Norme di attuazione del regolamento dei servizi di Rete di Ateneo: Gestione della Rete Dati e Fonia

Norme gestionali

PREFAZIONE

L'Università degli Studi di Modena e Reggio Emilia, riconoscendo il ruolo centrale e strategico che le nuove tecnologie informatiche e telematiche hanno nel miglioramento dei servizi offerti dalla Pubblica Amministrazione, ed essendo conscia dei problemi gestionali e dei potenziali fattori di rischio connessi con l'uso di tali tecnologie, ritiene opportuno definire delle regole per la gestione dei servizi di rete di Ateneo.

Tali norme hanno come obiettivo aumentare l'affidabilità delle componenti hardware e software del sistema e l'accessibilità, l'integrità e la riservatezza delle informazioni trattate. Inoltre la qualità dei servizi offerti all'utenza universitaria deve tenere in debita considerazione la sicurezza della rete; da questo punto di vista i comportamenti "non armonizzati" costituiscono una fonte di rischio e di possibili anomalie gestionali che si ripercuotono negativamente sul normale e quotidiano svolgimento sia dell'attività accademica che di quella amministrativa.

In questo documento vengono individuate ed illustrate a tutto il personale docente e tecnico-amministrativo dell'Ateneo ed ai fornitori/fruitori di servizi di rete, le direttive tecniche di sicurezza relative alla circolazione telematica delle informazioni ed all'accesso ai servizi di rete che l'Ateneo ha ritenuto opportuno adottare per il perseguimento delle proprie finalità istituzionali.

Vengono considerati non solo gli aspetti tecnici (sicurezza fisica e logica delle apparecchiature) ma anche gli aspetti organizzativi (definizione di ruoli e responsabilità, procedure, formazione) e legali (leggi e raccomandazioni, normative) secondo le attuali disposizioni legislative e gli obblighi delle singole Amministrazioni all'adozione di efficaci misure atte a prevenire e/o minimizzare i rischi di incidente informatico o di atti di pirateria informatica, responsabilizzando utenti e gestori dei servizi informatici.

La definizione delle norme in oggetto rappresenta uno strumento per migliorare la qualità complessiva dei servizi offerti dal nostro Ateneo.

Le norme contenute in questo documento, infine, sono principalmente uno strumento offerto ai **Referenti Informatici per Struttura** in modo da aiutarli a collaborare efficacemente con la DSIT, per la gestione della rete di Ateneo e dei suoi servizi.

I **Referenti per Struttura** sono individuati secondo il regolamento generale; il loro elenco viene mantenuto sul sito Web della DSIT al quale essi devono fare riferimento per conoscere le novità/cambiamenti di ogni servizio elencato in queste norme.

Avendo implementato la tecnologia VOIP (Voice Over IP) all'interno dell'Ateneo, la struttura e l'organizzazione della rete di trasmissione dati e quella delle centrali telefoniche sono intrinsecamente collegate e necessariamente interagenti. Di conseguenza vengono descritte le caratteristiche principali e la gestione dei due sistemi , ovvero la Rete Dati e la Rete Fonia di Ateneo: è ad entrambe che si applica il presente allegato.
Gli schemi dettagliati delle due reti si trovano all'indirizzo http:// _____ al quale va fatto riferimento per le informazioni tecniche aggiornate.

Gestione della Rete Dati

1. Descrizione del Sistema

La rete di Ateneo è oggi una complessa infrastruttura che collega 25 sedi tra Modena e Reggio Emilia servendo un bacino d'utenza dell'ordine di grandezza di 4000 macchine.
Nata nel 1983, con le prime sperimentazioni di collegamento in rete tra sistemi Digital, a partire dal 1990, adottando le tecnologie TCP/IP, si è poi presto evoluta alla rete attuale. Ultimamente si è sviluppata seguendo l'evoluzione tecnologica fino ad arrivare, nella seconda metà dell'anno 2002, a trasformarsi in rete metropolitana a larga banda, un sistema che condivide su un unico supporto trasmissivo in fibra ottica, la diffusione di servizi integrati di dati, voce e video.

La progettazione, lo sviluppo e la gestione della rete di Ateneo e della sua infrastruttura, compresi i server che erogano servizi centralizzati di rete (DNS, DHCP Server, Mail Server, Firewall, etc) gli apparati attivi, i cablaggi negli edifici, i collegamenti metropolitani ed i relativi contratti di manutenzione ed assistenza tecnica sono compiti della Direzione Sistemi Informativi e Tecnologie (DSIT).

Ogni nuova esigenza di collegamento deve essere concordata con la DSIT per individuare il miglior sviluppo armonico possibile.
E' vietata a qualunque entità facente parte dell'Università di Modena e Reggio Emilia l'attivazione di linee trasmissione dati e/o fonia e/o video da collegare alla rete d'ateneo esistente senza il preventivo accordo con la DSIT.
In particolare ***ristrutturazioni ed acquisizioni di nuove sedi, particolarmente in accordo con l'Ufficio Tecnico,*** devono tenere in debito conto i costi di cablaggio orizzontale fonia e dati all'interno delle strutture nonché degli armadi dati e di tutti gli apparati passivi. E' indispensabile il coinvolgimento di personale DSIT al momento della progettazione per garantire l'armonico inserimento nella struttura di Ateneo.

2. Topologia della Rete

La rete di Ateneo è collegata alla rete nazionale di ricerca GARR, e attraverso di essa ad internet, tramite il polo GARR di Bologna. Attualmente la linea che collega Modena a Bologna consiste in un circuito virtuale a 30 Mbps su fibra ottica. Le decisioni riguardo gli ampliamenti e

l'ottimizzazione su tale linea vengono prese dal GARR nel contesto della razionalizzazione dei collegamenti tra tutti i poli di cui esso è costituito.

Le principali sedi localizzate nella città di Modena e nella città di Reggio Emilia, compresa la tratta interurbana Modena-Reggio, sono collegate con fibra ottica spenta in tecnologia Gigabit su apparati di proprietà dell'Ateneo.
L'ambito metropolitano comprende i collegamenti urbani di Modena, di Reggio Emilia e il raccordo interurbano. Le sedi che vengono raccordate in ambito metropolitano presentano le seguenti caratteristiche di complessità, estensione e dimensione dell'utenza:

- Le sedi più complesse sono di tipo "**campus**". Esse sono costituite da più edifici dislocati su un'area comune. La tecnologia che si è scelto di utilizzare per raccordare gli edifici è la ***fibra ottica monomodale 9/125***, (salvo particolari casi come il polo scientifico di Via Campi che, per ragioni storiche, utilizza fibra ottica multimodale 62,5/125). Esempi di campus sono: il polo scientifico di Via Campi, il polo di ingegneria di Modena, il polo di ingegneria di Reggio Emilia, il Policlinico di Modena (per quest'ultimo tuttavia il discorso è particolare in quanto il cablaggio è di proprietà e gestione dell'azienda Policlinico).
  La topologia delle fibre dei campus è di tipo stellare. Questa topologia deve essere per quanto possibile mantenuta per semplificare le attività di ricerca guasti.

- Le sedi di media complessità sono di tipo "**edificio**". Esse sono costituite da un edificio di grosse dimensioni completamente cablato e fornito di 2 o più armadi di trasmissione dati. In questi edifici gli armadi sono collegati con ***fibra ottica multimodale 50/125*** (nelle sedi più datate con fibra ottica multimodale 62,5/125) per la parte dati e con cavi multicoppie di dimensioni adeguate per la gestione della fonia. La distribuzione orizzontale viene realizzata con il cablaggio strutturato in rame e connettorizzazione in armadio con strisce RJ45, salvo in casi particolari dove è ammissibile l'utilizzo di connettori block 110 per la sola parte fonia. Le reti di edificio devono tendere ad essere certificate alla massima categoria disponibile dalla tecnologia al momento della realizzazione.

- Le sedi meno complesse sono di tipo "**ufficio**". In tali sedi è possibile fare afferire tutto il cablaggio orizzontale ad un unico armadio. Per tali sedi si applicano le medesime regole inerenti la distribuzione orizzontale che deve essere realizzata con il cablaggio strutturato in rame e connettorizzazione in armadio con strisce RJ45. Anch'esse devono tendere ad essere certificate alla massima categoria disponibile dalla tecnologia al momento della realizzazione.

La rete di Ateneo integra in parte la fonia, con tecnologia IP-Trunking, tra alcune sedi. All'interno dei singoli edifici sono però sempre presenti centralini telefonici e pertanto la distribuzione orizzontale negli uffici verso gli apparecchi telefonici è in rame.

3. Gli armadi dati

Gli armadi dati devono essere di dimensione adeguate alla struttura che li ospita, tenuto conto anche del potenziale sviluppo che la struttura avrà a medio termine.
Devono avere la chiusura a chiave ed essere installati a pavimento o, se a parete, ad un altezza tale da poter lavorare senza uso di scale.
I raccordi verso altri armadi, quando in fibra ottica, devono essere di tipo SC multimodale 50/125 o monomodale 9/125 a seconda delle necessità.
Le terminazioni del cablaggio orizzontale devono essere di tipo RJ45, della categoria più elevata permessa dalla tecnologia a disposizione, sia per le connessioni di tipo dati che ti tipo telefonico. In determinati casi sarà possibile realizzare i soli collegamenti telefonici tramite block 110.
Per le nuove realizzazioni l'intero sistema di rete fisico di edificio deve essere certificato.
Il Referente di struttura ha il compito di mantenere gli armadi chiusi in modo che non intervengano modifiche alla configurazione dell'armadio, senza che egli ne sia a conoscenza. Deve inoltre tenere la mappatura aggiornata dei collegamenti tra le porte switch/hub e le prese di rete.

4. Gli apparati

La DSIT acquista in modo centralizzato gli apparati necessari al funzionamento della rete di Ateneo. Ha a sua disposizione il totale degli apparati attivi facenti parte della rete di Ateneo e ne può decidere la disposizione, lo spostamento e la riallocazione al fine di ottimizzare i costi nei suoi piani di sviluppo e svecchiamento.
Tale considerazioni si applica a tutti gli apparati di rete già presenti in Ateneo, anche se acquistati direttamente dalle strutture prima della nascita della DSIT, direttamente dalle strutture.

5. Espansione della Rete

E' fatto divieto di installare nuovi apparati di rete (router, switch, hub, firewall, access point, modem, etc) senza il consenso della DSIT.
La DSIT, informata delle necessità dell'utenza, provvederà nel modo migliore possibile e nei tempi più brevi a rendere fruibili all'utenza i servizi richiesti.
In particolare la DSIT, per motivi di sicurezza e monitoraggio della rete, deve essere a conoscenza di eventuali necessità di installazioni inerenti a:

- Hub/switch di stanza
- Apparati wireless
- Accessi via modem da e verso l'esterno
- Accessi a enti esterni all'Ateneo

6. Gestione guasti e contratti

I principali apparati di rete, cosi come le varie dorsali alle quali sono collegati, sono sotto contratto di manutenzione ed assistenza tecnica.
Nel sito Web della DSIT, in un area riservata con accesso via password, è presente l'elenco degli apparati con i numeri telefonici da attivare in caso di guasto. Il referente potrà sia avvertire la DSIT del malfunzionamento, che si attiverà per risolvere il problema, che chiamare direttamente la manutenzione, sempre avvertendo nel contempo anche la DSIT del fatto e del guasto riscontrato.

7. Sicurezza della Rete

La sicurezza totale della rete è un limite ottimale da raggiungere a cui ci si può avvicinare con misure idonee a minimizzare i rischi. I rischi incombono sulle risorse; è pertanto importante individuare e classificare con un criterio di "importanza" le risorse che si vogliono proteggere. Il sistema di sicurezza sarà sempre in evoluzione per adeguarsi ad affrontare o mutamenti che avvengono sia nelle risorse possedute che nelle minacce che incombono. I tecnici della DSIT e i responsabili informatici di struttura devono essere consapevoli che l'introduzione di misure di sicurezza comporta più lavoro a scapito dell'usabilità e della semplicità delle procedure.
Inoltre poiché la sicurezza è fatta di tanti anelli come in una catena, è svantaggioso concentrarsi per rendere robustissimo un singolo anello, perché un altro anello si potrebbe rompere. Occorre quindi distribuire le energie disponibili su tutti gli anelli della catena.

Politica di sicurezza

E' fondamentale che l'ateneo si doti di una politica di sicurezza ICT, espressa in un documento scritto e conoscibile. Tale documento è un requisito irrinunciabile per la predisposizione e la messa in sicurezza dell'organizzazione. Tale documento sarà costantemente aggiornato secondo il divenire del processo della sicurezza ITC e può partire dagli elementi già operativi descritti sotto. Esso poi dovrà essere costantemente aggiornato sia con le prescrizioni di alto livello, sia con le specifiche più tecniche. Esso sarà il punto di riferimento con il quale confrontare la realtà esistente. Dovrà inoltre contenere la metodologia

di analisi del rischio, i piani di business continuity, la gestione del personale addetto all'utilizzo dei sistemi ICT, l'accesso di terze parti ai sistemi ICT dell'ateneo, le regole di sicurezza in caso di outsourcing di determinati sistemi.
Di seguito vengono presentati gli elementi della politica di sicurezza di sicurezza che già oggi sono in uso, a cui occorre attenersi e che confluiranno nel documento più completo concernente l'intera politica di sicurezza da adottare.

7.1. Protezione perimetrale

La DSIT attiva una protezione perimetrale della rete di Ateneo inibendo alcuni servizi ritenuti pericolosi o veicolo di infezioni. Sul sito della DSIT vengono mantenute le liste dei servizi bloccati. Eventuali servizi necessari per il colloquio con l'esterno che dovessero essere riattivati vanno richiesti alla DSIT, tramite il referente di struttura.

7.2. Protezione locale

Ovunque vi siano laboratori informatici, postazioni di accesso alla rete di uso comune o di uso libero per gli studenti, occorre che vi siano implementati sistemi di identificazione, validazione, autorizzazione e protezione perimetrale.
Tali soluzioni vanno studiate congiuntamente dai referenti locali e dalla DSIT.
A tale scopo la DSIT ha già attivato una politica di inserimento di firewall e sistemi di identificazione/validazione gestiti in collaborazione con i referenti locali.
E' pertanto vietato allestire laboratori informatici o postazioni a libero accesso senza prima aver contattato la DSIT per gli opportuni adempimenti.

7.3. Protezione delle macchine

I Personal Computer afferenti alla rete di Ateneo, devono almeno essere protetti con:
- password di amministratore complessa
- password di utente (un'utenza per ogni utilizzatore)
- aggiornamenti di sicurezza
- antivirus
- personal firewall

Ogni attrezzatura in rete che può adottare le stesse protezioni indicate per il PC le deve adottare. Ogni altra attrezzatura in rete deve

adottare il massimo delle protezioni consentite dall'apparecchiatura stessa tra quelle elencate per il PC.

7.4. Software Antivirus

L'Ateneo fornisce il software antivirus per tutti i suoi dipendenti. E fatto obbligo di installare il software antivirus in ogni postazione dove questo sia possibile e di mantenerlo aggiornato. I referenti di struttura devono, per quanto possibile, promuovere ed incoraggiare l'adozione dei sistemi antivirus da parte dei loro utenti. Nel sito della DSIT sarà possibile trovare informazioni on-line sulle procedure da adottare per l'installazione e la configurazione.
In caso di segnalazione da parte della DSIT o per richiesta dell'utente stesso, il referente di struttura deve provvedere alla rimozione dei virus dalla postazione compromessa, mettere in sicurezza la postazione e redigere il modulo di intervento predisposto dalla DSIT.

7.5. Identificazione e censimento

E' compito della DSIT identificare chi genera traffico dannoso in quanto minaccioso per la sicurezza della rete o dei servizi erogati o che consuma inutilmente risorse a scapito degli altri. L'identificazione inizia dall'assegnazione dell'indirizzo IP agli apparati. E' obbligatorio richiedere l'indirizzo IP per qualsiasi apparecchiatura da collegare alla rete, anche se non è indispensabile per il funzionamento, in quanto l'indirizzo è ritenuto indispensabile per l'identificazione. L'indirizzo IP fornito sarà sempre un indirizzo pubblico della classe 155.185.xxx.xxx assegnato secondo le politiche predisposte dalla DSIT. E' vietato introdurre apparecchiature o servizi che svolgano funzioni di NAT (Network Address Translation) in quanto le macchine che usufruirebbero di tali servizi non potrebbero più essere agevolmente identificate.
Al momento della richiesta dell'indirizzo IP per una nuova attrezzatura devono essere fornite una serie di informazioni che vanno a popolare un data base degli asset collegati alla rete di ateneo. Elemento sostanziale è l'associazione di un responsabile dell'attrezzatura il quale ha il dovere di mantenere aggiornati i dati relativi all'attrezzatura stessa, ad esempio qualora sopravvengano variazioni di collocazione o di configurazione HW e/o SW, oppure la dismissione dell'apparecchiatura. In tal caso l'indirizzo IP assegnato deve essere restituito alla DSIT. Il responsabile si assume anche la responsabilità per eventuali fatti illeciti compiuti a mezzo dell'apparecchiatura del quale è responsabile.

7.6. Controllo degli apparati di rete

- E' compito della DSIT mantenere il salvataggio sia a breve che a lungo termine di tutte le configurazioni degli apparati attivi di rete.
- E' compito del Referente avere conoscenza degli apparati attivi presenti nella propria struttura e conoscerne le configurazioni.
- E' compito della DSIT e dei Referenti la realizzazione e il mantenimento di un inventario degli apparati attivi e passivi.
- E' compito del Referente e della DSIT predisporre la configurazione degli apparati attivi in modo tale da permettere il controllo remoto a tutti e soltanto gli amministratori autorizzati.

7.7. Censimento dei server e dei servizi di rete

- E' compito della DSIT mantenere il censimento dei servizi e dei server centralizzati (DNS, DHCP, RAS-Radius, LDAP/Directory, WWW, Mail, Antivirus, Antispam).
- E' compito della DSIT mantenere aggiornati i servizi e i server centralizzati.
- E' compito della DSIT individuare la necessità di avere o meno server e servizi decentrati e delegarne l'amministrazione eventualmente al referente.
- E' compito della DSIT e dei Referenti individuare servizi di rete non autorizzati o attivati senza coordinamento.
- E' compito del referente locale, su indicazione della DSIT, disattivare i servizi ritenuti inutili, illeciti e/o dannosi che si rivelassero presenti sulle postazioni degli utenti.
- E' compito della DSIT e dei Referenti applicare le sanzioni che conseguono dal comportamento di utenti che non rispetta il regolamento.
- E' compito del Referente avere una visione globale della propria struttura che comprenda la conoscenza personale di tutti gli utenti e le loro necessità, la conoscenza delle postazioni utilizzate, la situazione aggiornata dei software installati, il censimento delle licenze dei software acquistati a livello centralizzato.

Il referente deve essere inoltre l'interfaccia tra l'utenza e la DSIT per agevolare l'interscambio di informazioni allorché gli utenti richiedano di attivare servizi autonomi.

Servizi che gli utenti possono attivare liberamente

Gli utenti possono attivare liberamente sui propri sistemi i seguenti servizi:

- server ssh
- servizi di condivisione file nei limiti della normativa vigente in ambito di copyright e nei limiti di utilizzo armonico delle risorse di

rete. I servizio di condivisione di windows sono ammessi nella propria sottorete.

Servizi che l'utente può attivare in seguito a registrazione e ad assunzione di responsabilità

Gli utenti possono attivare, solo dopo aver chiesto l'autorizzazione, i seguenti servizi:
- server smtp
- server http
- server ftp
- servizi di accesso a data base (oracle, MS-SQL, MySQL, …) nel caso siano estesi al di fuori della propria sottorete
- servizi di console remota (windows terminal server, VNC, …)

Servizi che l'utente non può attivare autonomamente

L'attivazione dei seguenti servizi è esclusiva prerogativa della DSIT, con la quale si possono eventualmente concordare iniziative di settore:
- servizio telnet
- servizio DHCP
- servizio NAT
- ogni servizio di accesso wired o wireless alla rete di ateneo

7.8. Informazione degli utenti

La DSIT predispone informazioni per gli utenti riguardo alla sicurezza in varie maniere: corsi per utilizzatori, pagine on line, notizie tempestive, cosi come predisporre corsi di aggiornamento continuo sulla sicurezza per i referenti informatici di struttura.
E' compito del responsabile informatico di struttura promuovere la divulgazione e l'assimilazione delle informazioni sulla sicurezza presso i propri utenti, mediante principalmente il contatto diretto con essi.
L'informazione deve riguardare almeno i seguenti punti:
- la necessità di mantenere il proprio computer correttamente configurato con i parametri forniti dalla DSIT;
- il divieto di modificare tali parametri;
- la comunicazione della dismissione o variazione di utilizzo dei computer;
- i pericoli a cui si espone un computer in rete non sicuro;
- i danni che crea un computer o qualsiasi apparecchiatura che viene collegata alla rete senza l'accortezza di controllarne la corretta configurazione e il grado di aggiornamento;
- la necessità di mantenere sul proprio computer gli aggiornamenti di sicurezza;

- la necessità di avere dei programmi che difendono il proprio computer (personal firewall, antivirus, antispyware);
- la consapevolezza di non avere servizi di rete inutilmente aperti;
- la necessità di esaminare periodicamente il proprio computer per controllare che non contenga materiale o programmi non voluti.

7.9. Servizi di identificazione, validazione[1] e autorizzazione

7.9.1. Identificazione e validazione del personale

La DSIT attiverà nel prossimo futuro sistemi di identificazione e validazione centralizzati per tutta l'utenza universitaria basati sul possesso di credenziali personali di identificazione (username-password, certificati, smart-card).
Attualmente è comunque obbligatoria la validazione delle credenziali personali effettuata localmente da chi fornisce qualsiasi servizio. Le credenziali rilasciate sono personali, da mantenere riservate da parte dell'utente, non cedibili. La componente password della credenziale deve essere lunga almeno 8 caratteri, non banale e modificata almeno ogni 6 mesi.

7.9.2. Autorizzazione

La realizzazione del sistema di identificazione e validazione centralizzato è a fondamento di un valido sistema di autorizzazioni all'accesso dei più svariati servizi (posta elettronica, accesso alla rete, accesso remoto, consultazione banche dati, consultazione servizi per il personale quali le timbrature, consultazione dei documenti on-line, accesso a servizi riservati, …)

7.9.3. Firma Digitale

La DSIT mantiene una infrastruttura PKI (Public Key Certification) per rilasciare certificati per la firma Digitale all'interno del dominio unimore.it: la PKI è costituita dalla Certification Authority, dalla Registration Authority e dalla Revocation Authority di cui è stato nominato un responsabile tecnico.

La PKI è in grado di certificare le persone, i server e i servizi intranet/internet dell'ateneo dotandoli di un sistema sicuro per garantire la propria identità.

[1] In questo documento si usa il termine "validazione dell'identità" anziché il termine "autenticazione" in senso informatico, in conformità a quanto previsto dal nuovo "Codice dell'amministrazione digitale".

Si invitano pertanto tutti i responsabili di servizi on-line a certificare i loro server e servizi utilizzando la tecnologia fornita dalla DSIT. Si invitano inoltre tutti gli interessati, in particolare i referenti di struttura, a testare la trasmissione via e-mail di messaggi di posta elettronica "sicura" (di cui si possa cioè accertare il mittente e l'integrità del messaggio) richiedendo il certificato e/o il kit per l'installazione.

7.9.4. Identificazione/validazione/autorizzazione degli Studenti

E’ ormai ad un avanzato stadio di testing il sistema che permette l’identificazione/validazione/autorizzazione degli studenti nei laboratori informatici e nelle zone di libero accesso alla rete.
Il sistema (basato su un server LDAP e su repliche distribuite) si propone come standard per la validazione dell’identità degli studenti nei laboratori informatici. E’ attualmente attivo in 3 laboratori ed in fase di implementazione in ulteriori 10. E’ inoltre in fase di studio avanzato la possibilità di integrarlo come sistema di validazione dell’identità per l’accesso ai locali delle biblioteche, i sistemi di e-learning e formazione a distanza e per la posta elettronica.
I responsabili di struttura devono attivarsi, ciascuno nella propria struttura, per conoscere quali servizi locali necessitano di validazione e studiare insieme alla DSIT le strade di integrazione.

8. Posta elettronica

Il servizio di posta elettronica è attivo dal 1998 come servizio dell'ateneo a tutto il personale (rettorale n. 9486 del 29-04-1998). Il servizio è stato esteso dal 2001 anche agli studenti (progetto di ateneo "E-mail studenti: assegnazione di una mailbox a tutti gli studenti dell'ateneo" - Novembre 2000).

Il sistema attuale comprende il servizio di consegna delle e-mail su un server centralizzato, un sistema di antivirus centralizzato che blocca le e-mail virate sia in ingresso che in uscita, un sistema di antispam centralizzato che marca il Subject ed un sistema per la lettura della e-mail via web.
L'attivazione delle mailbox per i nuovi assunti avviene automaticamente sulla base delle segnalazioni dell'Ufficio Personale.

L'attivazione delle mailbox per gli studenti avviene automaticamente sulla base dei dati di ESSE3 con aggiornamenti a cadenza settimanale.
Il titolare della mailbox e' responsabile dell'eventuale uso improprio della mailbox stessa. Il titolare e' invitato a cambiare periodicamente la password di accesso alla mailbox (almeno ogni 6 mesi) e a utilizzare password non banali.

Il system administrator dei server mantiene uno storico dei log (in ottemperanza alle normative vigenti) con le transazioni delle e-mail sia in ingresso che in uscita. I server sono mantenuti sotto backup incrementale giornaliero su sistema Tivoli TSM.

La DSIT si riserva di inserire nella blacklist centralizzata gli indirizzi IP che risultano produrre un anomalo traffico di e-mail a causa di virus. La blacklist e' consultabile via web. La DSIT invia ai referenti l'elenco degli IP di loro competenza inseriti nella blacklist: essi sono pertanto tenuti a consultare la blacklist, a coordinarsi con lo staff DSIT per la pulizia del PC e per lo sblocco dell'IP.

La DSIT mantiene le liste di distribuzione del personale (per struttura, per ruolo) e degli studenti (per corso di laurea, per anno di corso).
La DSIT mantiene inoltre un sito web per le operazioni degli utenti (lettura via web, cambio password, attivazione vacation, etc, ricerca delle liste di distribuzione). Le transazioni tra mail server e client, se prevedono l'inserimento della password, sono fatte in modalità sicura tramite protocollo https.
Ogni nuova mailbox (esclusi studenti) viene inserita nelle liste di distribuzione ateneo@unimore.it ed eventi@unimore.it sulle quali la DSIT rispedisce messaggi di rilevanza per tutto l'ateneo.
Ogni nuova mailbox studente viene inserita nella lista di distribuzione studenti-l@unimore.it sulla quale la DSIT rispedisce messaggi di rilevanza per tutti gli studenti.

Il servizio HelpDesk prevede:
- e-mail: support_posta@unimore.it per le richieste di utenti e referenti (non studenti)
- e-mail: support_posta_studenti@unimore.it per le richieste di studenti

Le strutture possono richiedere il mantenimento di un proprio server di posta sia per le funzioni di delivery delle e-mail che per quelle di spedizione purchè venga inviato alla DSIT il modulo di assunzione di responsabilità da parte del responsabile della struttura (modulo reperibile sul sito), sia indicato un responsabile tecnico che concorda la configurazione del server con i tecnici della DSIT e purchè sia mantenuto un sistema di antivirus aggiornato sia in ingresso che in uscita.

Le strutture possono altresì richiedere il controllo antivirus centralizzato della posta in ingresso e in uscita dal loro sottodominio, oltre alla abilitazione della lettura della mail via web tramite il servizio centralizzato.
La DSIT si riserva di bloccare i server di posta che non rispettano i requisiti di sicurezza indicati

I referenti sono invitati a:

- Segnalare via e-mail la creazione di nuove mailbox per collaboratori di dipendenti segnalando nome, cognome, struttura, tel e fax e data di scadenza
- segnalare la cessazione dal servizio di un dipendente e chiedere l'eliminazione della mailbox e/o l'attivazione temporaneo di un forward
- segnalare la richiesta di alias e di mailbox aggiuntive indicando la data di scadenza
- configurare i client di posta elettronica degli utenti e risolvere i problemi dei client
- formare gli utenti sull'uso del client, sull'uso dell'accesso via web, sulla differenza tra protocollo imap e pop3 e sul salvataggio della mail sia in locale che sul server
- impedire la memorizzazione delle password da parte dei client
- pulire i pc infetti dai virus (e loro segnalati dalla DSIT) e segnalare l'ip da togliere dalla blacklist
- controllare periodicamente la rubrica di ateneo e segnalare eventuali spostamenti sia di struttura che di interni telefonici e/o di fax
- controllare periodicamente la lista degli iscritti alle liste di pertinenza della propria struttura http://liste.unimore.it segnalando via e-mail eventuali modifiche
- controllare l'inserimento di IP nella blacklist, provvedere al controllo del pc/ws titolare dell'IP e a chiedere via e-mail il ripristino dell'IP

9. Regole per la pubblicazione di siti WEB sulla rete di ateneo

Le norme per la pubblicazione di siti Web sulla rete di Ateneo sono regolamentati da un'apposita commissione denominata "Commissione Web di Ateneo" alla quale si rimanda per il regolamento completo. Tuttavia, per completezza, si riportano i punti chiave sui quali si strutturerà detto regolamento :

- pubblicazione di contenuti istituzionali
- osservanza delle leggi e delle normative nazionali ed internazionali
- adeguatezza dei supporti HW e SW per la salvaguardia dei dati

Per ogni sito web attivato sulla rete di ateneo e visibile al di fuori di essa si richiede la definizione delle seguenti figure:

- **Responsabile** dei contenuti pubblicati, ovvero titolare del sito
- **Webmaster**, colui che cura la pubblicazione delle informazioni nel sito
- **Sistemista**, tecnico addetto al corretto funzionamento del sistema

Per le figure individuate, non necessariamente distinte, si indicano le seguenti linee di comportamento:

Il Responsabile dei contenuti

- assume la piena responsabilità circa l'esattezza e veridicità dei contenuti immessi in nome e/o per conto proprio o di terzi;
- utilizza il sito esclusivamente per la diffusione di informazioni o servizi inerenti l'attività istituzionale dell'ateneo o attività collaterali comunque riconducibili a convenzioni, progetti, iniziative in cui l'ateneo è soggetto attivo;
- si impegna a non pubblicare contenuti che violano le vigenti leggi internazionali sul copyright; eventuale materiale protetto da copyright può essere pubblicato solo dopo l'acquisizione dei diritti di utilizzo dal titolare e con l'obbligo di citare la fonte e il permesso ottenuto;
- si impegna a non pubblicare contenuti reprensibili;

Il Webmaster:

- trasferisce sul server i contenuti indicati dal responsabile del sito;
- realizza il sito in osservanza delle disposizioni legislative in materia di siti delle Pubbliche Amministrazioni;
- conserva la password di accesso al sito nella massima riservatezza;

Il Sistemista:

- applica correttamente le politiche sulla sicurezza per la salvaguardia del sito da accessi indesiderati;
- consegna la password di accesso al responsabile del sito e al webmaster;
- crea periodicamente copie di backup dei contenuti pubblicati;
- monitorizza il corretto funzionamento del sistema;

La Direzione SIT si riserva di sospendere la visibilità all'esterno della rete qualora vengano riscontrati comportamenti non conformi al presente regolamento.

10. Riepilogo della Gestione operativa

Ai referenti viene di norma demandata :

- la buona gestione degli apparati collegati alla rete (da fare direttamente in accordo con gli utenti o tramite la gestione/supervisione dell'operato della ditta di assistenza qualora fosse stato acceso un contratto)
- la gestione del software operativo, di base e degli antivirus
- la gestione dell'allacciamento delle nuove macchine in rete
- la gestione di un lotto di indirizzi IP per la propria porzione di rete
- la gestione richieste di ampliamenti sul cablaggio e sugli apparati
- la raccolta delle esigenze degli utenti

- il monitoraggio di base della propria porzione di rete
- la gestione del primo intervento in caso di malfunzionamenti e attacchi virus
- la gestione della risoluzione dei problemi in staff con la DSIT
- la stesura di raccomandazioni per un uso appropriato della rete nel contesto specifico della propria struttura
- la protezione locale della rete in staff con la DSIT
- censimento dei server e delle macchine presenti
- la gestione delle problematiche inerenti la posta elettronica per i propri utenti

Al personale centralizzato della Direzione spettano:

- la progettazione degli ampliamenti della rete
- la gestione degli apparati di rete presenti
- la gestione dei firewall e della sicurezza
- l' evasione delle richieste di nuovi apparati/ampliamenti
- l'individuazione degli strumenti più opportuni e l'implementazione delle soluzioni per soddisfare le nuove esigenze avanzate dagli utenti
- la gestione dei contratti di manutenzione e assistenza tecnica
- la protezione perimetrale della rete
- la protezione locale della rete
- censimento dei server e dei servizi di rete
- la gestione della posta elettronica
- la gestione della visibilità Web

11. Contatti per la rete dati

Per i problemi di cui sopra rivolgersi a:

Funzionamento della rete:
Dario Montardi tel. 059 205 5004;
email montardi.dario@unimore.it

Sicurezza ed emergenza:
MariaLaura Mantovani tel. 059 205 5007;
email mantovani.marialaura@unimore.it

Posta elettronica:
Roberta Cantaroni tel. 059 205 5006;
email cantaroni.roberta@unimore.it

WEB:
Daniela Nasi tel. 059 205 5003;
email nasi.daniela@unimore.it

Gestione della Rete Fonia

1. Descrizione del Sistema

Il Sistema Fonia di Ateneo si basa su diverse Centrali telefoniche principali, ognuna collegata alla Centrale Urbana Telecom tramite linee ISDN.

Attraverso questi collegamenti passano le telefonate verso l'esterno.

Le centrali poi sono collegate tra loro e verso apparati remotizzati (centrali telefoniche secondarie) installati nelle sedi più piccole, tramite linee CDN o in fibra ottica. Attraverso questi collegamenti passano le chiamate interne che non generano quindi scatti e di conseguenza non generano costi.

Diverse piccole sedi distaccate dell'Ateneo, che non avevano dimensioni tali da rendere conveniente l'inserimento di una centrale autonoma, sono state collegate alla centrale più vicina tramite linee punto-punto denominate CDF. Attraverso questi collegamenti tali sedi utilizzano tutte le funzionalità messe a disposizione dall'impianto.

2. Costi fissi e costi variabili

Ognuna delle voci descritte sopra (ISDN, CDN, CDF) da origine ai cosiddetti costi di canoni. Il costo delle linee in fibra ottica viene ricompreso nei costi di gestione della rete dati di ateneo e quindi non grava nel monte dei canoni.

I canoni telefonici vengono pagati in modo centralizzato dall'ateneo e dopo ribaltati sulle strutture secondo un calcolo proporzionale approvato dalla conferenza dei direttori.

3. Gli apparati di Fonia

La DSIT acquista in modo centralizzato gli apparati necessari al funzionamento della rete Fonia di Ateneo (schede, apparecchi telefonici, cordless, dect, etc). Ha a sua disposizione il totale degli apparati e ne può decidere la disposizione, lo spostamento e la riallocazione al fine di ottimizzare i costi nei suoi piani di sviluppo e svecchiamento. Richieste di nuovi apparecchi telefonici e/o necessità di ampliamento della rete telefonica debbono essere fatti pervenire alla DSIT da parte del referente di struttura.

4. Espansione della Rete

E' fatto divieto di installare nuovi apparati di rete senza il consenso della Direzione.

La DSIT informata delle necessità dell'utenza provvederà nel modo migliore possibile e nei tempi più brevi a rendere fruibili all'utenza i servizi richiesti.

5. Gestione guasti, modifiche e interventi.

L'intero impianto di Fonia, è sotto contratto di manutenzione ed assistenza tecnica.

Nel sito della DSIT, in un area riservata con accesso via password, è presente l'elenco degli apparati con i numeri telefonici da attivare in caso di guasto. Il referente potrà sia avvertire la DSIT del malfunzionamento, che si attiverà per risolvere il problema, che chiamare direttamente la manutenzione, sempre avvertendo nel contempo anche la DSIT del fatto e del guasto riscontrato.

Nel caso invece nasca la necessità di intervenire per manutenzione, ampliamenti, modifiche delle abilitazioni del telefono, gestione dei centri di costo, gestione addebiti, produzione di rapporti particolari sul traffico, è necessario mandare una mail all'indirizzo : telefoni@unimo.it o chiamare il numero 5000 (dall'esterno 059/2055000) e lasciare un messaggio.

6. Servizi erogati e gestione addebiti.

E' presente un sito di servizio all'indirizzo : www.telefoni.unimo.it dove è possibile ricercare persone e numeri e si trova una piccola sezione di FAQ che spiega l'utilizzo delle funzioni messe a disposizione del sistema.

Nello stesso sito, per i referenti, accedendo mediante username e password, è possibile compilare una forma attraverso la quale richiedere gli interventi tecnici.

La gestione degli addebiti avviene mediante la suddivisione del sistema in centri di costo che rispecchiano le entità che rappresentano (Rettorato, Dipartimenti, Centri, etc). Gli apparecchi telefonici sono attribuiti ai vari centri di costo secondo la loro afferenza e possono a loro volta essere ancora suddivisi in sottocentri per individuare, ad esempio, singoli uffici, gruppi di ricerca, etc.

Tale suddivisione può essere modificata ed integrata a richiesta del referente.

La gestione degli addebiti inerenti l'utilizzo del telefono crea mensilmente un report che viene mandato al referente di struttura e per conoscenza all'ufficio bilancio, per assolvere le pratiche amministrative necessarie.

7. Gestione operativa

Ai referenti viene di norma demandata :

a. la gestione dell'elenco telefonico locale (segnalando tempestivamente i
   cambi di numeri ai quali rispondono gli utenti)
b. la segnalazione di anomalie sul funzionamento dei telefoni e delle linee

c. la segnalazione di necessità di ampliamenti e modifiche di configurazione
d. le gestione richieste di ampliamenti sul cablaggio e sul num. di apparecchi.
e. la raccolta delle esigenze degli utenti
f. la produzione di rapporti sul traffico e la loro gestione

Al personale centralizzato della Direzione spettano:

f. la progettazione degli ampliamenti della rete telefonica
g. la gestione degli apparati di rete presenti
h. l' evasione delle richieste di nuovi apparati/ampliamenti
i. l'individuazione degli strumenti più opportuni e l'implementazione delle soluzioni per soddisfare le nuove esigenze avanzate dagli utenti
j. la gestione dei contratti di manutenzione e assistenza tecnica

8. Contatti per la rete fonia

Per i problemi di cui sopra rivolgersi a:

Dario Montardi tel. 059 205 5004; email montardi.dario@unimore.it