UNIVERSITÀ DEGLI STUDI DI MILANO

REGOLAMENTO DI SICUREZZA ICT PER L'UNIVERSITÀ DEGLI STUDI DI MILANO

INDICE

STRUTTURA ORGANIZZATIVA PER L'IMPLEMENTAZIONE DEL REGOLAMENTO DI SICUREZZA D'ATENEO

1 DEFINIZIONE DELLA STRUTTURA ORGANIZZATIVA PER L'IMPLEMENTAZIONE DELL REGOLAMENTO DI SICUREZZA D'ATENEO

1.1 Commissione sicurezza permanente.

Sottocommissione della Commissione Strategie Informatiche allargata anche a esponenti del personale tecnico del gestore della rete, del gruppo sicurezza di rete, e dei referenti di sicurezza per i servizi informativi centrali, nominata con decreto rettorale.

1.2 Gruppo sicurezza di rete.

Gruppo permanente, composto di 5/6 persone, interno al gestore della rete, a carattere prevalentemente tecnico. Si occupa attivamente e giornalmente della gestione della sicurezza per l'intero Ateneo, fa da punto di riferimento centrale per tutti i referenti di struttura relativamente ai problemi riguardanti la sicurezza.

1.3 Incident Response Team (IRT).

Gruppo permanente tecnico di 2/3 persone scelto nell'ambito del personale afferente al gestore della rete con alte professionalità nel campo sicurezza e reti

1.4 Servizio legale per gli aspetti di sicurezza informatica.

Servizio composto da personale della Divisione Affari Legali e da docenti dell'università di Milano con specifiche competenze giuridiche in campo informatico, nominato con decreto rettorale.

1.5 Gestore della rete.

Il gestore della rete d'ateneo dell'Università di Milano è la Divisione Telecomunicazioni dell'Università di Milano.

1.6 Referenti di sicurezza per i servizi informativi centrali.

Le strutture dell'università che erogano servizi centrali, nel nome e per conto dell'Ateneo, identificano dei responsabili tecnici nel campo della sicurezza informatica, in numero adeguato ai servizi offerti.

1.7 Referenti di struttura.

E' il delegato del Direttore della struttura d'appartenenza alla gestione della sottorete della rete d'Ateneo afferente alla struttura stessa.

2 FUNZIONI DEGLI ORGANI E DEI LORO RAPPORTI

2.1 Funzioni della commissione sicurezza permanente.

Ha lo scopo di definire le direttive del processo di messa in sicurezza della rete d'Ateneo, di mantenerle aggiornate e di verificare e controllare lo stato dei lavori. Si occupa di mantenere aggiornato il presente regolamento, modificandolo per adeguarlo alle necessità e sottoponendo tali modifiche alla commissione strategie informatiche, curando l'iter per la modifica presso gli organi competenti.

2.2 Funzioni del gruppo sicurezza di rete.

Il gruppo di sicurezza di rete si occupa di rendere operative le direttive di sicurezza decise e approvate nella commissione sicurezza e di garantirne l'operatività. Il gruppo si incarica di scegliere le tecnologie e i mezzi appropriati per l'implementazione delle suddette direttive e di suggerire eventuali variazioni/correzioni/ampliamenti alla commissione sicurezza permanente. Si incarica di comminare le sanzioni per i trasgressori e di applicarle o farle applicare.
Compiti accessori del gruppo sono:

- tenere la rete d'Ateneo e gli host che vi appartengono sotto osservazione dal punto di vista della sicurezza allo scopo di individuare, se possibile preventivamente, i problemi che abbiano ripercussioni sulla rete o per individuare sistemi non conformi al presente regolamento. Il gruppo sicurezza di rete a questo scopo può operare degli scan delle varie sottoreti della rete di Ateneo;
- produrre statistiche annuali relative a tutti gli eventi di sicurezza occorsi, e sulla base di questi dati fornire un rapporto sullo stato dell'implementazione della sicurezza in UNIMI alla commissione sicurezza permanente. Sulla base di questi dati e sull'esperienza maturata propone suggerisce alla commissione sicurezza gli spunti e le considerazioni necessari alla perpetua revisione e aggiornamento del presente regolamento;
- interagire con i referenti di struttura e con il gestore della rete per la risoluzione di tutti i problemi di sicurezza;
- mantenere e aggiornare una lista di tutti i servizi e i loro responsabili disponibili nella rete d'Ateneo;
- valutare l'opportunità di installare sulla rete dispositivi di filtraggio del traffico (firewall, acl sui router), curare la loro istallazione, configurazione, manutenzione e gestione, di concerto con il gestore della rete;
- valutare l'opportunità di installare sulla rete o su segmenti di rete dispositivi NIDS/HIDS e di monitoraggio del traffico (netflow, RMON) per il controllo dell'effettiva applicazione delle direttive, di concerto con il gestore della rete;
- valutare l'attività dell'IRT ed eventualmente rimuovere, modificare o rendere definitivi i provvedimenti di emergenza da esso adottati;
- valutare i regolamenti di sicurezza locali di cui le strutture dell'università dovranno dotarsi, esprimendo un parere tecnico sulle soluzioni scelte e sulla

loro fattibilità all'interno della rete d'ateneo. Tale parere avrà potere di veto sulla realizzazione, se le soluzioni scelte dalla struttura in esame dovessero influire in modo negativo sulla rete o su altre strutture/servizi/sistemi dell'università;

- per eventuali reti sprovviste di amministratore locale operare, con i mezzi più opportuni da valutare caso per caso, un filtro sul traffico in ingresso, in modo da consentire soltanto connessioni established che hanno avuto origine all'interno della rete. Questo per impedire la raggiungibilità dall'esterno di eventuali servizi/server non amministrati presenti nella sottorete.
- Acquisire e controllare i regolamenti di sicurezza specifici relativi ai servizi erogati in nome e per conto dell'università;
- occuparsi della formazione nel campo della sicurezza del personale addetto (referenti di struttura, IRT);
- occuparsi della sensibilizzazione dell'utenza dell'Università relativamente alla sicurezza informatica, in modo finalizzato a promuovere la corresponsabilizzazione e la consapevolezza riguardo alle nuove logiche, modelli e comportamenti organizzativi della sicurezza;
- gestire un sito web d'ateneo ove pubblicare avvisi relativi alla sicurezza, informative sull'attività del gruppo, incidenti in corso, materiale di supporto ai referenti di struttura e in genere materiale di cultura informatica relativo alla sicurezza;
- gestire gli aspetti di sicurezza relativi alle aule informatiche e l'insieme di firewall ad esse dedicati;
- curare gli aspetti di sicurezza nella progettazione e implementazione delle reti wireless;
- controllare e approvare il livello di sicurezza fornito dai servizi ICT presi in outsourcing dalle strutture centrali dell'Università;
- consultare il servizio legale per la sicurezza informatica prima di progettare/implementare nuovi progetti o attività, in modo da verificarne la compatibilità con la legislazione vigente;

2.3 Funzioni dell'Incident Response Team (IRT).

L'IRT si occupa di rispondere in tempi brevi ad eventi imprevisti riguardanti la sicurezza nella rete d'ateneo: agisce di concerto con il gestore della rete e con i Referenti di struttura. Si occupa di problematiche relative a DDOS, intrusioni, virus e worm, e in generale di tutti quei problemi di sicurezza che possono assumere proporzioni tali da riguardare l'intera rete d'Ateneo o di una sua intera sottorete. Per periodi di tempo limitati o comunque da stabilirsi in relazione agli accadimenti può prendere tutte le misure necessarie atte a ripristinare il corretto funzionamento della rete o dei servizi d'Ateneo, compreso la possibilità di applicare sanzioni provvisorie senza consultare il gruppo sicurezza di rete.
Attività accessorie dell'IRT, sono:

- possibilità di effettuare su singole LAN, sevizi o sistemi dei test per valutare il grado di sicurezza raggiunta, su richiesta della struttura o del gruppo sicurezza di rete.

- attività di consulenza nei confronti delle strutture per incidenti di sicurezza di piccole dimensioni in cui il gruppo per definizione non è strettamente coinvolto.

2.4 Funzioni del servizio legale per gli aspetti di sicurezza informatica.

Il servizio legale per gli aspetti di sicurezza è l'ufficio che si occupa di tutti gli aspetti giuridici relativi agli incidenti informatici, ivi comprese le azioni di risposta intraprese dall'IRT, dal gruppo sicurezza di rete o dal gestore della rete. Specifico compito è quello di supportare le varie entità che si occupano di sicurezza informatica da un punto di vista giuridico. In generale deve rappresentare il punto di riferimento per gli aspetti giuridici della sicurezza informatica per l'intero ateneo. I membri del servizio devono essere in grado di firmare digitalmente e di garantire l'integrità dei propri documenti elettronici oltre che della corrispondenza con le altre entità definite in questo documento.

2.5 Funzioni del gestore della rete.

Il gestore della rete si occupa della gestione e del mantenimento della rete d'Ateneo così come intesa al punto 3.1 del presente regolamento. Si occupa inoltre della progettazione realizzazione e messa in opera di tutte le nuove sottroreti e dei loro collegamenti di cui l'università intende dotarsi, oltre che del continuo aggiornamento della rete esistente. Il gestore dalla rete è il punto di contatto tra le strutture del GARR e la rete d'ateneo; è il referente presso questa struttura anche relativamente alla sicurezza di rete. Gestisce il collegamento geografico con il GARR e con tutte le altre reti con le quali l'università di Milano possiede una connessione diretta.
Il gestore della rete scambia con i referenti di Struttura gli avvisi relativi alle interruzioni di rete, alle problematiche di sicurezza, all'attivazione/sospensione di servizi o dispositivi. Agisce, di concerto con il Referente di struttura e con il gruppo sicurezza di rete, per ogni problematica relativa al trasporto, gestione, filtraggio, controllo e logging dei dati verso la WAN. Avverte e collabora con il gruppo sicurezza di rete/IRT per ogni incidente di sicurezza. Su richiesta del gruppo sicurezza di rete/IRT, mette in atto tutti quegli accorgimenti tecnici ad esso disponibili per disattivare ogni trasporto dati sulla rete relativo ai sistemi giudicati non conformi alle regole, sino all'intervento correttivo operato dalla struttura. Allo scopo di individuare preventivamente possibili problemi che abbiano ripercussioni sulla rete o per individuare sistemi non conformi il gestore può operare degli scan delle varie sottoreti della rete di Ateneo. Sotto la sua responsabilità ricade la sicurezza dei routers e di tutti gli apparati attivi di rete dell'università, delle connessioni per l'amministrazione remota di tali apparati e dei protocolli di routing utilizzati. In particolare il gestore della rete si incarica di implementare per ogni sottorete dell'università le opportune regole anti-spoofing, allo scopo di non consentire il mascheramento dell'indirizzo IP sorgente.

2.6 Funzioni dei referenti di sicurezza per i servizi informativi centrali.

I referenti di sicurezza per i sistemi informativo d'ateneo sono identificati tra il personale tecnico afferente alle strutture che erogano servizi centrali per conto dell'Ateneo, e si occupano di sovrintendere all'interno della struttura stessa il lavoro dei vari amministratori di sistema e responsabili della sicurezza dei singoli sistemi e servizi per quanto concerne la sicurezza informatica. Sono l'interfaccia tra le strutture centrali che offrono il servizio e il gruppo sicurezza di rete/IRT, ovvero si pongono come punto di contatto, per i problemi di sicurezza, tra le strutture centrali definite in precedenza e gli amministratori di sistema o i gestori dei servizi. Si occupano inoltre della stesura dei regolamenti di sicurezza particolari per la propria struttura e, una volta approvati dagli organismi competenti, s'incaricano di implementarli, controllarli e farli rispettare.

2.7 Funzioni del referente di struttura.

Il referente di struttura occupa della gestione tecnica delle postazioni individuali, dei server ed eventualmente in accordo con il gestore della rete, degli apparati attivi della rete locale della struttura.
In particolare il referente di struttura ha il dovere di:

- conoscere la topologia del cablaggio della rete LAN di competenza
- conoscere la posizione e il tipo degli apparati attivi di rete dislocati sulla LAN di competenza;
- conoscere i responsabili/gestori dei vari host connessi in rete;
- conoscere la quantità e la tipologia (nel dettaglio) dei servizi forniti in rete mediante i server attivi all'interno della struttura e comunicarli al gruppo sicurezza di rete insieme ai relativi responsabili;
- mantenere queste informazioni in una lista, che rappresenta un sottoinsieme relativo alla struttura locale della lista generale dei servizi, mantenuta dal gruppo sicurezza di rete, e comunicare a questo gruppo ogni variazione/aggiornamento;
- garantire che solo i servizi registrati e amministrati siano accessibili in rete dall'esterno della struttura, ovvero che non esistano servizi/server non controllati;
- essere un punto di riferimento a livello di struttura per la diffusione delle informazioni di carattere informatico e di sicurezza d'interesse per l'utenza;
- segnalare al gruppo sicurezza di rete eventuali incidenti/problemi di sicurezza, intrusioni o tentativi di intrusione che abbiano avuto come oggetto host appartenenti alla propria struttura;
- segnalare al gruppo sicurezza di rete applicazioni ad alto consumo di banda e qualunque altra attività in rete della struttura di appartenenza che comporti un carico sulla rete o un suo utilizzo improprio o non standard. In particolare ogni applicazione che abbia un impatto significativo sulla disponibilità della banda di un tratto di rete di Ateneo, metropolitana o geografica, compreso il collegamento con il GARR, deve essere preventivamente segnalata al gestore della rete e al gruppo sicurezza di rete, che devono dare un parere

sulla fattibilità. In particolare va verificata la fattibilità della messa in funzione di servizi quali la posta elettronica, DNS, salvataggi ed archiviazioni di grandi quantità di dati, utilizzo di basi dati di elevate dimensioni, server web pubblici con alti numeri di contatti previsti, server ftp con file massicci, servizi di streaming audio/video/multimedia. Nel caso che l'impatto di un'applicazione non consentisse di mantenere l'equilibrio nella condivisione delle risorse o fosse al di là delle possibilità della rete, si deve concordare con il gestore della rete una soluzione alternativa in tempi e modi compatibili con i servizi esistenti e le risorse economiche disponibili. È espressamente vietato attivare un'applicazione con rilevante impatto sulla rete prima dell'ottenimento del parere favorevole da parte del gestore della rete. La Struttura che dimostrasse la buona fede nel considerare una sua applicazione con rilevante impatto non come tale, è obbligata a disattivare immediatamente la stessa nel momento in cui le venga notificata la rilevanza dell'impatto, e fino al momento dell'eventuale ottenimento del parere favorevole a seguito dell'individuazione di una soluzione alternativa. In seguito a una segnalazione del gruppo sicurezza di rete sulla inadeguatezza di un sistema per quanto concerne la sicurezza, il Referente di struttura si occupa di portare a norma il sistema in oggetto o di staccarlo dalla rete;

- amministrare eventuali sistemi di filtraggio dei dati (per es. firewall, proxy) o di rinumerazione IP verso indirizzi privati e conseguente uso di NAT/PAT, relativi alla LAN della struttura; tali sistemi vanno in ogni caso concordati preventivamente col gruppo sicurezza di rete e con il gestore della rete.

REGOLAMENTO DI SICUREZZA ICT D'ATENEO

3 DEFINIZIONE DEL REGOLAMENTO DI SICUREZZA PER LA RETE DI ATENEO

3.1 La rete di ateneo.

La rete d'ateneo è costituita:

- dalla rete di collegamento telematico tra tutte le varie sedi di UNIMI (WAN o rete di Backbone);
- dalle sottoreti (LAN) afferenti ai vari dipartimenti, istituti, centri, facoltà di cui è composta UNIMI;
- dai servizi di gestione della rete;
- dai servizi applicativi di base forniti sulla rete, quali Posta, News, Proxy, Web;
- dal servizio di accesso remoto via linee commutate o via tunnel VPN;
- da tutti quegli strumenti di interoperabilità e apparati attivi di rete che permettono ai soggetti autorizzati di accedere alla rete e di comunicare tra loro.

3.2 Protocolli consentiti.

Nella rete d'Ateneo viene garantito il supporto per la suite di protocolli TCP/IP, le strutture possono utilizzare al loro interno anche altri protocolli, dandone comunicazione preventiva al gestore della rete, a patto che essi rimangano totalmente confinati all'intero delle strutture medesime. La propagazione di altri protocolli di rete (per esempio Decnet, Appletalk, NetBeui, ecc.) non può essere consentita esternamente alle strutture. In casi particolari (per esempio se la Struttura è distribuita su più edifici), di concerto tra il gestore della rete e la Struttura, verrà studiata la fattibilità tecnica dell'utilizzo di un altro protocollo che graviti su parte della rete di Ateneo. In caso positivo verrà adottata una soluzione che comunque non influisca sull'affidabilità e sulle prestazioni della rete. Inoltre, non è consentito utilizzare protocolli di comunicazione o per la condivisione di risorse, studiati per agire in ambito di rete locale (per es. NFS) sulla rete WAN d'Ateneo o su collegamenti geografici (GARR);

3.3 Elenco dei soggetti che possono accedere alla rete.

La rete viene fornita alle strutture dell'ateneo e agli Enti e Organizzazioni universitarie esplicitamente autorizzate dal CdA dell'ateneo.
L'acceso alla rete è consentito solo a Docenti e ricercatori dell'ateneo, personale tecnico-amministrativo dell'ateneo, borsisti, dottorandi, assegnisti, studenti, cultori della materia afferenti all'ateneo e ad altri soggetti esplicitamente autorizzati dal responsabile della struttura di riferimento.
Per quanto riguarda gli studenti, l'accesso avviene dai laboratori informatici, dalle aule informatiche e dalle biblioteche.

3.4 Accesso alla rete dalle postazioni per il pubblico presenti nelle biblioteche.

Le biblioteche possono fornire i servizi bibliotecari disponibili in rete d'Ateneo a tutti i propri utenti, attraverso postazioni presenti al loro interno e collegate alla rete d'Ateneo. Tali postazioni sono soggette ai criteri di sicurezza previsti per gli host in rete [vedi p.ti 3.11, 3.12] e in aggiunta devono soddisfare le seguenti regole:

- Gli utenti non devono mai accedere al sistema con i privilegi di amministratore, non deve essere possibile l'installazione di applicativi di qualsiasi genere;
- Gli applicativi utilizzabili dall'utente devono essere soltanto quelli consentiti;
- L'utente deve essere preventivamente informato, qualora si utilizzi un sistema di monitoraggio/filtraggio dei dati in transito applicato al fine di verificare il corretto utilizzo della postazione.

Si distinguono inoltre due tipi di postazioni al pubblico:

- quelle che consentono l'accesso ai soli servizi erogati dalle biblioteche;
- quelle in cui è consentito anche il libero accesso alla sola rete web attraverso un browswer http esente da filtri/limitazioni;

Nel primo caso le postazioni devono essere limitate nelle funzioni: ovvero deve essere possibile esclusivamente la navigazione in Internet verso i siti relativi ai periodici elettronici sottoscritti dall'Ateneo, la consultazione bibliografica presso le banche dati d'ateneo o convenzionate, oppure il solo lancio di client specifici necessari alla consultazione di una particolare banca dati convenzionata. Per queste postazioni non è necessaria alcuna autenticazione dell'utente che ne faccia uso.

Nel secondo caso l'utilizzatore deve invece necessariamente essere identificato.
Tale identificazione può avvenire mediante un sistema di autenticazione automatico sicuro, in grado di identificare ed autorizzare sulla base di credenziali fornite dall'utente. Le credenziali minime sono la coppia username e password, personali e non cedibili.
Tale sistema di autenticazione e autorizzazione può anche essere locale, cioè appoggiarsi a una base dati locale di competenza e responsabilità della singola biblioteca o di più biblioteche.
All'atto dell'utilizzo del servizio, all'utente deve venire sottoposto in visione un banner o un documento cartaceo contenente le regole fondamentali di comportamento a cui attenersi ed avvertenze circa eventuali responsabilità nelle quali sia possibile incorrere con un uso non corretto del mezzo informatico. A seguito dell'accettazione di questo documento di utilizzo l'utente è libero di usufruire del servizio e della postazione, altrimenti gli deve essere negato l'accesso. I log relativi alle autenticazioni e agli accessi alle postazioni (login/logout) vanno mantenuti per il periodo di un anno.
Nel caso non si potesse disporre di un sistema di autenticazione e autorizzazione automatico, bisogna individuare un referente all'interno della struttura che identifichi, a mezzo di registri, il soggetto che utilizza la postazione (segnando il momento di accesso alla macchina – login - e il momento di uscita - logout). Tale soggetto sottopone all'utilizzatore della postazione, dopo la compilazione di un registro, il documento, di cui si è parlato per il caso automatico da leggere e sottoscrivere. Tali attività esauriscono i compiti di presidio dei soggetti preposti alla cura delle postazioni pubbliche e del loro utilizzo. Ogni necessario intervento del personale preposto al presidio, nel caso ci sia il

sospetto di un utilizzo non idoneo del mezzo telematico, è ammesso nel rispetto della privacy dell'utilizzatore della postazione.

I periodici elettronici sottoscritti dall'Ateneo che sono accessibili liberamente dalla rete via protocollo http, possono essere consultati anche da postazioni situate al di fuori della rete d'Ateneo esclusivamente facendo uso dell'accesso alla rete via VPN [vedi p.to 3.6] o attraverso il proxy server, munito di autenticazione via user-id/password, messo a disposizione per questo scopo dalla divisione biblioteche: è vietato l'utilizzo di altri proxy server oltre a quello gestito centralmente.

3.5 Accesso alla rete via linee commutate.

Il servizio di accesso remoto messo a disposizione dal gestore della rete di Ateneo è disponibile per alcune tipologie di utenti della rete: docenti, ricercatori, borsisti, dottorandi, dipendenti dell'ateneo. Username e password sono strettamente personali e non cedibili a terzi. L'utilizzo di modem installati direttamente sui PC utente facenti parte della rete di ateneo contattabili dall'esterno della rete è vietato, a meno di casi particolari relativi a specifiche esigenze, che devono essere concordati con il gestore della rete. Qualora una struttura intenda intraprendere soluzioni autonome per la fornitura di accesso remoto, deve darne preventiva comunicazione al gestore della rete e al gruppo sicurezza di rete, garantendo l'adozione di tutte le misure di sicurezza atte a prevenire intrusioni e/o utilizzi illeciti attraverso linea commutata. L'attività può essere intrapresa solo a seguito del riconoscimento da parte del gestore della rete e del gruppo sicurezza di rete dell'idoneità delle misure di sicurezza adottate

3.6 Accesso/estensioni della rete, via VPN o sistemi di tunnelling.

Estensioni della rete di Ateneo, temporanee o permanenti, via VPN o altri meccanismi di tunnelling analoghi sono vietate, a meno di casi particolari da concordarsi con il gestore della rete e sotto la supervisione del gruppo sicurezza di rete. Sono consentiti singoli tunnel VPN verso utenti autorizzati per permetterne l'accesso da reti esterne a quella d'ateneo, allo scopo di connettere utenti remoti in alternativa all'accesso in commutata di cui al 3.5. Il servizio è disponibile per alcune tipologie di utenti dell'ateneo: docenti, ricercatori, dipendenti, che riscontrino l'esigenza di operare come se fossero connessi direttamente alla rete di ateneo dalla loro sede remota (ad es. per l'utilizzo di particolari programmi applicativi, per l'accesso a dati sensibili o nel caso dei telelavoratori). Il concentratore di VPN per l'accesso dell'utenza in questa modalità viene gestito centralmente dal gestore della rete; gli utenti connessi vengono mappati su una sottorete di unimi dedicata. Qualora una struttura necessiti, per particolari esigenze, di fornire ai propri utenti accessi VPN terminati all'interno delle proprie LAN, dovrà richiederne autorizzazione preventiva al gestore della rete e al gruppo sicurezza di rete. La richiesta dovrà contenere la motivazione della scelta di questo tipo di accesso e il numero di utenti previsto, per permetterne una corretta valutazione. La struttura si fa carico del server per la concentrazione delle VPN in tutti i suoi aspetti, conformadosi alle norme di sicurezza descritte in questo documento (p.to 3.14). In particolare gli utenti devono venire autenticati.

3.7 Le reti wireless.

L'implementazione di una rete via radio (wireless) comporta a tutti gli effetti un'estensione della rete d'Ateneo, e risulta quindi soggetta a tutte le regole stabilite per le sottoreti dell'università. In particolare non è consentito implementare in proprio un tale tipo di rete senza l'intervento del gestore della rete e del gruppo sicurezza di rete. Come le sottoreti cablate dell'università anche queste reti devono essere progettate e realizzate dal gestore della rete in accordo con la struttura che ne ha fatto richiesta o per la quale questo tipo di tecnologia è stata ritenuta più idonea dal gestore della rete per soddisfare particolari esigenze ambientali o di mobilità. L'utilizzo delle reti wireless deve essere giustificato da una effettiva esigenza che richieda questo tipo di soluzione, in ragione degli inconvenienti che tale scelta comporta (basse velocità, intercettabilita', estensione del campo d'azione al di fuori dei confini universitari, sicurezza). Per quanto riguarda la sicurezza, l'implementazione della soluzione wireless deve essere tale da garantire l'accesso soltanto agli utenti abilitati (autenticazione) e deve prevedere la crittazione del traffico (riservatezza), per portare il livello di sicurezza di questo tipo di reti allo stesso livello garantito da quelle cablate. Possono essere prese in considerazione reti wireless aperte agli studenti [p.to 3.13] purché realizzino le stesse condizioni di sicurezza previste per le postazioni presenti all'interno delle aule informatiche.

3.8 Assegnazione degli indirizzi IP e sotto-domini logici della gerarchia unimi.it.

Gli indirizzi IP per gli host all'interno della rete d'Ateneo vengono assegnati dal gestore della rete, in modo statico o dinamico (DHCP). Il piano di indirizzamento IP della rete d'ateneo è amministrato dal gestore della rete. Il server DNS relativo a questo piano di indirizzamento è curato e mantenuto dal gestore della rete. La gestione di server DNS primari all'interno delle sottoreti va concordata con il gestore della rete, il quale fornirà presso i suoi server centrali il servizio di DNS secondario per tali server primari locali.
I nomi a dominio corrispondenti ad indirizzi IP della rete GARR, debbono essere registrati sotto il ccTLD "it"; nel caso della rete di Ateneo questo si riduce naturalmente al TLD "unimi.it". Solo in casi eccezionali, riconosciuti da questa Università e dietro autorizzazione del GARR-NIC, possono essere utilizzati domini sotto il gTLD "org": in nessun caso sono ammessi domini registrati sotto altri TLD. Sarà cura del gestore della rete operare le necessarie registrazioni per rendere operativo il nome o filtrare i nomi a dominio che non sono stati richiesti ed autorizzati ed i loro relativi servizi.

3.9 Host multi-homed.

La presenza all'interno della rete di Ateneo di host multi-homed va autorizzata dalla struttura competente e concordata con il gestore della rete, per evitare problemi di routing e di naming. Il traffico relativo alle diverse reti a cui tali host possono essere collegati va mantenuto separato.

3.10 Identificazione dei soggetti in rete

Tutti gli utenti a cui vengono forniti accessi alla rete di Ateneo devono essere riconosciuti ed identificabili; fanno eccezione, gli utilizzi dei computer nel corso delle lezioni ed esercitazioni tenute presso le aule informatiche sotto la sorveglianza del docente, per le quali è richiesta la identificazione dei partecipanti ma non è necessaria la identificazione del singolo utente della singola postazione, ove non praticabile. Al di fuori di questa ipotesi è vietata l'assegnazione di password collettive o non riconducibili ad un singolo soggetto fisico.

3.11 Inserimento in rete di un host.

Per inserire un host nella rete d'ateneo è necessario:

- Richiedere un indirizzo IP al gestore della rete oppure configurare la macchina per riceverlo dinamicamente, a seconda delle istruzioni ricevute dal gestore della rete.
- Installare una protezione antivirus per i sistemi operativi che lo necessitino .
- Controllare se la macchina offre servizi di rete e in caso affermativo eliminarli tutti
- Applicare tempestivamente tutte le patches di sicurezza del sistema e degli applicativi di cui si intende fare uso e mantenerne nel tempo l'aggiornamento

La persona a cui la macchina in rete è data in consegna è ritenuta responsabile per quella macchina e per la sua attività nella rete d'Ateneo

3.12 Limiti di utilizzo della rete da parte degli host.

Un host che produce un grande flusso di dati in rete diviene fonte di problemi per la rete che lo ospita, in questi casi il gruppo sicurezza di rete/IRT potrà limitare l'utilizzo della banda trasmissiva da parte di singoli hosts. Per server o host che necessitino di produrre un elevato volume di traffico è necessario il permesso preventivo del gestore della rete e comunque va con esso concordata una soluzione che incida il meno possibile sulla sottorete d'appartenenza e sulla rete D'ateneo.

3.13 Aule informatiche/laboratori informatici per l'accesso degli studenti.

Le aule informatiche devono essere strutturate come sottoreti private con un unico link di accesso alla rete di ateneo, a indirizzamento IP privato, protette da firewall/gateway. Tutti questi firewall/gateway devono disporre di una configurazione standard stabilita a livello centrale in modo da consentire un'implementazione omogenea delle politiche di sicurezza all'interno della rete d'Ateneo. I server presenti nelle aule sono da considerarsi server di rete locale, cioè i servizi da loro offerti devono essere limitati all'interno dell'aula informatica. Eventuali server di rete vanno posti al di fuori del perimetro della rete privata. Tutti i client interni alle aule informatiche dovranno essere configurati per utilizzare un proxy server centrale d'ateneo per i protocolli http e ftp o un proxy posto in gerarchia con esso, anche amministrato dalla struttura che ospita l'aula, purché tale gerarchia sia concordata con il gruppo sicurezza di rete e con il gestore della rete. L'utilizzo del proxy è condizione necessaria per poter utilizzare questi protocolli al di fuori dell' dell'aula. L'utilizzo del proxy per il protocollo http può essere imposto in modo automatico e trasparente all'utente via meccanismi di redirect. Il set di regole del firewall deve essere adattabile ad ogni singola aula informatica in modo da permettere un

eventuale colloquio tra i server locali e server esterni, a patto che i server interni si comportino come client di quelli esterni, cioè inizino per primi la conversazione. Deve essere inoltre possibile permettere agli host ospitati nelle aule transazioni di dati per applicativi che usino porte TCP diverse dalla porta 80 (http) verso ben identificati server esterni, a patto che gli host interni siano gli iniziatori della conversazione. Il traffico in uscita dalle aule deve essere limitato in banda in ragione del numero delle postazioni presenti nell'aula e della capacità trasmissiva della rete locale in cui l'aula si trova, tale limitazione di banda deve essere attuata sul primo apparato attivo di rete sul quale viene collegato il gateway dell'aula informatica o sul gateway stesso. Il traffico del server proxy centrale deve anch'esso poter essere limitato in banda per contenerne l'impatto, poiché esso raccoglie il traffico di tutte le aule informatizzate nei confronti della rete, rispetto al link GARR verso la rete della ricerca italiana e quindi verso internet. L'autenticazione degli utenti all'interno delle aule può essere a carico delle singole aule informatizzate o appoggiarsi a un sistema di autenticazione centralizzato di ateneo. L'amministrazione dell'aula ha il dovere di registrare, conservare per un anno e fornire su richiesta del gestore della rete o del gruppo sicurezza di rete/IRT solo i seguenti dati fondamentali per venire incontro ad eventuali richieste dell'autorità giudiziaria; l'identità della persona che in un dato momento utilizzava un determinato host interno all'aula (log di login/logout) nel caso di autenticazione locale, o i soli dati di login/logout nel caso di autenticazione centralizzata erogata dall'ateneo.

3.14 Servizi erogati in rete da parte delle strutture periferiche.

Per tutti i servizi di rete che vengono erogati da host appartenenti alla rete di Ateneo è necessario individuare uno o più responsabili che si occupino in maniera continuativa dell'oggetto messo in rete. I servizi che devono essere visibili al di fuori della rete locale della struttura debbono venir registrati a livello centrale dalle strutture di competenza, la registrazione comprende i dettagli dell'implementazione (tipo di servizio, nome e versione dell'applicativo che lo realizza eventuali funzioni accessorie e loro caratterizzazione) dell'accessibilità del servizio (quali utenti sono autorizzati a fruirne, meccanismo di autenticazione, stima del numero massimo possibile di utenti),dei tempi di operatività (data di start-up del servizio, eventuale data di dismissione, tempi in cui il servizio è operativo [es 24x7x365 per servizi sempre on line]) e i dati relativi ai responsabili del servizio sia amministrativi che tecnici. Gli elaboratori messi in rete per erogare uno o più servizi devono limitarsi a questi: tutti i servizi non necessari vanno spenti. I server vanno costantemente aggiornati, sia per i problemi di sicurezza del software relativo ai servizi erogati, sia nelle patches di sicurezza del sistema operativo che li supporta. I servizi devono essere contattabili e utilizzabili soltanto da coloro i quali sono autorizzati a farlo; ovvero bisogna autenticare gli utenti, o le macchine, o le reti che devono poter accedere al servizio. Ovviamente i server pubblici sono contattabili da chiunque nel mondo. I server eseguono il logging delle connessioni e lo mantengono, ove tecnicamente possibile, per un periodo di un anno. I server vanno tenuti sincronizzati con il server di sincronizzazione d'ateneo per permettere una corretta interpretazione dei log. L'accesso privilegiato al sistema deve essere riservato al solo amministratore in modalità locale o in modalità cifrata se effettuato da remoto (ad esempio tramite il protocollo SSH). Devono essere messe in atto almeno tutte le procedure minime per la sicurezza del sistema che ospita il servizio e sul servizio stesso, compresa la protezione contro virus informatici, laddove necessaria, e la protezione fisica della macchina da accessi incontrollati.

Per quanto attiene al servizio di posta elettronica: tutte le strutture dell'università possono dotarsi, se lo desiderano, di un server SMTP per l'inoltro e la ricezione della posta elettronica in aggiunta o alternativa a quello centrale d'ateneo. Questo servizio, oltre a rispondere a tutte le richieste comuni agli altri servizi erogati in rete dalle strutture, deve uniformarsi al livello di sicurezza fornito dal server d'ateneo, ovvero dotarsi di un sistema di scan antivirus e antispam per il traffico SMTP e non permettere il relay. Per l'installazione di un server SMTP le strutture devono farne richiesta al gestore della rete e al gruppo sicurezza di rete precisando i dettagli dell'implementazione; solo a seguito dell'esito positivo di opportuni test di verifica, svolti da tali enti, il servizio di posta potrà essere reso operativo rimuovendo il filtro sulla porta smtp presente sul link di accesso di ogni sottorete universitaria.

3.15 Servizi in outsourcing.

I privati che prendono in outsourcing un servizio per conto dell'università devono uniformarsi al regolamento di sicurezza di questa università e garantire lo stesso livello di sicurezza da questa definito o superiore.

3.16 Attività di logging.

Il gestore della rete opera un'attività di logging sui router della rete WAN allo scopo di produrre statistiche di utilizzo, occupazione di banda e per tipologia di servizio/protocollo atte ad ottimizzare i flussi di dati entro la rete di Ateneo; parte di tali informazioni sono rese pubbliche mediante un sito web. Le strutture che offrono servizi informatici sono tenute, ove tecnicamente possibile, a conservare per un periodo di almeno un anno. la registrazione degli accessi ai servizi in modo da consentire eventuali indagini interne o richieste dall'autorità giudiziaria, in caso di uso improprio delle risorse. Le strutture devono assicurare all'utenza che dette registrazioni non siano disponibili ad alcuno se non nei casi di emergenza o di indagine, nel rispetto della legge sulla tutela dei dati personali

3.17 Provvedimenti verso i trasgressori.

In caso di accertata inosservanza delle norme di utilizzo della rete, l'organismo incaricato prenderà le opportune misure, necessarie al ripristino del corretto funzionamento della rete, compresa la sospensione dell'accesso alla rete stessa da parte del trasgressore per motivi cautelari. In caso di reiterata inosservanza, per colpa grave o dolo, il trasgressore sarà suscettibile di provvedimento disciplinare secondo la normativa vigente. In caso di misure d'emergenza, tese a salvaguardare il funzionamento della rete nel suo insieme o in una delle sue parti (es: attacchi D-DOS, worm ecc.), il gestore della rete o l'Incident Response Team può, come misura transitoria, attuare una sospensione parziale o totale all'accesso alla rete di un singolo o di un'intera LAN, oppure di uno o più servizi di rete o effettuare una riduzione anche drastica nella banda assegnata a una certa struttura o su un particolare link WAN.

3.18 Regolamenti di sicurezza locali.

Le strutture dell'università devono dotarsi di direttive di sicurezza informatica, particolarizzate per le loro realtà. In queste direttive locali vengono specificate le responsabilità e le competenze in ambito di sicurezza informatica, oltre a tutte le ulteriori specifiche di sicurezza che ogni struttura sceglierà eventualmente di darsi. In questo ambito vanno specificati anche i provvedimenti, comminati a livello locale, in cui si incorre a seguito della violazione del regolamento locale e l'entità che si occupa di applicarli. Resta inteso che questi regolamenti locali devono uniformarsi a quelli generali d'ateneo fissati in questo documento e devono essere approvati dal gruppo sicurezza di rete prima di divenire operativi.

3.19 Acceptable Use Policy (AUP)

A tutti gli utenti della rete d'ateneo deve essere distribuito un documento – AUP - che renda noti per sommi capi i contenuti del regolamento di sicurezza d'ateneo nei riguardi dei comportamenti da tenere nell'uso della rete e dei servizi dell'ateneo.

4 DEFINIZIONE DEL REGOLAMENTO DI SICUREZZA PER I DATI.

4.1 Protezione dei dati personali e dei sistemi

Ciascuna struttura universitaria che tratta dati personali deve operare nel rispetto delle disposizioni contenute nel decreto legislativo n. 196 del 30 giugno 2003 “Codice in materia di protezione dei dati personali” e s.m.i. e del correlato regolamento adottato dall’Università degli Studi di Milano.
Per la sicurezza dei dati e dei sistemi le strutture devono seguire le indicazioni riportate nel predetto codice e nel documento programmatico sulla sicurezza di cui l’Università si è dotata.

5 DEFINIZIONE DEL REGOLAMENTO DI SICUREZZA PER I SERVIZI INFORMATIVI E I SERVER CENTRALI D'ATENEO.

I server che erogano in rete un servizio informatico in nome e per conto dell'ateneo, cioè tutti server centrali gestiti dalle divisioni tecniche dell'università e ogni altro server che debba fornire un servizio ufficiale d'ateneo, devono uniformarsi alle particolari direttive di sicurezza e continuità del servizio descritte di seguito.

In particolare le direttive per questi server riguardano:

- Sicurezza fisica/controllo accessi
- Continuità del servizio/disaster ricovery
- Integrità dati e sistemi
- Antivirus/worm/trojan
- Aggiornamenti dei sistemi operativi
- Gestione delle password
- Management locale e remoto
- Logs di sistema e loro controllo
- Configurazioni di base per la sicurezza
- Interventi sui sistemi da parte di personale esterno

I servizi ufficiali erogati dall'ateneo devono uniformarsi al regolamento descritto nel seguito. In particolare le direttive per questa tipologia di servizi riguardano:

- Privilegi dei servizi
- Aggiornamenti
- Gestione delle password
- Accessi ai servizi
- Logs e loro controllo
- Statistiche sui servizi offerti

5.1 Definizioni

Sono considerati servizi centrali di ateneo tutti quei servizi informatici erogati in nome e per conto dell'ateneo dalle strutture amministrative centrali e che vengono utilizzati per l'amministrazione dell'ateneo e per la ricerca: rientrano in questa definizione tutti i servizi erogati dalla Divisione Sistemi Informativi, dalla Divisione Telecomunicazioni e i servizi informatici erogati dalla Divisione Coordinamento Biblioteche.

Nel presente documento, con server centrali di ateneo si indicano i sistemi che ospitano i servizi informatici centrali di ateneo.

Previo parere della Commissione Permanente per la Sicurezza, anche altre strutture possono erogare servizi informatici centrali di ateneo; l'ambito di applicazione delle direttive descritte nel presente documento si estende anche a questi.

5.2 Soggetti Coinvolti

Il presente documento è rivolto alle strutture che decidono di implementare servizi centrali di ateneo.

Le direttive sono suddivise per profilo e riguardano gli amministratori di sistema (gestori dei server che ospitano i servizi), i gestori delle applicazioni (responsabili dei servizi erogati) e altri soggetti interessati quali, per esempio, utenti e fornitori.

5.3 Regole Generali per la Struttura

La struttura deve nominare un responsabile per ciascun sistema e per ciascun servizio applicativo; discrezionalmente, in funzione della natura dei sistemi e dei servizi, una stessa persona può essere nominata responsabile di più sistemi e/o servizi.

La struttura deve inoltre nominare al proprio interno un responsabile della sicurezza, eventualmente coincidente con uno dei responsabili di sistema o servizio, con il compito di:

- svolgere un'attività di supervisione e coordinamento tra i vari responsabili interni dei server e delle applicazioni in tema di sicurezza informatica;
- costituire l'interfaccia ufficiale della struttura nei confronti del gruppo sicurezza di rete per le tematiche connesse alla sicurezza dei sistemi e dei servizi offerti;
- costituire l'interfaccia ufficiale della struttura nei confronti dell'Incident Respose Team per le emergenze connesse alla sicurezza di sistemi e servizi.

La struttura deve poi stilare un regolamento interno di sicurezza e, qualora lo ritenga opportuno, una carta dei servizi.

Il regolamento di sicurezza sarà un documento ad uso strettamente interno che conterrà le norme di sicurezza specifiche per i sistemi presenti, i servizi effettivamente erogati e il trattamento dei dati ospitati; non dovrà essere in disaccordo con ll regolamento generale di ateneo e dovrà essere sottoposta all'approvazione del gruppo sicurezza di rete.

La carta dei servizi sarà invece un documento destinato alla diffusione e conterrà l'informativa generale per il pubblico con la descrizione dei servizi erogati, tempi e modi di fruizione del servizio, modulistica per le richieste di adesione al servizio, indirizzi di posta elettronica e i numeri di telefono del personale tecnico cui fare riferimento in caso di problemi nell'utilizzo di un servizio, etc.

5.4 Regole Generali per i Sistemisti - Gestione dei Server

Criteri Generali

Gli amministratori di sistema devono garantire l'efficiente fruibilità del servizio minimizzando il rischio di usi impropri.

Essi devono garantire, per quanto possibile, la disponibilità del servizio secondo i tempi e i modi previsti dal regolamento interno di sicurezza e dalla eventuale carta dei servizi e operare in modo da minimizzare il rischio di:

- accessi non autorizzati al sistema;
- accessi non autorizzati ai dati;
- usi impropri del sistema che possano arrecare danno ad altri utenti del sistema, al sistema stesso o ad altri sistemi collegati alla rete dell'ateneo o alla Internet;
- usi impropri del sistema ovvero non attinenti alle attività istituzionali o comunque estranei alle finalità del trattamento dei dati, anche da parte degli utenti autorizzati.

Sicurezza Fisica di Base dei Sistemi

Al fine di proteggere i sistemi, i locali che li ospitano dovranno possedere alcune caratteristiche indipendenti dal tipo di piattaforme hardware e dai sistemi operativi adottati.

Più precisamente, è opportuno che tali locali siano:

- dedicati ai server e preferibilmente presidiati;
- dotati di un sistema, meccanico o elettronico, di selezione degli accessi;
- dotati di un sistema di estinzione degli incendi;
- equipaggiati con dispositivi di stabilizzazione e continuità della tensione;
- climatizzati.

Eventuali interventi di qualsiasi natura (anche non informatica) in tali locali devono sempre avvenire in presenza di personale autorizzato.

In aggiunta a queste misure è consigliabile l'adozione di ulteriori accorgimenti per la restrizione degli accessi da implementare direttamente sui server, tra cui:

- l'impostazione di password per l'accesso al BIOS;
- il settaggio del BIOS in modo tale che l'avvio del sistema possa avvenire esclusivamente dal disco rigido di sistema.

Sicurezza Logica di Base dei Sistemi

Gli amministratori di sistema dovranno prevedere alcuni meccanismi per la sicurezza logica dei server che consentano di ridurre il rischio di esposizione dei dati e di accessi indesiderati ai server.

Protocolli e Socket TCP-UDP aperti sui sistemi

I server dovranno avere attivi solo i protocolli effettivamente necessari, tenendo presente che a livello di ateneo viene instradato esclusivamente il traffico IP; a livello IP dovranno essere attivi solo i protocolli strettamente necessari per il corretto funzionamento delle applicazioni.

A livello TCP e UDP dovranno essere disabilitate tutte le porte inutili e pericolose: dovranno essere aperte solo le porte strettamente necessarie per il funzionamento delle applicazioni (sui sistemi unix, ad esempio, è preferibile disattivare porte quali systat, netstat, finger, smtp, r-utilities, chargen, syslog, echo, etc).

Aggiornamento dei Sistemi Operativi e Patch di Sicurezza

Gli amministratori devono prestare attenzione agli alert in tema di sicurezza per i sistemi che gestiscono (con particolare riferimento alla vulnerabilità dei sistemi operativi e alle applicazioni di base), installare le patches non appena disponibili e valutare le azioni da intraprendere nel periodo intermedio in base al tipo e livello di rischio.

In ogni caso i sistemi operativi e i pacchetti di base dovranno essere regolarmente aggiornati, compatibilmente con le applicazioni installate sui sistemi.

Monitoraggio e Logging

I sistemi dovranno disporre di procedure per la registrazione dei messaggi di sistema e delle applicazioni di base attraverso meccanismi di logging per tutte le operazioni critiche.

I log di sistema devono essere analizzati regolarmente, preferibilmente per mezzo di meccanismi automatici di scansione in grado di generare allarmi a seguito di eventi rilevanti per la sicurezza del sistema.

Selezione e Controllo del Traffico Diretto ai Sistemi

I sistemi dovranno essere configurati in modo da accettare connessioni solo da parte dei client autorizzati e dagli amministratori.

Ove possibile, a livello di rete dovranno essere adottati sistemi per il controllo e la selezione del traffico di rete (traffic filtering, firewalling, etc.) previo accordo con il gruppo sicurezza di rete ed il gestore della rete.

Nel caso in cui l'amministrazione dei server venga effettuata anche da remoto, la comunicazione tra il client e il server dovrà avvenire in maniera cifrata, il server dovrà essere configurato in modo da non accettare chiamate dirette all'utente superuser e le chiamate dovranno essere limitate ad un gruppo identificato di indirizzi IP sorgenti.

Gestione degli Account per l'Accesso ai Sistemi

Gli amministratori devono assegnare a ciascun utente una userid personale per l'accesso ai sistemi: una stessa userid non può essere assegnata a persone diverse neanche in tempi diversi, con l'eccezione delle userid di amministrazione se i sistemi operativi usati ammettono un solo livello di userid per l'amministrazione.

Gli accessi degli amministratori devono comunque avvenire in prima istanza con la userid personale per consentire la tracciabilità delle sessioni.

Gli amministratori devono prontamente disattivare le userid degli utenti se questi perdono il diritto di accesso ai sistemi o se le userid rimangono inutilizzate per più di sei mesi.

Le password di amministrazione dei sistemi dovranno essere:

- cambiate spesso
- note esclusivamente agli amministratori
- diverse per ciascun sistema
- diverse da quelle già utilizzate in passato
- non coincidenti con le userid di amministrazione, neanche temporaneamente
- non banali e comunque di complessità adeguata al tipo di sistema
- non usate per scopi diversi dall'amministrazione dei sistemi

Si presti particolare attenzione a che nessun applicativo faccia uso delle password di amministrazione, nè abbia bisogno dei privilegi di amministratore per il corretto funzionamento.

Protezione da Virus Informatici

I sistemi che ne necessitano devono essere dotati di applicazioni per la difesa da parte di virus informatici, worm, trojan e, in generale, codice indesiderato e dannoso.

Tali applicazioni dovranno avere, di preferenza, la possibilità di controllare i file in tempo reale e di notificare automaticamente la presenza di un virus nel sistema.

Le applicazioni antivirus dovranno essere aggiornate in maniera automatica su base periodica; dovranno inoltre consentire la possibilità di aggiornamento manuale per far fronte ai casi di emergenza, per esempio in seguito a segnalazioni di diffusione di virus importanti.

Interventi sui Sistemi da Parte di Personale Esterno

Gli accessi ai sistemi da parte di personale esterno, fornitori di hardware o di servizi, dovranno avvenire sotto la supervisione degli amministratori.

Qualora si rendesse necessario comunicare una o più password di amministrazione, di sistema o di base dati, le stesse dovranno essere sostituite prima e dopo il periodo di utilizzo in modo da svincolarle da un'eventuale logica di assegnazione adottata.

Nel caso di interventi che richiedano l'accesso per un periodo prolungato da parte di fornitori (es. upgrade, manutenzione, installazioni, test, etc.), le modalità di accesso dovranno essere definite a livello contrattuale.

Gli accessi con i privilegi di amministrazione devono di norma avvenire da postazioni interne alla struttura. Eventuali accessi dall'esterno dovranno essere ridotti al minimo indispensabile, ove possibile in maniera cifrata e in ogni caso valutati con estrema cautela.

Continuità del Servizio e Disaster Recovery

In caso di fermo, i servizi dovranno essere ripristinati nei tempi definiti dal regolamento interno di sicurezza e dalla eventuale carta dei servizi.

Per i fermi causati da guasti hardware è possibile stipulare contratti di manutenzione nei quali siano specificati i tempi di intervento oppure, qualora la struttura disponga di personale qualificato, dotarsi di parti di ricambio o sistemi alternativi che consentano alla struttura stessa di far fronte alle emergenze con mezzi propri nei tempi stabiliti.

Per i fermi di natura software o legati alla consistenza delle banche dati, dovranno essere implementati opportuni meccanismi di backup, le cui modalità e tempistiche dovranno essere specificate nel regolamento interno di sicurezza.

5.5 Regole per gli Applicativi – Gestione dei Servizi Centrali di Ateneo

Criteri Generali

Gli amministratori delle basi di dati e i gestori delle applicazioni devono garantire l'efficiente fruibilità dei servizi applicativi minimizzando il rischio di usi impropri.

Essi devono adoperasi, per quanto possibile, a rendere disponibili dei servizi secondo i tempi e i modi previsti dal regolamento interno di sicurezza e dalla carta dei servizi e operare in modo da minimizzare il rischio di:

- accessi non autorizzati ai dati;
- usi impropri delle applicazioni che possano arrecare danno ad altri utenti del sistema, al sistema stesso o ad altri sistemi collegati alla rete dell'ateneo o alla Internet;
- usi illeciti dei dati o non attinenti alle attività istituzionali anche da parte degli utenti autorizzati.

Gestione degli Account per l'Accesso ai Servizi Applicativi

I gestori dei servizi applicativi devono assegnare a ciascun utente una userid personale: una stessa userid non può essere assegnata a persone diverse neanche in tempi diversi e non sono ammesse userid condivise per gruppi di utenza.

Nel caso di account per accessi espliciti a database valgono le stesse regole, con la sola eccezione della userid di superuser se il database ammette un solo livello di userid per l'amministrazione.

Gli accessi degli amministratori dei database e dei gestori delle applicazioni devono comunque avvenire in prima istanza con la userid personale per consentire la tracciabilità delle sessioni.

Gli amministratori e i gestori devono disattivare prontamente le userid degli utenti se questi perdono il diritto di accesso al servizio o se le userid rimangono inutilizzate per più di sei mesi.

Le password di amministrazione dei database e delle istanze dovranno essere:

- cambiate spesso;
- note esclusivamente agli amministratori;
- diverse per ciascuna base dati e istanza;
- diverse da quelle già utilizzate in passato;
- non coincidenti con le userid di amministrazione, neanche temporaneamente;
- non banali e comunque di complessità adeguata al tipo di dati custoditi;
- non usate per scopi diversi dall'amministrazione delle basi dati.

Accessi ai Servizi

Gli accessi ai servizi devono avvenire secondo le modalità e i tempi previsti dal regolamento interno di sicurezza e dalla eventuale carta dei servizi emessa dalla struttura.

I gestori delle applicazioni devono prendere misure opportune per assicurare la fruibilità del servizio agli utenti autorizzati e minimizzare i rischi di accesso da parte di altri utenti.

Attivazione di Nuovi Utenti

I gestori dei servizi applicativi devono predisporre sistemi di registrazione degli utenti con le informazioni minime necessarie per la trasmissione delle comunicazioni di servizio.

Al momento dell’attivazione, i gestori devono informare i nuovi utenti sulle modalità di accesso al servizio, fornire l’assistenza necessaria per la corretta procedura di connessione e informarli che, in caso di emergenza e per motivi di sicurezza, le userid possono essere disattivate anche senza preavviso.

I gestori devono inoltre informare gli utenti sulle responsabilità personali in caso di utilizzo da parte di terzi della propria password personale: tutti gli accessi effettuati con quella coppia userid-password saranno attribuiti a quell'utente anche se effettuati da altri.

Gli utenti devono pertanto essere invitati a:

- utilizzare i permessi di accesso esclusivamente per le finalità previste;
- non cedere la propria coppia userid-password a terzi;
- non lasciare in vista note o appunti che riportano userid e password;

- effettuare il logout dalle applicazioni e/o dal sistema oppure bloccare la workstation o attivare lo screen-saver con password in caso di allontanamento dalla stazione di lavoro;
- adottare password non banali
- sostituire periodicamente le password personali senza riutilizzare quelle già adottate in passato.

In relazione alla natura dei dati coinvolti, potrà essere chiesto agli utenti di firmare un modulo dal quale risulti che sono stati informati sulle regole di sicurezza da osservare.

Logging e Controllo

Le applicazioni devono prevedere un meccanismo di logging che consenta di tracciare le sessioni fino ad un livello di dettaglio ragionevole in virtù del tipo di applicazione.

I log devono essere regolarmente analizzati e conservati per un periodo non inferiore ad un anno.

L'analisi dei log potrà avvenire manualmente ma è fortemente consigliata l'adozione di un sistema automatico in grado di segnalare tempestivamente situazioni anomale.

Statistiche sui Servizi Offerti

È fortemente consigliata la predisposizione di un meccanismo di creazione e analisi delle statistiche di utilizzo di ciascun servizio erogato che permetta di valutare, ad esempio, il livello effettivo di accessi da parte dell'utenza, la banda di rete impegnata e il livello di carico imposto al sistema.

L'analisi delle statistiche in relazione ai dati storici, fornisce elementi oggettivi importanti ai fini del dimensionamento dei sistemi e dei servizi e consente di valutare l'opportunità di estendere o sospendere i servizi stessi. Inoltre consente di rilevare eventuali attività anomale che comportino, ad esempio, un aumento improvviso del volume di richieste, di carico di sistema o di traffico di rete.

I parametri da utilizzare per la creazione degli archivi statistici potranno essere specificati nel regolamento interno di sicurezza stilato della struttura.

Gestione Remota dei Servizi

Nel caso in cui l'amministrazione dei servizi venga effettuata anche da remoto, la comunicazione tra il client e il server dovrà avvenire in maniera cifrata, il servizio dovrà essere configurato in modo da non accettare chiamate dirette all'utente superuser e le chiamate dovranno essere limitate ad un gruppo identificato di indirizzi IP sorgenti.

5.6 Regole per lo Sviluppo e l'Installazione delle Applicazioni

Le seguenti direttive valgono per tutte le applicazioni e i programmi installati sui sistemi, siano essi shareware, con licenza di pubblico utilizzo, acquistati su licenza o sviluppati ad hoc internamente o da aziende esterne fornitrici di servizi.

Privilegi dei Servizi

Nessun servizio applicativo può fare uso delle password di amministrazione, siano esse di sistema, di database o di istanza.

Inoltre nessun servizio applicativo dovrà aver bisogno dei privilegi di amministratore a nessun livello.

Gli amministratori dei database e i gestori dei servizi applicativi dovranno essere in condizione di poter sostituire le proprie password in qualunque momento senza che ciò abbia alcun impatto sul corretto funzionamento degli applicativi.

Inserimento di Password nel corpo dei Programmi

L'inserimento di password nel corpo dei programmi, ad esempio per evitare all'utente la digitazione di una serie di userid-password per l'accesso ad una sola applicazione, è una pratica pericolosa; come tale, di norma, deve essere evitata.

Nel caso in cui tale pratica sia indispensabile, si devono osservare le seguenti regole:

- l'utente deve essere sempre identificabile: non è consentito effettuare tutte le autenticazioni in automatico ma almeno una password deve essere inserita manualmente dall'utente;
- le password non possono essere memorizzate in chiaro;
- le password devono poter essere cambiate: deve esistere una procedura attivabile centralmente che ne permetta la sostituzione senza intervento da parte degli utenti;
- gli utenti non devono conoscere le password embedded;
- una password embedded deve essere relativa ad una sola applicazione, non può coincidere con le password di amministrazione e non deve essere usata per altri scopi.

Aggiornamenti di Release

Gli amministratori dei database e i gestori delle applicazioni devono prestare attenzione agli alert in tema di sicurezza per le piattaforme applicative gestite, con particolare riferimento alla possibilità di intrusione e di perdita dei dati.

In presenza di exploit o vulnerabilità devono installare le patches non appena disponibili e valutare le azioni da intraprendere nel periodo intermedio in base al tipo e livello di rischio.

Nel caso di applicazioni custom, le attività di sviluppo, test e staging del nuovo software dovranno avvenire su appositi sistemi diversi da quelli in produzione.

I server di staging dovranno essere quanto più possibile allineati ai server di produzione in modo da agevolare l'introduzione del nuovo software.

Nel caso in cui lo sviluppo degli applicativi venga affidato a consulenti, fornitori di servizi o comunque personale esterno, l'installazione sui server di produzione dovrà avvenire sotto stretto controllo da parte degli amministratori.

In ogni caso eventuali interruzioni del servizio dovranno essere segnalate all'utenza con congruo anticipo specificando i tempi di fermo.

Prima di procedere con le nuove installazioni, sarà cura degli amministratori e degli sviluppatori adottare le dovute precauzioni affinché in caso di fallimento dell'upgrade sia possibile ritornare in tempi brevi alla versione precedente.