**INDICE**



| Rev | Data | Motivo | Pagina |
|---|---|---|---|
| 00 | 22/04/2021 | Emissione | Tutte |

| REDAZIONE | VERIFICA | APPROVAZIONE |
|---|---|---|
| Direttore CSI | Responsabile Sistema Qualità | Direttore Generale |
| Ing. Giovanni Marconi | Prof.ssa Lucia Aquilanti | Dott. Alessandro Iacopini |
| ..... | ..... | ..... |

## 1. SCOPO DEL PROCESSO

- Gestione delle procedure di sicurezza informatica adottate dall'Ateneo

## 2. INPUT

- Una persona può richiedere di usufruire di servizi da parte dell'Ateneo, nella maggior parte dei casi per l'accesso alla rete interna ed esterna (tramite rete Garr) o per l'accesso a dispositivi come laboratori o computer personali in dotazione.

## 3. OUTPUT

- L'erogazione del servizio secondo criteri di sicurezza informatica

## 4. UTENTE FINALE

- Coincide con il richiedente, quindi tutto il personale interno ed esterno che richiede un servizio all'Ateneo

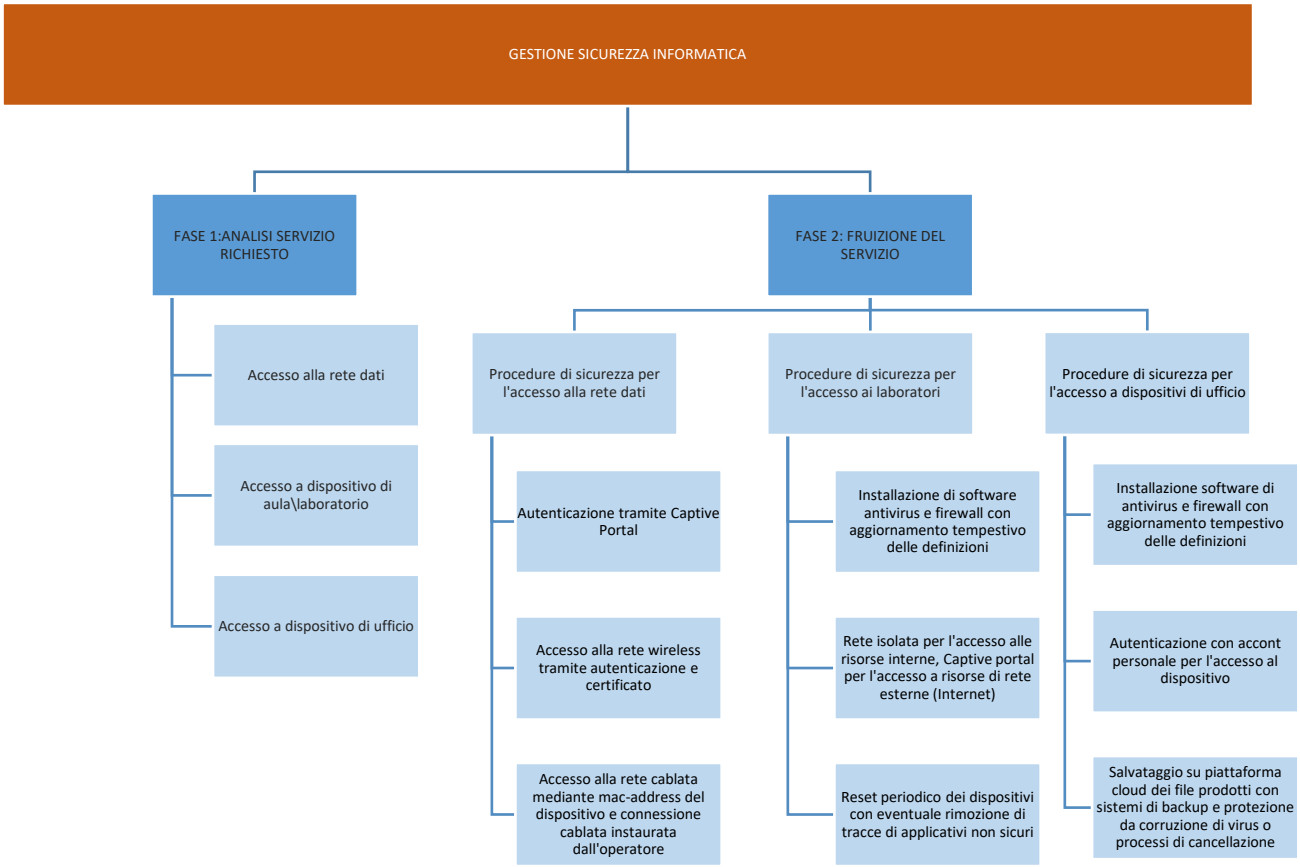
## 5. INDICATORI DI PERFORMANCE

- Percentuale di pc aggiornati alla versione raccomandata del software di Antivirus Symantec

## 6. ABBREVIAZIONI

- CSI Est = Operatore del CSI che supporta l'attività di registrazione degli utenti esterni
- CSI Rete = Operatore del CSI che supporta l'attività di controllo e risoluzione dei problemi di accesso alla rete
- RIC= Richiedente
- RES=Responsabile esterno referente della creazione di utenti esterni

## 7. WORK BREAKDOWN STRUCTURE



## 8. DESCRIZIONE DEL PROCESSO

Nella fase 1 avviene l'analisi della richiesta da parte dell'utente che vuole usufruire di un servizio offerto dall'Ateneo. Sono state individuati 3 scenari:

- Accesso con proprio dispositivo alla rete di Ateneo: è lo scenario più frequente, l'accesso può avvenire mediante:
    - Accesso alla rete wireless: in questo caso l'utente deve installare sul proprio dispositivo un apposito certificato, quindi è richiesta l'autenticazione tramite le proprie credenziali di Ateneo.
    - Accesso alla rete cablata: in questo caso l'utente si collega ad un cavo di rete appositamente predisposto dal tecnico di riferimento. Il computer che si vuole collegare deve disporre di un indirizzo IP valido oppure può ottenerlo tramite servizio DHCP. In questo secondo caso è necessario che il mac address della scheda di rete del computer che si vuole utilizzare sia registrato nei sistemi informativi del CSI per consentire al DHCP di assegnare l'indirizzo. La comunicazione del MAC Address può avvenire tramite mail o altri canali. Una volta registrato il computer potrà accedere alle risorse di rete locali;
    - Accesso alla rete esterna tramite captive portal: per i dispositivi collegati mediante cablaggio di rete è necessaria una ulteriore autenticazione tramite captive portal con le credenziali di Ateneo per l'accesso alle risorse esterne. Una volta autenticato il captive portal dovrà restare necessariamente attivo per tutta la durata della connessione. Nel caso venga chiuso la connessione in ingresso o in uscita sarà interrotta
- Accesso a dispositivi di aula\laboratorio. In questo scenario l'utente (solitamente uno studente) accede ad un dispositivo di laboratorio. I dispositivi in questo contesto sono installati appositamente per il funzionamento in sicurezza mediante applicativi antivirus e firewall. Inoltre la rete del laboratorio è una rete apposita isolata da reti esterne per non consentire agli utenti la visibilità di risorse esterne a quelle necessarie per la finalità del laboratorio. Infine per l'accesso alla rete esterna è comunque richiesta l'autenticazione dell'utente mediante il captive portal descritto nei paragrafi precedenti. Infine i dispositivi di laboratorio sono periodicamente resettati, operazione che oltre a mantenere efficiente la macchina ed eliminare file o applicazioni non più necessarie consente anche di rimuovere eventuali file pericolosi o applicativi che possano aumentare la vulnerabilità del dispositivo.
- Accesso a dispositivi di ufficio. In questo scenario l'utente è solitamente il dipendente che nel suo ufficio utilizza il computer in dotazione. In questo caso il dispositivo consente l'accesso solo mediante autenticazione e sono di default installati applicativi di sicurezza come antivirus e firewall. I file e documenti di lavoro sono poi protetti ulteriormente da un salvataggio automatico in cloud che oltre a preservare i dati da perdita accidentali ne consente anche una gestione completa in termini di controllo degli accessi (per cui è possibile impostare per ogni file gli utenti autorizzati) sia alla protezione rispetto all'accesso da parte di virus che vanno a cancellare o criptare la documentazione a scopi di estorsione; i documenti salvati sul cloud consentono un recupero più semplice e sicuro nel caso di dispositivi compromessi

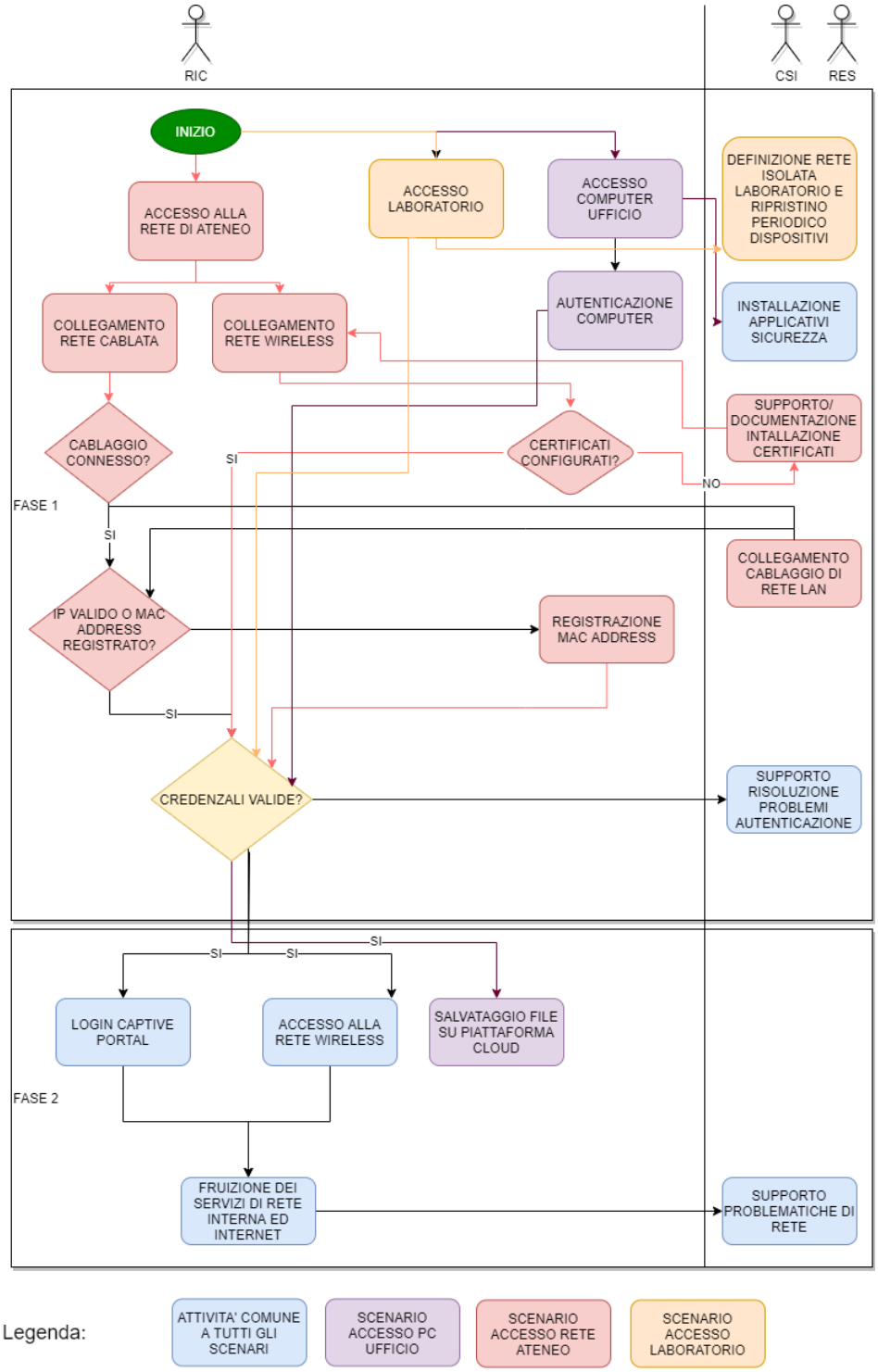
## 9. MATRICE DI RESPONSABILITÀ

| WBS | | METODOLOGIA OPERATIVA | TEMPISTICA | ATTORI | | |
|---|---|---|---|---|---|---|
| FASI | ATTIVITA' | | | RIC | CSI | RES |
| 1 | Collegamento alla rete wireless | | | E | S | |
| 1 | Collegamento alla rete dati cablata | | | E | E | |
| 1 | Accesso a laboratorio | | | E | S | |
| 1 | Accesso a computer ufficio | | | E | E | |
| 2 | Fruizione dei servizi di rete tramite rete Wireless | | | E | S | |
| 2 | Fruizione dei servizi di rete Internet tramite Captive Portal | | | E | S | |
| 2 | Accesso alla rete cablata con proprio dispositivo | | | E | E | A |
| 2 | Accesso al dispositivo del laboratorio | | | E | S | |
| 2 | Installazione antivirus\firewall sul dispositivo di laboratorio | | | | E | |
| 2 | Reset dispositivo laboratorio | | | | E | |
| 2 | Accesso autenticato al pc di ufficio | | | E | S | |
| 2 | Installazione software antivirus\firewall sul pc di ufficio | | | | E | |
| 2 | Salvataggio documenti su piattaforme cloud | | | E | S | |

LEGENDA:

| | | | |
|---|---|---|---|
| **E** = esegue | **I** = viene informato | **S** = Supporta | **A** = approva |

## 10. DIAGRAMMA DI FLUSSO




Legenda: