Regolamento per l'accesso alla rete informatica dell'Osservatorio Astronomico di Cagliari

Acceptable Use Policy V5

Norme di utilizzo, raccomandazioni, considerazioni pratiche

Selargius (CA), Aprile 2017

Indice

Introduzione

Questo documento contiene le linee guida per l'uso della rete di trasmissione dati dell'INAF - Osservatorio Astronomico di Cagliari (OAC).

Poiché la rete locale dell'OAC è collegata alla rete GARR[1], e tramite il GARR alla rete pubblica Internet, l'utilizzo della rete è soggetta alle norme GARR e alle leggi in vigore (vedi Appendice B).

Lo scopo principale del documento è rendere consapevoli gli utenti delle potenzialità, dei limiti e delle possibili responsabilità nell'uso della rete.

Qualunque documento che si proponesse di stabilire regole definitive di utilizzo di mezzi informatici, ben presto sarebbe superato dallo sviluppo della tecnologia.

Di conseguenza questa nota intende richiamare i principi generali, specificando alcuni casi attuali e rimanda ad aggiunte specifiche ogni qualvolta sia necessario aggiornare l'applicazione delle regole generali**.**

1GARR: è la rete Italiana dell'Università e della Ricerca

Principi generali

I principi alla base dell'utilizzo corretto della rete locale dell'OAC sono:

- La rete è a disposizione dei ricercatori, del personale tecnico-amministrativo, degli studenti e ospiti dell' OAC, per un uso strettamente coerente alle finalità proprie dell'Ente.
- Ogni uso diverso che interferisca con l'uso istituzionale degli altri utenti non è accettabile. L'uso personale è tollerato e permesso secondo i criteri descritti nel §4.2.

Definizioni

La rete locale dell'OAC.

La rete locale dell'OAC, nel seguito semplicemente la LAN, è un'infrastruttura fisica e logica che permette l'interconnessione di stazioni di lavoro, detti anche nodi, per la trasmissione dati fra loro e con la rete nazionale della ricerca GARR. Tramite l'infrastruttura del GARR viene garantito il collegamento ad Internet.

Utenti

Sono **utenti regolari:** i dipendenti dell'OAC.

Sono **utenti temporanei:** gli studenti, i dottorandi, i titolari di borse post-dottorato e di assegni di ricerca, gli specializzandi ecc., nonché i collaboratori esterni impegnati nelle attività istituzionali svolte dall'OAC, finché sono nello stato di collaborazione.

Accesso ed uso accettabile

Accesso ed uso individuale della rete

La rete può essere utilizzata esclusivamente per l'attività didattica, scientifica e tecnico-amministrativa di interesse dell'OAC.

Ogni utilizzatore della LAN è tenuto a adottare le necessarie misure per non interferire nel corretto funzionamento delle comunicazioni, per garantire l'integrità dei sistemi e l'accesso alle risorse da parte degli altri utenti ed evitare che le attività svolte producano disturbo o danni agli altri utenti.

Qualsiasi accesso alla LAN deve essere associato ad una persona fisica cui imputare le attività svolte utilizzando il nome utente, il sistema personale, il sistema server, l'accesso remoto, l'indirizzo TCP/IP.

Per il solo fatto di utilizzare la LAN, gli utenti accettano senza riserve il presente regolamento ed il regolamento del GARR e si assumono la totale responsabilità delle attività che svolgono tramite la LAN.

Uso personale della rete

Si definisce personale qualunque uso della LAN che non sia per attività didattica, di ricerca o comunque nell'interesse dell'OAC.

L'uso personale della rete è tollerato purché:

- non sia a scapito dei compiti istituzionali, inclusi quelli degli altri utenti,
- non sia avvertibile da altri utenti e/o costituisca un carico per la LAN;
- non costituisca un'attività politica, commerciale o comunque con profitto;
- non sia offensiva;
- non violi le norme GARR (Appendice B) e le leggi in vigore, come violazione dei diritti di autore, pornografia con minori ecc.
- rispetti la direttiva del Ministro Brunetta sull'utilizzo di strumenti informatici sui luoghi di lavoro pubblico.

Abusi

Costituisce abuso:

- qualsiasi atto che possa compromettere la sicurezza e la riservatezza delle risorse informatiche dell'OAC attraverso la LAN;
- l'accesso, l'utilizzazione, la distruzione, l'alterazione o la disabilitazione non autorizzata di risorse informatiche, anche per mezzo di chiavi di accesso (password, badge, ecc.) rese disponibili ad altri soggetti, nonché l'abbandono senza custodia di stazioni di lavoro già connesse a risorse informatiche riservate;
- la duplicazione, l'archiviazione e l'uso di software su qualsiasi risorsa informatica dell'OAC in violazione a disposizioni contrattuali;
- l'utilizzazione per scopi di interesse esclusivamente privato di qualsiasi risorsa informatica dell'OAC;
- qualsiasi atto che, tramite la LAN, possa recare disturbo o danni a terzi; ad esempio sono abusi la diffusione indiscriminata di e-mail tramite la LAN, "catene" di e-mail, applicazioni non autorizzate con elevata occupazione di banda, attacchi di "denial-of-service", ecc.
- l'uso di dati o di altre risorse informatiche per scopi non consentiti dalle norme vigenti o in contrasto con le norme del presente documento;
- Il collegamento peer-to-peer (o file-sharing) quando finalizzato allo scambio indiscriminato di file coperti da diritto d'autore (a titolo di esempio non esaustivo: file MP3 contenenti canzoni o album, filmati AVI, MPEG o altro formato estratti da supporti commercializzati da case cinematografiche, materiale bibliografico, software licenziato o crack software ecc.) tramite l'utilizzo di programmi di pubblico dominio e gratuiti (ad esempio: eMule, Kazaa, Gnutella ecc.). Poiché molte di queste applicazioni di file-sharing funzionano solo se è abilitata l'opzione di condivisione delle proprie librerie con gli altri peers, gli utenti di tali applicazioni cadono più o meno consapevolmente nella violazione della legge sul diritto d'autore (Legge 22 aprile 1941 n. 633), sia mettendo a disposizione le proprie collezioni di audio, video, software ecc. (anche se regolarmente acquistate), sia scambiando copie illegittime ottenute da terzi (via rete e non).

Provvedimenti e sanzioni

Gli abusi ripetuti a danno di altri gestori di reti o utenti della rete Internet possono provocare la disconnessione d'autorità di tutta la LAN dal GARR fino a completa bonifica.

E' evidente a tutti che un'eventualità del genere avrebbe gravi conseguenze.

La connessione alla LAN di qualunque dispositivo informatico deve essere attuata seguendo alcune prescrizioni che assicurino il corretto funzionamento dell'apparato da connettere, ma soprattutto non causino malfunzionamenti della rete, disturbi involontari o impediscano ad altri utenti di connettersi in rete.

Tra le più comuni configurazioni scorrette, da evitare tassativamente, citiamo le seguenti:

- indirizzo di rete errato o attribuzione autonoma di un indirizzo già assegnato. Questo errore, estremamente grave, impedisce il corretto funzionamento del PC con i numeri duplicati;
- errore nell'indirizzo del gateway o del DNS. La conseguenza è l'impossibilità di connettersi in rete è la generazione di traffico spurio con aggravio del carico sulla dorsale;
- configurazione della postazione di rete come "open relay". La conseguenza di tale imperfetta configurazione è la possibilità offerta a chiunque, anche a utenti fuori della LAN, di utilizzare la postazione come "mail relay" per effettuare "spamming". Lo spamming, in breve la diffusione di e-mail tramite meccanismi automatici, genera non solo traffico e ricevimento di e-mail indesiderate sulla nostra rete, ma potenzialmente su altre reti connesse ad Internet. Se il fenomeno non dovesse essere controllato e bloccato, l'intera LAN potrebbe essere "isolata" di autorità dal GARR. La configurazione di rete di ogni macchina dell' OAC deve essere eseguita da personale del CED.

Nel caso di abusi segnalati dal servizio GARR-CERT o da altri gestori di reti che siano documentati da log-file, si provvederà a limitare la connessione alla LAN interna e contestualmente si notificherà al responsabile del nodo la segnalazione via e-mail. Nel caso in cui vi siano segnalazioni di violazioni di norme di legge, ad esempio violazione dei diritti di autore, oltre a isolare il nodo dalla LAN, il responsabile del CED notificherà la segnalazione al responsabile del nodo con lettera o e-mail ed invierà al Direttore dell'OAC copia della segnalazione.

L'uso non autorizzato della LAN o la violazione delle regole GARR o violazioni di norme di legge può condurre ad azioni disciplinari ed in alcuni casi ad azioni legali.

Informazioni pratiche

Utilizzo degli account

Gli account sul server di posta elettronica, su altri server dell'OAC e sulle proprie postazioni di lavoro ad accesso singolo o multiutente sono ad uso personale. L'utente è quindi tenuto a tutelare il proprio account e postazioni di lavoro entro i limiti del possibile utilizzando password di accesso non facilmente individuabili (ad esempio contenenti lettere maiuscole o caratteri numerici e punteggiatura, della lunghezza minima di 8 caratteri), non diffondendole a terzi e non consentendo l'accesso indiscriminato al proprio account. Secondo le leggi vigenti ogni utente deve essere tracciabile ed è personalmente responsabile del proprio nodo collegato alla LAN e di qualsiasi azione compiuta attraverso il nodo stesso. La presenza di ospiti temporanei che necessitino di accesso alla LAN con strumenti propri o dell' OAC deve essere perlomeno segnalata al personale CED.

Raccomandazioni per la sicurezza in rete

La maggior parte dei virus si diffonde attraverso Internet. Un primo metodo di diffusione sfrutta vulnerabilità note di sistemi operativi, è pertanto buona norma tenere sempre aggiornato il proprio PC installando di volta in volta le patch segnalate. Un altro metodo di diffusione è la posta elettronica attraverso allegati (attachment). Il server di posta elettronica dell'OAC ha un software di protezione che normalmente è in grado di identificare e-mail infetti e di inviare automaticamente un avviso. Poiché compaiono sempre nuovi virus, è possibile che l'antivirus non sia aggiornato. Di conseguenza non aprite gli allegati se non li attendete, anche se l'e-mail proviene da un mittente da voi conosciuto.

E' meglio controllare prima con il mittente. Infine è buona norma non scaricare file o programmi da siti che non siano ufficiali e affidabili. La protezione dai virus e da abusi come lo spamming (invio di posta non desiderata) richiede la collaborazione attiva di tutti gli utenti. Si raccomanda in particolare di installare sul proprio PC i sistemi operativi più recenti o comunque con le patch di sicurezza periodicamente rilasciate.

Informazioni sulla protezione da virus sono ottenibili al sito del GARR: www.cert.garr.it

Si sottolinea inoltre che quasi tutti gli avvisi di virus che arrivano via e-mail sono falsi (hoax), che inducono l'utente a cancellare o sostituire file di sistema assolutamente legittimi, compromettendone il buon funzionamento. Simili considerazioni spesso riguardano le "catene di

Sant'Antonio" recanti messaggi allarmistici su prodotti commerciali, messaggi di richieste di aiuto di tipo medico o che assicurano il versamento di una somma di denaro ad associazioni benefiche per ogni e-mail diffuso.

Queste catene oltre a generare carico sulla rete costituiscono una potenziale fonte di indirizzi e-mail per gli spammer, che li estraggono dal corpo del messaggio. Perciò prima di procedere con la cancellazione di file di sistema o con la diffusione di messaggi potenzialmente falsi controllate la loro validità sul sito: http://www.f-secure.com/virus-info/hoax/

Nell'eventualità che il vostro PC sia stato in qualche modo compromesso, per riottenerne il controllo è opportuno seguire nell'ordine i seguenti passi:

- disconnettere il PC dalla rete,
- analizzare l'intrusione: se vi sono modifiche di sistema, di dati o se l'intrusione ha installato file come sniffer, trojan horse, backdoor ecc. Se possibile occorre individuare la fonte dell'infezione e eliminarla per non rischiare di ricompromettere il PC copiando sulla nuova installazione anche il file infettante insieme ai dati salvati;
- informare l'Help Desk dell'intrusione ed eventualmente richiederne l'assistenza, ripristinare il sistema installando una versione sicura del sistema operativo, disabilitare i servizi non indispensabili, installare i pacchetti di sicurezza, cambiare password su tutti gli account;
- riconnettere il sistema alla rete solo dopo i passi precedenti.

Registrazione di un nodo, indirizzo IP di un client o server

Ai fini del presente paragrafo si intende per:

- CLIENT, un PC o apparato che accede a risorse in rete, sia all'interno sia all'esterno della LAN; tale configurazione è la più diffusa (circa il 90% dei PC connessi). Ad esempio, un PC che naviga le pagine web di www.oa-cagliari.inaf.it e/o www.google.it, che abbia installato un programma di posta elettronica (Eudora, Thunderbird, Outlook o altri), o che abbia installato il programma di contabilità dell'INAF
- SERVER, un PC o apparato che abbia attivi servizi di rete per altri CLIENT, sia verso la LAN, sia verso la rete GARR/Internet. A titolo di esempio non esaustivo, ricadono in questo caso i PC con installato: software WWW server (httpd), FTP server (ftpd), DNS server, MAIL server, ecc.). Costituiscono un eccezione i servizi destinati a utenti della stessa LAN (ad esempio la condivisione di file e stampanti all'interno della stessa rete locale). Da un

punto di vista tecnico, un CLIENT non ha servizi attivi sulle proprie porte TCP/UDP disponibili verso l'esterno della propria rete locale, mentre il server sì; ai SERVER è permesso tutto quanto detto per i CLIENT, nonché la disponibilità di servizi verso l'esterno della propria rete locale.

Qualunque nodo per poter comunicare in rete deve essere configurato con un indirizzo di rete sia numerico che nominativo. Gli indirizzi numerici, o indirizzi IP, e gli indirizzi nominativi si ottengono dal personale del CED. E` fatto divieto assoluto configurare un qualunque nodo con un indirizzo scelto a caso.

Registrazione di un nuovo account

La richiesta di assegnazione di un nuovo indirizzo IP, di account di posta elettronica o altro, va fatta compilando un apposito modulo messo a disposizione dal CED, che riporta referente INAF, periodo di utilizzo delle risorse, e visto dell'Amministrazione o della Direzione.

A decorrere dalla data di scadenza vengono concessi due mesi solari di proroga, trascorsi i quali l'account viene definitivamente rimosso. L'eventuale rinnovo dev'essere richiesto entro tale periodo, con le stesse modalità che si applicano alle nuove richieste.

Accesso Wi-Fi

Il CED fornisce il servizio Wi-Fi, che va richiesto con le stesse modalità dell'accesso alla LAN cablata. É pertanto proibita l'implementazione individuale di access point Wi-Fi.

Monitoraggio della rete

Le ultime disposizioni di legge impongono la registrazione e la conservazione per 36 mesi dei log di sistema di tutto il traffico telematico che avviene nella rete, nonché l'identificazione di un responsabile per ogni nodo che viene collegato alla rete tramite un indirizzo IP. Questo implica che rimane traccia di tutte le transazioni che vengono fatte dalla LAN a Internet. In caso di incidente informatico grave o di segnalazione alle autorità competenti da parte di terzi danneggiati, l'Autorità competente può richiedere ai responsabili della rete la consegna dei log e compiere una analisi dettagliata del tipo di traffico svolto.

APPENDICI

Appendice A: - Riferimenti legislativi

- Legge n. 633 del 22/4/1941: Protezione del diritto d'autore e di altri diritti concessi al suo esercizio. Gazzetta Ufficiale n.166 del 16 luglio 1941
- Legge n. 159 del 22/5/1993: Norme in materia di abusiva riproduzione di opere librarie....Gazzetta Ufficiale n. 122 del 27 maggio 1993
- Legge n.248 del 18/8/2000: Nuove norme di tutela del diritto di autore. Gazzetta Ufficiale n.205 del 4 settembre 2000
- DL n. 518 del 29/12/1992: Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore.
- Legge n. 547 del 23/12/1993: Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica.
- Legge N°. 196/2003 intitolato "Codice in materia di protezione dei dati personali".
- DPR n. 318 del 28/7/1999: Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675.
- DPR n.137 del 7/4/2003: Regolamento recante disposizioni di coordinamento in materia di firme elettroniche. Gazzetta Ufficiale n.138 del 17/6/2003

Appendice B: - Acceptable Use Policy (AUP) del GARR

1. La Rete Italiana dell'Università e della Ricerca, denominata comunemente "Rete GARR", si fonda su progetti di collaborazione di ricerca ed accademica tra le Università, le Scuole e gli Enti di Ricerca pubblici italiani. Di conseguenza il servizio di Rete GARR è destinato principalmente alla comunità che afferisce al Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR). Esiste tuttavia la possibilità di estensione del servizio stesso anche ad altre realtà, quali quelle afferenti ad altri Ministeri che abbiano una Convenzione specifica con il Consortium GARR, oppure realtà che svolgono attività di ricerca in Italia, specialmente, ma non esclusivamente, in caso di organismi "no-profit" impegnati in collaborazioni con la comunità afferente al MIUR. L'utilizzo della Rete è comunque soggetto al rispetto delle Acceptable Use Policy (AUP) da parte di tutti gli utenti GARR.
2. Il "Servizio di Rete GARR", definito brevemente in seguito come "Rete GARR", è costituito dall'insieme dei servizi di collegamento telematico, dei servizi di gestione della rete, dei servizi applicativi e di tutti quelli strumenti di interoperabilità (operati direttamente o per conto del Consortium GARR) che permettono ai soggetti autorizzati ad accedere alla Rete di comunicare tra di loro (Rete GARR nazionale).
   Costituiscono parte integrante della Rete GARR anche i collegamenti e servizi telematici che permettono la interconnessione tra la Rete GARR nazionale e le altre reti.
3. Sulla rete GARR non sono ammesse le seguenti attività:
   - fornire a soggetti non autorizzati all'accesso alla Rete GARR il servizio di connettività di rete o altri servizi che la includono, quali la fornitura di servizi di housing, di hosting e simili, nonchè permettere il transito di dati e/o informazioni sulla Rete GARR tra due soggetti entrambi non autorizzati all'accesso sulla Rete GARR (third party routing);
   - utilizzare servizi o risorse di Rete, collegare apparecchiature o servizi o software alla Rete, diffondere virus, hoaxes o altri programmi in un modo che danneggi, molesti o perturbi le attività di altre persone, utenti o i servizi disponibili sulla Rete GARR e su quelle ad essa collegate;
   - creare o trasmettere (se non per scopi di ricerca o comunque propriamente in modo controllato e legale) qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza o il credo;
   - trasmettere materiale commerciale e/o pubblicitario non richiesto ("spamming"), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività;
   - danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di parole di accesso (password), chiavi crittografiche riservate e ogni altro “dato personale” come definito dalle leggi sulla protezione della privacy;
   - svolgere sulla Rete GARR ogni altra attività vietata dalla Legge dello Stato, dalla normativa Internazionale, nonchè dai regolamenti e dalle consuetudini ("Netiquette") di utilizzo delle reti e dei servizi di Rete cui si fa accesso.

4. La responsabilità del contenuto dei materiali prodotti e diffusi attraverso la Rete è delle persone che li producono e diffondono. Nel caso di persone che non hanno raggiunto la maggiore età, la responsabilità può coinvolgere anche le persone che la legge indica come tutori dell'attività dei minori.
5. I soggetti autorizzati (S.A.) all'accesso alla Rete GARR, definiti nel documento "Regole di accesso alla Rete GARR", possono utilizzare la Rete per tutte le proprie attività istituzionali. Si intendono come attività istituzionali tutte quelle inerenti allo svolgimento dei compiti previsti dallo statuto di un soggetto autorizzato, comprese le attività all'interno di convenzioni o accordi approvati dai rispettivi organi competenti, purchè l'utilizzo sia a fini istituzionali. Rientrano in particolare nelle attività istituzionali, la attività di ricerca, la didattica, le funzioni amministrative dei soggetti e tra i soggetti autorizzati all'accesso e le attività di ricerca per conto terzi, con esclusione di tutti i casi esplicitamente non ammessi dal presente documento.
   Altri soggetti, autorizzati ad un accesso temporaneo alla Rete (S.A.T.) potranno svolgere solo l'insieme delle attività indicate nell'autorizzazione.
   Il giudizio finale sulla ammissibilità di una attività sulla Rete GARR resta prerogativa degli Organismi Direttivi del Consortium GARR.
6. Tutti gli utenti a cui vengono forniti accessi alla Rete GARR devono essere riconosciuti ed identificabili. Devono perciò essere attuate tutte le misure che impediscano l'accesso a utenti non identificati. Di norma gli utenti devono essere dipendenti del soggetto autorizzato, anche temporaneamente, all'accesso alla Rete GARR.
   Per quanto riguarda i soggetti autorizzati all'accesso alla Rete GARR (S.A.) gli utenti possono essere anche persone temporaneamente autorizzate da questi in virtù di un rapporto di lavoro a fini istituzionali. Sono utenti ammessi gli studenti regolarmente iscritti ad un corso presso un soggetto autorizzato con accesso alla Rete GARR.
7. È responsabilità dei soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR di adottare tutte le azioni ragionevoli per assicurare la conformità delle proprie norme con quelle qui esposte e per assicurare che non avvengano utilizzi non ammessi della Rete GARR. Ogni soggetto con accesso alla Rete GARR deve inoltre portare a conoscenza dei propri utenti (con i mezzi che riterrà opportuni) le norme contenute in questo documento.
8. I soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR accettano esplicitamente che i loro nominativi (nome dell'Ente, Ragione Sociale o equivalente) vengano inseriti in un annuario elettronico mantenuto a cura degli Organismi Direttivi del Consortium GARR.
9. In caso di accertata inosservanza di queste norme di utilizzo della Rete, gli Organismi Direttivi del Consortium GARR prenderanno le opportune misure, necessarie al ripristino del corretto funzionamento della Rete, compresa la sospensione temporanea o definitiva dell'accesso alla Rete GARR stessa.
10. L'accesso alla Rete GARR è condizionato all'accettazione integrale delle norme contenute in questo documento.