UNIVERSITA' DEGLI STUDI DI PARMA

NORME DI ATTUAZIONE DEL REGOLAMENTO DI ACCESSO AI SERVIZI DI RETE

SOMMARIO

INFORMAZIONI PRELIMINARI

Art. 1 - Oggetto ed ambito di applicazione

Il presente documento, di seguito indicato con il termine Norme, contiene la descrizione dell'architettura di sicurezza dei servizi di rete di Ateneo e le norme tecniche per l'attuazione del "Regolamento di accesso ai servizi di rete dell'Ateneo di Parma ", di seguito indicato con il termine Regolamento, ed ha quindi lo stesso ambito di applicazione.

Le Norme recepiscono ed aggiornano i documenti di coordinamento tecnico dei servizi di rete precedentemente predisposti dal Centro di Calcolo Elettronico (Circolari Tecni-

che di Rete).

Art. 2 - Definizioni

Applicazioni ad alto impatto sulla rete

Programmi che richiedano una significativa disponibilità di banda sulla dorsale di
Ateneo (es. videoconferenza su IP, multimedialità, realtà virtuale, etc.).

Client
Un host che utilizza un servizio di rete.

Dispositivo di rete
Router, switch, modem o qualunque apparecchiatura che permetta di estendere la rete
di Ateneo.

Domain Name Service di Ateneo: l'insieme dei server di Ateneo autorizzati alla
traduzione degli indirizzi Ip nei corrispondenti nomi di host e viceversa.

Firewall
Un sistema di restrizione degli accessi tra Internet e la rete del Polo GARR-PARMA

Host
Un computer connesso alla rete.

Internet
L'insieme mondiale di tutte le reti interconnesse tra di loro. Internet è per definizione
untrusted e nell'ambito delle Norme coincide con tutte le reti diverse dal quelle del Polo
GARR-PARMA.

Proxy server
Un server Internet che abilita e filtra un servizio di rete tra Internet e la rete del Polo
GARR-PARMA.

Rete di Ateneo (intranet)
E' la rete di trasmissione dati che interconnette tutti gli insediamenti dell'Università di

Parma. Il nome del dominio è unipr.it. La trasmissione verso l'esterno è realizzata
mediante linee dedicate attestate sui router del Centro di Calcolo Elettronico e in piccola
parte tramite accessi commutati.

Rete di backbone (dorsale)
Collegamento principale tra i router intranet e router esterno.

Rete del Polo GARR-PARMA
E' l'insieme delle reti di trasmissione dati costituita dalla rete di Ateneo più le reti locali
o i punti di accesso alla rete GARR nazionale appartenenti agli altri membri del Polo
GARR PARMA. La numerazione pubblica registrata al NIC è la classe B 160.78.0.0. A
questa va aggiunta la classe C 192.135.11.0 assegnata al Gruppo Collegato INFN di
Parma. Esiste anche la numerazione privata (area nascosta)172.28.0.0. Quest'ultima è ad
uso interno, non è cioè riconosciuta al di fuori della rete GARR-PARMA.

Router intranet
Un router eventuale di separazione tra una sottorete interna e la rete di backbone.

Router esterno (screening router)
Router di separazione tra la rete GARR-PARMA ed Internet.

Server Internet
Un server di rete accessibile da Internet.

Server Intranet
Un server di rete visibile solo all'interno della rete del Polo GARR-PARMA.

Server di rete
Un trusted host che offre servizi di rete, sia Internet che Intranet.

Servizi Internet (extranet) di Ateneo
Tutti i servizi di rete erogati da server di Ateneo per Internet.

Servizi intranet di Ateneo
Tutti i servizi di rete con connessioni stabilite esclusivamente tra due

o più host
appartenenti a GARR-PARMA.

Trusted Host
Un dispositivo che appartiene alla rete del Polo GARR-PARMA e soddisfa le condizioni
di sicurezza contenute nelle Norme, con particolare riferimento agli articoli
12, 13, 14, 15, 16, 17.

Art. 3 - Classificazione dei dati

Si definiscono, per gli scopi del presente regolamento, le seguenti tipologie di dati:

dati personali: tutte le informazioni che riguardano la persona, sia dei dipendenti che
degli studenti dell'Ateneo; in particolare ogni messaggio di posta elettronica contenente
informazioni riguardanti il mittente e il destinatario (nome, indirizzo IP, ora dell'invio
del messaggio);

dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni
religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sinda-
cati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale,
nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

dati scientifici: le informazioni riguardanti l'attività didattica e di ricerca dell'Ateneo;

dati amministrativi: informazioni e comunicazioni riguardanti l'amministrazione
dell'Ateneo per il conseguimento dei propri fini istituzionali;

dati riservati: dati amministrativi ad uso interno o coperti dal segreto d'ufficio;

dati critici: le informazioni, le applicazioni informatiche o i sistemi operativi relativi agli
host fornitori di servizi di rete ed a quelli che possono compromettere

significativamente
la sicurezza della rete di Ateneo.

Art. 4 - Classificazione dei soggetti

Si definiscono, per gli scopi del presente regolamento, i seguenti soggetti:

Utente: soggetto con il diritto di accesso ai servizi di rete.

Utenti strutturati: docenti, personale tecnico e amministrativo.

Utenti non strutturati: collaboratori esterni, dottorandi.

Studenti: soggetti regolarmente iscritti ad un corso di laurea o di diploma dell'Ateneo.

di Parma o provenienti da altri Atenei a seguito di scambi nell'ambito di programmi
nazionali ed internazionali.

Amministratore di sistema: la persona che gestisce il sistema operativo dell'elaboratore
che eroga un servizio di rete e, se non diversamente specificato, anche il servizio stesso.

Amministratore di rete: la persona che si occupa della connessione in rete degli
elaboratori appartenenti ad una singola struttura.

Referente di dominio: la persona che si occupa della distribuzione e della gestione degli
indirizzi IP nell'ambito di un dominio assegnato ad una o più strutture.

Responsabile di struttura: il Direttore della struttura che accede a servizi Internet e
Intranet, o che li eroga.

CCE: Centro di Calcolo Elettronico.

Art. 5 - Classificazione dei luoghi d’accesso

Si definiscono, per gli scopi del presente regolamento, i seguenti luoghi di accesso:

Uffici e studi: luoghi riservati al personale strutturato dell'Ateneo ed

eventualmente a
collaboratori temporanei;

Laboratori didattici: luoghi dedicati alle esercitazioni didattiche;

Laboratori di ricerca: luoghi dedicati all'attività di ricerca;

Biblioteche: luoghi di consultazione di materiale librario, cartaceo o digitale;

Spazi comuni: luoghi di passaggio o di incontro dove siano installati terminali di accesso
ai servizi di rete.

Art. 6 - Architettura generale dei servizi di rete

La tecnologia utilizzata per l'implementazione della sicurezza di rete è un sistema
firewall con architettura screened host, realizzata da packet filtering sul router esterno
ed eventualmente integrato da proxy server e da router intranet.

Il sistema firewall applica dei filtri software alle richieste esterne di connessione: ogni
struttura che voglia erogare un servizio di rete visibile da Internet, deve non solo
garantire il rispetto delle norme di sicurezza indicate dal Regolamento e dalle Norme,
ma deve anche avere la necessaria autorizzazione affinché le regole di filtro implemen-.

tate sul router esterno consentano il transito di pacchetti destinati al server che eroga il
servizio. In caso contrario il servizio di rete non è accessibile dall'esterno.

In sintesi:

il firewall è trasparente alle connessioni uscenti, ovvero ogni utente può accedere,
secondo le modalità descritte dalle Norme, ai servizi Internet;

il firewall filtra le connessioni entranti, cioè quelle provenienti da Internet verso i server
Internet di Ateneo, secondo le modalità descritte all'Art. 16 delle Norme;

in entrambi i casi le informazioni relative alle connessioni da e per Internet (durata e tipo
della connessione, mittente e destinatario)vengono registrate e rese disponibili secondo
le modalità descritte dalle Norme;

i servizi di rete sono erogati in forma distribuita: le singole strutture possono fornire
servizi internet/intranet qualora possano garantire i requisiti di sicurezza descritti nel
Regolamento e nelle Norme;

un servizio di rete è accessibile da host esterni alla rete di Ateneo se e solo se - una volta
verificate dal GSI le condizioni di sicurezza - questo viene "autorizzato "dal sistema
firewall: in altre parole, solo le connessioni entranti verso i server di rete ufficiali sono
permesse, le altre vengono bloccate;

i server di rete intranet sono consentiti purché nel rispetto delle condizioni poste dal
Regolamento ma comunque non sono visibili all'esterno della rete di Ateneo.

Art. 7 - Servizi di rete disponibili

I servizi disponibili sulla rete di backbone dell'Ateneo (intranet)sono quelli specifici
della suite di protocolli Tcp/ip. Per sopravvenute esigenze di sicurezza o di necessità,
alcuni servizi possono essere soppressi. Altre suite di protocolli di comunicazione (es.
Appletalk e NetBeui)devono essere mantenute all'interno delle lan interessate o
incapsulate in Tcp/ip.

Per applicazioni ad alto impatto di rete è necessaria l'autorizzazione del CCE.

Art. 8 - Modalità generali di accesso

Le modalità di accesso ai servizi variano a seconda delle classi di utenti e di servizi,
comunque tramite assegnazione di password personali e segrete di

accesso:

studenti
Gli studenti hanno diritto di accedere alle risorse informatiche disponibili per l'attività.

didattica dietro presentazione di una richiesta su apposita modulistica, che può essere
redatta a carico della struttura di afferenza seguendo il prototipo in Appendice I
(Richiesta di Accesso a Laboratori e Servizi);

l'autorizzazione viene rilasciata dal Responsabile di struttura;

gli studenti non possono avere funzioni di gestione di servizi di rete.

utenti strutturati e non strutturati
Gli utenti strutturati e non strutturati hanno diritto di accedere ai servizi di rete dietro
autorizzazione del Responsabile di struttura, eventualmente corredata da opportuna
modulistica (v. Appendice I - Richiesta di Accesso a Laboratori e Servizi);

NORME GENERALI DI CONFIGURAZIONE DEI DISPOSITIVI DI RETE, SERVER E CLIENT

Art. 9 - Norme generali

Su tutti gli host (client, server internet, server intranet)e i dispositivi di rete (router,
switch e modem)devono essere garantiti opportuni meccanismi e procedure di sicurez-
za, adeguati alla loro funzione ed al grado di criticità rispetto alle possibili ripercussioni
sulla collettività accademica in caso di un loro eventuale malfunzionamento.

La connessione di un client alla rete di Ateneo avviene dietro autorizzazione del
Responsabile di Struttura.

I dispositivi di rete e i server possono essere connessi alla rete solo previa autorizzazione
del Direttore del CCE, attraverso l'apposita modulistica.

Il Direttore del CCE è tenuto ad informare il GSI di ogni modifica significativa apportata
all struttura di rete;

I server di rete, sia internet che intranet, devono essere protetti fisicamente da accessi non
autorizzati, ovvero non risiedere in spazi non sorvegliati.

L'accesso ai servizi da elaboratori (client)posti in spazi comuni deve essere ristretto ai
soli servizi preventivamente specificati, conformemente alle norme locali di accesso
emanate dal Responsabile di struttura.

Art. 10 - Assegnazione di indirizzi IP e di Domini

L'assegnazione degli indirizzi IP avviene su disposizione del CCE, il quale demanda ai
Referenti di dominio la gestione delle classi C riservate alla struttura di appartenenza:

è vietato pertanto assegnare un indirizzo IP senza opportuna comunicazione al Referente
di dominio, il quale deve annotare il nominativo dell'utente assegnatario dell'indirizzo.

E' obbligatorio registrare i nomi di host e dispositivi nel Domain Name Service di
Ateneo.

Ogni richiesta di attivazione di Dominio va sottoposta al Comitato GARR PARMA
attraverso il CCE.

Ogni Dominio deve necessariamente avere un Referente, nominato dal Responsabile
della struttura che ne fa richiesta.

Criterio base per l'assegnazione di un nome di Dominio (del tipo "dominio.unipr.it")è
la rilevanza accademica e/o il numero di host appartenenti al Dominio.

E' fatto divieto alle strutture intraprendere autonomamente

procedure di richiesta alle
autorità internazionali di ulteriori numerazioni o domini senza l'autorizzazione del
Comitato GARR PARMA e agli utenti di configurare indirizzi IP senza l'autorizzazione
del proprio Amministratore di Rete.

Art. 11 - Organizzazione degli indirizzi

Ogni sottorete di classe C dovrebbe rispettare le seguenti convenzioni:

- L'indirizzo 254 è sempre associato ad un router;
- Gli indirizzi da 230 a 253 sono riservati a dispositivi di rete;
- Gli indirizzi da 200 a 229 sono riservati a DHCP server;
- Gli indirizzi da 1 a 199 sono riservati a host statici.

Art. 12 - Gestione di username e password

Ogni accesso ai servizi di rete deve avvenire tramite assegnazione di username e di
password segrete e personali; è vietata l'assegnazione di password collettive o non
riconducibili ad un soggetto fisico.

L'Amministratore di sistema, che ha il compito di gestire le modalità di assegnazione e
distribuzione delle password, deve implementare le procedure più opportune per
garantirne l'integrità e la riservatezza.

Gli username devono rispettare i seguenti criteri:

- per utenti strutturati: scadenza di validità alla risoluzione del rapporto di lavoro
con l'Ateneo;
- per utenti non strutturati e per studenti: scadenza periodica, rinnovabile.

Le password devono rispettare i seguenti criteri:

- lunghezza minima 6 caratteri,

• scadenza semestrale e rinnovabile dall'utente;

• titolarità (divieto di uso di password collettive).

Art. 13 - Server di rete internet

Gli elaboratori con funzioni di server internet devono essere autorizzati dal GSI previa
richiesta presentata su appositi moduli (v. Appendice)e devono garantire le seguenti
condizioni:

• aggiornamento periodico del sistema operativo e del software applicativo e
comunque ogniqualvolta il GSI ne riscontri l'opportunità;

• identificazione precisa dei servizi di rete e del sistema operativo offerti e
disabilitazione dei servizi non necessari;

• accesso privilegiato al sistema riservato al solo Amministratore, in modalità locale
o, se remota, in modalità cifrata (ad esempio tramite il protocollo SSH);

• accesso pubblico al sistema solo per i servizi di rete installati;

• adozione di una adeguata e rigorosa normativa di gestione delle password di
accesso, ivi compresa l'attivazione di opportuna modulistica (v. Appendice);

• verifica del timer di sistema;

• configurazione dei meccanismi di logging, in particolare per gli accessi e i servizi;

• configurazione e pianificazione delle procedure di backup;

• mentenimento delle informazioni di logging e di backup per un periodo di tempo
non inferiore a 6 mesi;

• accesso riservato e protetto alle informazioni di logging ed,

eventualmente, di
auditing;

• protezione contro virus informatici;

• protezione fisica da accessi incontrollati;

• adozione di meccanismi adeguati di ripristino del sistema e di rilevazione delle
intrusioni.

La mancata applicazione di queste operazioni può comportare la revoca dell'autorizza-
zione del server da parte del GSI, quindi la non visibilità esterna dei servizi.

Art. 14 - Server di rete intranet

Gli elaboratori con funzioni di server intranet devono essere comunicati al GSI e devono
garantire le seguenti condizioni:

• identificazione precisa dei servizi di rete e dei servizi di sistema offerti e
disabilitazione dei servizi non necessari;

• adozione di regole locali di accesso e di erogazione dei servizi intranet;

• adozione di meccanismi hardware e software atti a delimitare il traffico locale;

• numerazione IP nascosta dei server dei laboratori didattici (172.28.xxx.xxx).

Art. 15 - Client

Sugli elaboratori con funzioni di client, situati in uffici, studi, laboratori e spazi comuni,
devono essere garantite le seguenti condizioni:

• disattivazione di tutti i servizi di rete in modalità server, escluso X11;

• accesso univoco al sistema (account personali e non collettivi);

• codici di accesso a scadenza, per studenti e utenti non

strutturati; disattivazione
automatica degli account (se consentito dal sistema operativo)in caso di mancato
utilizzo per un periodo superiore a 6 mesi;

• riservatezza nell'assegnazione delle password agli utenti;

• numerazione IP nascosta dei client dei laboratori didattici (172.28.xxx.xxx)e di
quelli situati in spazi comuni;

• assegnazione del nome/indirizzo IP da parte del Referente di Dominio e loro
registrazione nel Domain Name Service di Ateneo.

Art. 16 - Router esterno (screening router)

Le regole di filtro applicate su tutti i pacchetti in entrata alla rete del Polo GARR-PARMA
sono le seguenti:

• i pacchetti entranti che dichiarano un indirizzo sorgente appartenente alla classe
di indirizzi 160.78.0.0, 192.135.11.0, 172.28.0.0. (forged source)sono bloccati;

• il source routing è disabilitato;

• ICMP, SSH e tutti i protocolli cifrati non hanno restrizioni;

• i pacchetti di servizi unicast presenti sulla rete di backbone (ad esempio: SMTP,
POP3, IMAP, HTTP, FTP, NNTP, DOMAIN)transitano solo se indirizzati verso i
server di rete autorizzati;

• le porte non privilegiate (>1023)Tcp e Udp non sono filtrate;

• le connessioni Tcp/Ip uscenti non sono filtrate;

• tutti gli altri servizi Tcp/Ip, compreso X11, vengono filtrati (deny any).

Sono ammesse deroghe alle regole di filtro purché opportunamente

documentate ed
approvate dal GSI.

Le informazioni relative alle connessioni da e per Internet (durata e tipo della connes-
sione, mittente e destinatario)vengono registrate e conservate su apposito supporto per
almeno 6 mesi, presso il CCE.

Art. 17 - Router e switch intranet

Sui dispositivi di rete con funzione di router intranet devono essere garantite le seguenti
condizioni:

- filtro su tutti i protocolli non ammessi sul backbone;
- routing abilitato solo per gli host della lan di appartenenza.

NORME GENERALI DI CONFIGURAZIONE DEI SERVIZI DI RETE

Art. 18 - Posta elettronica (smtp, pop, imap)

Il server ufficiale di posta elettronica è installato al CCE: ogni utente strutturato è
reperibile all'indirizzo nome. cognome@unipr.it; gli utenti possono avere indirizzi
diversi da quello ufficiale attraverso un meccanismo di forwarding implementato sul
server ufficiale di Ateneo.

Una struttura può disporre di un proprio server autorizzato di posta elettronica, del
quale il Responsabile deve dare informazione al GSI; è opportuno comunque limitare il
numero di server di posta elettronica locali a non più di uno per struttura: in ogni caso,
il responsabile della Struttura comunicherà al GSI l'installazione e le modifiche succes-
sive.

I server di posta devono avere adeguati meccanismi di sicurezza, in particolare anti-
spamming (presenti in Sendmail a partire dalla release 8. 8. 8)ed evitare, se possibile, il
mail-relay per host esterni alla rete del Polo GARR-PARMA.

Ogni messaggio di posta elettronica viene considerato personale ed è vietata ogni
intercettazione non autorizzata, fatte salve esigenze specifiche del GSI.

La trasmissione non cifrata di informazioni personali o sensibili a mezzo di posta
elettronica è subordinata all'accettazione da parte del mittente della loro vulnerabilità.

La trasmissione di informazioni riservate mediante posta elettronica è subordinata
all'approvazione del Responsabile della struttura.

La trasmissione di posta internet è filtrata dal sistema firewall; ciò significa che solo i
server di posta locali autorizzati sono visibili all'esterno della rete del Polo GARR-
PARMA.

L'accesso ai server di posta elettronica deve gradualmente migrare verso protocolli in
modalità cifrata (ad esempio: SPOP, SIMAP).

Le comunicazioni ufficiali di Ateneo tramite posta elettronica sono autenticate con
sistemi di certificazione interni a chiave asimmetrica, gestiti temporaneamente dal CCE;

la lettura di tali messaggi è dunque certificata solo con i software che prevedano tale
modalità (ad esempio: mail agent di Netscape e Explorer Messanger);

Art. 19 - Risoluzione nomi/indirizzi (dns)

I server dns primari per i domini dell'Ateneo sono:

- 160.78.48.10 (caio.cce.unipr.it);
- 192.135.11.20 (server.fis.unipr.it);
- 160.78.31.139 (habana.cedi.unipr.it).

Una struttura può attivare, previa autorizzazione del GSI, server dns

primari per i
sottodomini assegnati qualora tali server soddisfino i criteri di cui all'Art. 13 ed il
servizio abbia implementato le norme di sicurezza specifiche e aggiornate allo stato
dell'arte;

nel caso si implementi un server dns in ambiente unix, si dovrà configurare il bind
resolver (release non inferiore alla 8. 0. 0)permettendo lo zone-transfer solo verso i server
dns ufficiali di Ateneo;

l'indirizzo dei server dns deve essere comunicato al GSI che provvederà ad autorizzare
il transito dal firewall;

non è possibile assegnare nomi che iniziano con un numero o che contengano caratteri
non alfanumerici (RFC1178).

Art. 20 - Web (http)

Il sito ufficiale dell'Ateneo è www.unipr.it.

Qualora una struttura voglia gestire un proprio server web deve comunicarne l'indiriz-
zo al GSI, il quale provvederà ad autorizzare il transito dal firewall.

L'installazione di un web server deve essere approvata dal Responsabile di struttura.

L'installazione di un web server ufficiale deve essere approvata dal Responsabile di
struttura e deve adeguarsi alle scelte editoriali che l'Ateneo esprime attraverso il
Servizio Relazioni Pubbliche, in particolare per quanto riguarda la grafica dei primi
livelli del sito e per la scelta dei dati da pubblicare.

Un web server non deve coinvolgere attività commerciali, attività a scopo di lucro o
private e non deve costituire potenziale fonte di rischio informatico o provocare caduta
di immagine per l'Ateneo.

Il browsing web personale è ammesso, purché rispetti il Regolamento e comunque non
interferisca con le normali attività istituzionali dell'Ateneo.

Art. 21 - Connessione da Internet (telnet, ftp)

Le connessioni in chiaro entranti da Internet sono consentite solo in fase transitoria e
comunque attraverso proxy; gradualmente i protocolli non cifrati dovranno essere
sostituiti a favore di protocolli cifrati.

Art. 22 - News e servizi di mirror (nntp, ftp anonymous)

Ogni struttura che voglia fornire servizi di news e di mirror deve essere autorizzata dal
CCE ed attenersi al Regolamento.

Art. 23 - Accesso commutato (modem)

Gli accessi commutati (via modem)sono da considerarsi come un'estensione della rete
di Ateneo e pertanto soggetti al Regolamento; in particolare, devono essere richiesti ed
autorizzati dal CCE tramite l'apposita modulistica (vedi Appendice).

Occorre mantenere la documentazione relativa alle persone autorizzate all'accesso e ai
collegamenti effettuati nel corso dell'ultimo anno.

Le apparecchiature di connessione devono rispettare le norme Telecom per la connes-
sione di apparati alla rete pubblica (L. 314 del 23. 5. 92).

Art. 24 - Routing e controllo (rip, igrp, ospf, icmp, snmp)

Solo i router ufficiali possono avere attivati i servizi di routing.

L'installazione di router deve armonizzarsi con le strategie adottate CCE e comunque
previa autorizzazione del Centro medesimo.

I servizi di controllo dei router (SNMP)devono essere attivi.

PIANO OPERATIVO

Art. 25 - Fase preparatoria

Tutte le strutture che accedano ai servizi di rete devono comunicare al CCE e al GSI le
informazioni relative ai servizi internet/intranet erogati alla data di emanazione del.

Regolamento, utilizzando la Modulistica riportata in Appendice; contestualmente
verranno attivati i sistemi di comunicazione per gli Amministratori:

- Censimento dei servizi di rete

Vengono distribuiti i "Moduli di censimento dei servizi di rete "(in Appendice)che
richiederanno ai Responsabili le seguenti informazioni:

piattaforma di erogazione e tipologia dei server
servizi erogati
numero di client e/o utenti afferenti ai servizi erogati
tipologia dei dati trattati
Referente di dominio (se la struttura è assegnataria di uno o più domini)
Amministratore di Rete

- Attivazione di sistemi di comunicazione e di informazione

E' attivata la lista chiusa di discussione netadmin@listserv.unipr.it.

E' attivato il sito www.unipr.it/netadmin nel quale sono contenute tutte le novità, le
indicazioni tecniche e la documentazione relative ai vari aspetti di sicurezza informatica.

Tali strumenti di comunicazione vengono considerati primari ed ufficiali per il coordi-
namento tra gli Amministratori e il GSI.

Art. 26 - Fase di attuazione

Le richieste di erogazione di servizi di rete sono valutate dal CCE e dal GSI, sentiti i
Responsabili di Struttura; l'autorizzazione è comunicata direttamente a quest'ultimi;

ogni Amministratore deve successivamente far pervenire al GSI il

"Modulo di Assun-
zione di Responsabilità " (in Appendice)debitamente compilato e firmato;

ogni Amministratore deve provvedere alla corretta configurazione dei servizi erogati,
con l'adozione dei criteri di sicurezza previsti dalle Norme e dal Regolamento.

Art. 27 - Fase di verifica

Gli Amministratori di sistema dovranno trasmettere al GSI una relazione riepilogativa
contenente tutte le informazioni organizzative e tecniche dei dispositivi e dei servizi di
rete erogati.

- Logging e modalità di accesso ai file di log

Con modalità già attuate a decorrere dal 1 gennaio 2000, i primi 64 byte di ogni pacchetto
transitato dal router esterno vengono registrati da un host posto nel perimetro di
sicurezza (logger). I file di log sono memorizzati su supporto elettronico e conservati per
almeno 6 mesi. Le informazioni di ogni struttura sono accessibili dal relativo Responsa-
bile, dal GSI e, su specifica autorizzazione del Rettore, dal personale con apposite
funzioni di gestione ed amministrazione di servizi di rete.

- Verifica periodica dello stato di sicurezza dei servizi di rete

Periodicamente il CCE può effettuare operazioni di censimento, monitoraggio e verifica
dei servizi di rete erogati dall'Ateneo, anche attraverso scansioni automatiche su tutti i
dispositivi connessi alla rete.

Art. 28 - Rilevazione e gestione degli incidenti per la sicurezza

E' compito degli Amministratori di rete e di sistema predisporre meccanismi tecnici ed
organizzativi per il monitoraggio periodico, anche quotidiano, dei servizi di rete. In caso

di rilevazione di incidente, il GSI e il Responsabile della struttura devono essere avvisati
tempestivamente; a loro volta informeranno il Rettore e le altre strutture potenzialmente
coinvolte e predisporranno le contromisure necessarie.

Gli Amministratori devono provvedere nel più breve tempo possibile al ripristino del
servizio a meno che, di comune accordo con il GSI e con il Responsabile di struttura, non
si decida prioritariamente di individuare la causa dell'incidente interrompendo tempo-
raneamente il servizio stesso.

L'Amministratore di sistema deve salvare i file modificati prima del loro ripristino e
comunque mantenere adeguatamente le informazioni utili per la descrizione dell'inci-
dente.

Art. 29 - Sanzioni

Il mancato rispetto delle Norme e del Regolamento comporterà per i trasgressori la
temporanea sospensione dei servizi di rete.

Se la situazione di conflitto generata dalla non osservanza delle Norme e del Regolamen-
to persisterà per tempi ritenuti non giustificati a giudizio del GSI, si provvederà a darne
opportuna comunicazione al Rettore.

Qualora il conflitto generato dalla non osservanza delle Norme e del Regolamento abbia.

ripercussioni esterne o possa comportare anche sanzioni civili e/o penali da parte delle
Autorità competenti, l'Ateneo si riserva di adottare tutte le misure previste dalla
legislazione vigente per l'individuazione delle responsabilità.

Art. 30 - Modalità di revisione

Le Norme possono essere modificate dal GSI secondo quanto espresso nel Regolamento

-Art. 4.

I Responsabili di struttura verranno in tal caso avvisati con ragionevole preavviso,
affinché possano predisporre le eventuali variazioni necessarie per l'accesso ai servizi.

Trascorsi 30 giorni dalla data di comunicazione delle variazioni apportate alle Norme,
durante i quali coesisteranno vecchie e nuove norme, il GSI considererà valida solo
l'ultima versione.

APPENDICE

Modulistica

- Modulo di Censimento dei servizi di rete
- Richiesta di attivazione di servizi di rete
- Modulo di Assunzione di Responsabilità
- Richiesta di accesso a servizi e laboratori - facsimile
- Rilascio della password personale di accesso - facsimile