (indirizzo IP, nome computer, etc.);
   - informazioni relative al sistema operativo e all'applicativo utilizzato (nome, produttore, versione, etc.);
   - identificativo del server o del servizio remoto (es. indirizzo IP, nome computer, etc.);

- parametri applicativi (codice dell'operazione effettuata, id delle informazioni accedute, esito dell'operazione effettuata, messaggio di errore, etc.).

6) **Comunicazione.** Per le finalità del trattamento, i dati non sono oggetto di comunicazione, salvo che diversamente previsto dalle disposizioni vigenti in materia.
7) **Periodo di conservazione.** I dati sono conservati solo per il tempo strettamente necessario al perseguimento delle finalità di cui al punto 3) e, comunque, per un periodo di tempo non inferiore a 6 mesi.
8) **Fonte dei dati.** I dati di log vengono raccolti automaticamente dai sistemi informatici quando gli utenti interagiscono con i vari servizi. Questi dati sono generati durante l'uso dei servizi e non vengono forniti direttamente dagli interessati.
9) **Processi decisionali automatizzati.** Non esiste alcun processo decisionale automatizzato, compresa la profilazione, basato sui dati di log.
10) **Diritti dell'interessato.** Restano fermi i diritti degli interessati di cui agli articoli da 14 a 21 del GDPR.

Allegato 5 - Posta elettronica

L'invio di comunicazioni alle liste di distribuzione istituzionali (es.: [redacted], [redacted], etc.) è riservato alle circolari, agli avvisi, alle comunicazioni di servizio, ai messaggi dei soggetti istituzionali e dei rappresentanti sindacali.

Un paragrafo di avvertimento (disclaimer) sulla privacy viene accodato automaticamente al testo dei messaggi inviati a caselle di posta elettronica esterne al dominio @consrc.it. Detto paragrafo contiene un richiamo alla riservatezza del contenuto della conversazione ed un invito alla cancellazione per chi dovesse ricevere accidentalmente il messaggio. Non è consentito modificare né rimuovere il paragrafo.

Al fine di prevenire la diffusione di e-mail contenenti spam, posta indesiderata, malware, phishing, etc., è effettuata una scansione di sicurezza dei messaggi mediante strumenti automatici.

A seguito dei controlli di sicurezza automatici, se necessario, l'amministratore di sistema accede ai singoli messaggi identificati come potenzialmente malevoli esclusivamente per analizzare e bloccare l'eventuale attacco o tentativo di intrusione.

Allegato 6 - Galateo della comunicazione digitale

Si elenca, di seguito, una serie di suggerimenti comportamentali e accorgimenti espressivi per un utilizzo consono degli strumenti di comunicazione digitale (mail, chat, sistemi di web conference).

Con riferimento alla posta elettronica:

- indicare nel campo “oggetto” l’argomento del messaggio in modo chiaro e conciso;
- scrivere il corpo del messaggio in modo sintetico, seguendo un ordine logico preciso e comprensibile;
- evitare espressioni vaghe o indeterminate, per non incorrere in fraintendimenti;
- evidenziare la presenza di allegati, indicandone il contenuto e se necessitano di lettura immediata;
- utilizzare un linguaggio adeguato all’interlocutore, non eccedendo in tecnicismi o formalismi burocratici e utilizzando toni e termini che non risultino offensivi o polemici;
- prima di rispondere a un messaggio, assicurarsi di averlo letto accuratamente e compreso;
- riportare sempre in fondo al messaggio il proprio nominativo, anche nel caso in cui si stia utilizzando una casella di posta condivisa;
- rileggere e controllare il proprio messaggio prima di inviarlo, prestando sempre attenzione alla grammatica, alla punteggiatura e alla coniugazione dei verbi, per non dare un’impressione di scarsa accuratezza;
- prima di inviare un messaggio, assicurarsi di spedirlo solo ai soggetti effettivamente interessati;
- rispondere preferibilmente solo al mittente, coinvolgendo altri soggetti solo se necessario;
- inserire allegati (soprattutto di grandi dimensioni) solo se gli stessi non risultano disponibili in spazi di condivisione aziendale o reperibili in rete;
- chiedere al destinatario la conferma di lettura unicamente se necessario.

Con riferimento ai servizi messaggistica istantanea (chat):

- per comunicazioni brevi, preferire tali servizi alla posta elettronica;
- mantenere aggiornato il proprio stato di presenza e/o disponibilità;
- controllare lo stato di presenza degli utenti con cui si vuole comunicare, evitando, quando non necessario, di attivare una comunicazione sincrona se l’utente è già occupato.

Con riferimento alle riunioni in videoconferenza:

- mantenere il proprio microfono silenziato, a meno che non si debba prendere la parola;
- prima di prendere la parola, utilizzare lo strumento “alzata di mano” e attendere il proprio turno per prendere la parola, evitando di interrompere o di sovrapporsi a chi sta già parlando;
- utilizzare la chat di riunione in modo selettivo, salvo che sia necessario rivolgersi a tutti i partecipanti alla riunione;
- aver cura, durante l’utilizzo della webcam in presenza, di evitare inquadrature che ledano la riservatezza di persone non coinvolte nella conversazione.