FACOLTÀ DI ECONOMIA

SAPIENZA
UNIVERSITÀ DI ROMA

Il Preside

Al Direttore Generale

Sapienza Università di Roma

Dott.ssa Simonetta Ranalli

e p.c.

al Direttore del Centro InfoSapienza

Sapienza Università di Roma

Dott.ssa Raffaela Iovane

Caro Direttore,

facendo seguito alla Circolare del Direttore Generale del 5 Luglio 2017, relativa alla misure minime di sicurezza ICT per le pubbliche amministrazioni indicate nella circolare AGID del 18 Aprile 2017, come avevo già avuto modo di comunicarti, all'interno della Facoltà di Economia è stato costituito un gruppo di lavoro composto dal Delegato del Preside per l'ICT all'interno della Facoltà, dal Referente Informatico di Facoltà e dai Referenti Informatici dei quattro Dipartimenti che compongono la Facoltà stessa. Tale gruppo ha elaborato un progetto congiunto di attività che ha come obiettivo quello di sviluppare una attività organica e coordinata per adempiere a quanto richiesto dalla citata circolare per tutte le macchine che operano all'interno della Facoltà. Sempre all'interno di questo progetto, sono state messe a sistema tutte le attività sinora svolte dai singoli referenti dei Dipartimenti a livello di amministrazione ed unite all'interno del progetto di cui sopra.

Il piano così elaborato, che ancora non è stato reso operativo unicamente perché è necessario perfezionare le procedure di acquisto dell'hardware e del software previsto ma che verrà messo a regime entro il mese di Gennaio, è stato approvato all'unanimità nell'ultima Giunta di Facoltà dello scorso 7 Dicembre, cui hanno preso parte, oltre i Direttori dei Dipartimenti, anche i relativi Referenti per l'Informatica. Il documento che si riporta in allegato a questa nota, corredato anche dall'estratto della delibera della Giunta di cui sopra, si compone di una nota tecnica esplicativa

Sapienza Università di Roma – Facoltà di Economia
Presidenza
Via del Castro Laurenziano, 9 – 00161 Roma
T (+39) 06 49.766.921 F (+39) 06 49.41.621
www.economia.uniroma1.it

delle varie attività che verranno svolte e di un diagramma di Gantt in cui vengono riportate le singole tempistiche di ogni attività.

Ci tengo a sottolineare che con le attività che verranno svolte e che sono singolarmente dettagliate nel documento, si potrà ottemperare a tutte le prescrizioni della nota AGID, sia quelle con tempistica più immediata e sia quelle previste per il futuro.

Con l'intenzione di potere svolgere una operazione costruttiva e sinergica, la Giunta di Facoltà ha, inoltre deliberato di mettere a disposizione dell'Ateneo sin da subito questo documento, pur nella consapevolezza della dilazione dei termini per la presentazione delle attività, in modo da potere contribuire, se lo si riterrà utile ed interessante, a dare un contributo ad una attività coordinata che potrà essere disponibile anche per altre strutture che volessero ispirarsi.

Alla fine del documento sono riportati i nominativi di tutti i colleghi che hanno fatto parte del gruppo e la presente è una ottima occasione per ringraziarli di tutto il lavoro che hanno prestato.

Mantenendo la massima disponibilità in caso di richieste di chiarimenti o approfondimenti, approfitto per formulare i migliori auguri per le prossime festività.

Un saluto cordiale.

Prof. Fabrizio D'Ascenzo

SAPIENZA
UNIVERSITÀ DI ROMA

Estratto
Verbale della Giunta di Facoltà

Seduta ordinaria del 7 dicembre 2017

Il giorno **giovedì 7 dicembre 2017 alle ore 10:00** presso la Sala delle Lauree, si è riunita la Giunta di Facoltà di Economia, convocata in seduta ordinaria dal Preside, prof. Fabrizio D'Ascenzo, per la discussione del seguente

ORDINE DEL GIORNO

Approvazione verbale della seduta del 14 novembre 2017

Comunicazioni

1. **Autorizzazioni**
2. **Pratiche studenti**
3. **Didattica**
   - Programmazione didattica 2017/2018
   - Scheda SUA-CdS 2018/2019 – Procedure e tempistica
4. **Reclutamento personale docente**
5. **Eurosapienza** - Assegnazione uso locali
6. **Fondo sostegno giovani**
7. **Sicurezza informatica di Facoltà** – Piano degli investimenti
8. **Personale TA Presidenza**
9. **Centro di spesa**
10. **Varie**
11. **Proposta del Dipartimento di Management per il conferimento della Laurea *Honoris Causa* in Intermediari, finanza internazionale e risk management al dott. Fabio Gallia**

12. **Contratto di consulenza professionale per esperto di particolare e comprovata specializzazione linguistica: avvio procedure**

Presiede la seduta il Preside, Prof. Fabrizio D'Ascenzo; assume le funzioni di segretaria verbalizzante la coordinatrice degli uffici di Presidenza Rita Giuliani. Partecipa alla seduta il Vice-Preside Vicario Francesco Maria Sanna, il delegato del Preside agli Affari amministrativi Marco Benvenuti, il Manager didattico Hermes Setti, il Capo settore Segreteria studenti Economia Antonio Onorati, il Presidente del CAD di Latina Bernardino Quattrociocchi, i referenti informatici dei dipartimenti di Facoltà: Riccardo Sucapane, Enrico Mastrostefano, Stefano Sansone e Luigi Basilici, Domenico D'Orazi.

Alle ore 10:15, constatata la presenza del numero legale, come risulta dall'allegato A, si apre la seduta.

Sapienza Università di Roma – Facoltà di Economia
Presidenza
Via del Castro Laurenziano, 9 – 00161 Roma
T (+39) 06 4976(2)6921 F (+39) 06 4976(2)6097
www.economia.uniroma1.it

ORDINE DEL GIORNO

.....omissis.....

7. **Sicurezza informatica di Facoltà** – Piano degli investimenti

Il Preside informa la Giunta che, in riferimento alla comunicazione del Direttore Generale del 5 luglio 2017, riportante le misure di sicurezza ICT per le pubbliche amministrazioni indicate nella Circolare AGID del 18 aprile 2017, dovranno essere adottate, entro il 15 dicembre 2017 le misure minime di sicurezza informatica, evidenziate nella circolare. Il Preside invita il dott. Basilici ad illustrare le azioni necessarie e la proposta per una gestione centralizzata dell'adeguamento.
Il dott. Basilici interviene e riferisce che l'obiettivo dell'intervento ha il fine di contrastare le minacce più comuni e frequenti a cui sono soggette le PP. AA. In particolare derivanti da attacchi informatici e fenomeni di pirateria.
Sulla base delle premesse sopra riportate, si rende necessario un intervento di verifica, integrazione e aggiornamento dell'infrastruttura di rete della Facoltà nonché le modifiche delle impostazioni su ogni dispositivo (PC, notebook, tablet etc.) collegato alla rete pubblica o privata della stessa.
Da una ricognizione fatta emerge che per ottemperare a quanto richiesto dobbiamo creare una rete di servizio, completamente dedicata alle operazioni di backup.
Tutto questo è possibile grazie alla ridondanza di cavi in fibra che da ogni armadio di piano, raggiungono il Servizio di Calcolo su cui verranno installati detti dispositivi.
Tale strategia è necessaria per non saturare la banda a disposizione ed evitare così il collasso della rete nel momento in cui le postazioni effettuano le operazioni di backup.

Il Preside, in considerazione dell'imminente scadenza del termine entro il quale è necessario presentare il piano di sicurezza informatica e tenuto conto delle indicazioni sopra citate, propone alla Giunta di approvare il piano complessivo degli investimenti e di procedere alla ripartizione dei costi tra le strutture in accordo tra i RAD e i Direttori dei Dipartimenti.

DELIBERAZIONE N. 427/2017

La Giunta di Facoltà

Vista la comunicazione del Direttore Generale del 5 luglio 2017, riportante le misure di sicurezza ICT per le pubbliche amministrazioni indicate nella Circolare AGID del 18 aprile 2017;
Tenuto conto che il termine previsto per l'adozione delle misure minime di sicurezza informatica **è il** 15 dicembre 2017;

delibera

con voto unanime e seduta stante di approvare il piano di sicurezza informatica e il piano complessivo degli investimenti.

.....omissis.....

Null'altro essendovi da discutere e deliberare, la seduta termina alle ore 12:28

.....omissis.....

Preside
f.to Prof. Fabrizio D'Ascenzo

Segretaria verbalizzante
f.to dott.ssa Rita Giuliani

Il presente estratto, composto da n. 3 pagine, è conforme al verbale originale depositato agli atti di questa Facoltà.

Preside
Prof. Fabrizio D'Ascenzo

Allegati:
A – Presenze Giunta

Progetto per la Sicurezza ICT
Facoltà di Economia

Acronimi

IP	Internet Protocol
Indirizzo IP	Indirizzo univoco di una macchina all'interno di una rete
MMS	Misure Minime di Sicurezza AgID
Firewall	Hardware/Software che filtra il traffico di rete
LDAP	Lightweight Directory Access Protocol
VLAN	Virtual Local Area Network, una sottorete della rete principale

1. Premessa

In riferimento alla comunicazione del Direttore Generale del 5 luglio 2017 - misure minime di sicurezza ICT per le pubbliche amministrazioni indicate nella Circolare AGID del 18 aprile 2017, i referenti informatici dei Dipartimenti afferenti alla Facoltà di Economia e il delegato del preside ICT di Facoltà di Economia sono stati invitati a coadiuvare le operazioni di implementazione delle misure previste dalla normativa. Valutata l'esigenza comune di procedere in modo coordinato, è stato costituito un gruppo di lavoro per definire modalità adeguate per ottemperare a quanto richiesto.

L'obiettivo delle disposizioni è fornire tempestivamente alle PA un riferimento normativo per consentire di intraprendere un percorso di progressiva verifica e adeguamento in termini di sicurezza informatica. Le misure minime di sicurezza informatica indicate prevedono tre diversi livelli di attuazione e costituiscono parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione.

Il Gruppo di lavoro, dopo un'attenta analisi del documento AgID e a seguito di una valutazione della situazione attuale, ha cercato di individuare la migliore soluzione possibile per poter implementare nel breve periodo le misure minime e adottare un sistema in grado di garantire la gestione e il controllo nel tempo dell'efficacia dell'azione intrapresa.

E' opportuno evidenziare da subito la difficoltà dovuta alla situazione eterogenea sia del parco macchine, sia dell'utilizzo specifico delle stesse all'interno della Facoltà. In particolare, risulta difficile l'implementazione delle misure minime di sicurezza sulle macchine affidate esclusivamente ai docenti, come descritto nei paragrafi successivi.

2. Livelli minimi di sicurezza richiesti da Agid

Le misure minime di sicurezza (MMS) descritte nel documento AgID prevedono tre livelli di attuazione: *minimo, standard, alto*. Il primo stadio di attuazione (minimo) prevede l'implementazione entro il 2017 di una serie di misure articolate in macro aree, dette AgID Basic Security Control(s) (ABSC).
Per completezza riportiamo di seguito gli ABSC:

- ABSC 1: INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI.
  Gestire attivamente tutti i dispositivi hardware sulla rete (monitorandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

- ABSC 2 INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI.
  Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

- ABSC 3: PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER.
  Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni

- ABSC 4: VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ.
  Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

- ABSC 5: USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE.
  Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

- ABSC 8: DIFESE CONTRO I MALWARE.
  Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

- ABSC 10: COPIE DI SICUREZZA.
  Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni, così da consentirne il ripristino in caso di necessità.

- ABSC 13: PROTEZIONE DEI DATI.
  Processi interni, strumenti e sistemi necessari per evitare il furto di dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti

3. **Analisi del contesto della Facoltà di Economia**

I Dipartimenti

I referenti informatici, dopo una valutazione dello stato dei rispettivi parchi macchina, hanno rilevato le seguenti criticità in una elevata percentuale di postazioni di lavoro:

- Gli utenti, anche in mancanza delle necessarie competenze, hanno account con privilegi di amministratore.
- Le password utente non rispettano i requisiti previsti dai criteri minimi di sicurezza.
- I software ed i sistemi operativi non sono sistematicamente aggiornati e/o l'aggiornamento è affidato all'iniziativa del singolo utente.
- Non esiste un elenco di software autorizzati.
- I backup dei dati non sono effettuati regolarmente.
- Non vengono effettuate immagini di sicurezza del disco dei pc
- La riservatezza di alcuni dati sensibili non è garantita.
- Non esiste una procedura di controllo delle vulnerabilità presenti.
- Non esiste una procedura standard per la mappatura delle macchine che hanno accesso alla rete privata.

La rete di Facoltà

L'infrastruttura di rete della Facoltà interconnette tutti i dipartimenti, gli uffici della presidenza, la biblioteca centrale, la segreteria studenti, le aule e tutti i laboratori presenti.
La connessione di queste strutture avviene attraverso 15 armadi *rack* di piano, interconnessi in fibra ottica con il centro stella posizionato nei locali del Servizio di Calcolo che gestisce oltre i servizi telematici di facoltà anche la connessione al backbone d'Ateneo.
Sono presenti 12 laboratori informatici utilizzati da studenti con 360 personal computer installati. Sono 540 il numero di postazioni a disposizione del personale TAB e dei Docenti.
Sono state identificate le seguenti criticità:

- obsolescenza delle macchine attualmente adibite al controllo del traffico di rete;
- disomogeneità della rete interna (pubblica/privata);
- nessuna corrispondenza tra utente e dispositivo (PC) utilizzato.

Considerazioni generali sullo stato di fatto

Si evidenzia la necessità di iniziare un lavoro coordinato che coinvolga tutte le varie realtà della Facoltà per poter implementare le misure minime di sicurezza indicate da AgID. Inoltre si auspica il consolidamento delle macchine server presso il Servizio di Calcolo.

Tra gli aspetti analizzati si è riscontrato che il coinvolgimento del personale docente ed amministrativo rappresenta un punto fondamentale per l'implementazione delle misure di sicurezza. La situazione attuale è molto eterogenea ma, sia il personale TAB che il personale docente è stato abituato nel corso degli anni ad una gestione autonoma delle postazioni disponibili. Per il personale TAB, in generale, non sussiste una difficoltà oggettiva nell'implementazione delle MMS, in quanto l'utilizzo delle macchine è ben definito e standardizzato. Il personale TAB avrà un account con privilegi limitati mentre il ruolo di amministratore e responsabile della macchina verrà affidato al personale tecnico con le opportune competenze.

Risulta, invece, problematico garantire le MMS sui PC in dotazione ai docenti:
in primo luogo, data l'eterogeneità dell'utilizzo, esiste una difficoltà oggettiva nel definire una configurazione standard, inoltre, non è semplice valutare l'opportunità di lasciare o togliere i privilegi di amministratore a ciascun docente rischiando, nel secondo caso, di limitare la possibilità di gestione autonoma della propria macchina per le specifiche esigenze di didattica e di ricerca.

Occorre trovare una soluzione che garantisca al docente la possibilità di scegliere se amministrare il proprio PC salvaguardando al contempo la sicurezza della rete di Facoltà.

3. **Studio di fattibilità**

Introduzione

Attualmente la gestione del parco macchine è affidata a ciascun dipartimento, in modo non strutturato ed incompleto rispetto a quanto previsto dalla normativa.
La soluzione ottimale individuata dal gruppo di lavoro consiste nella realizzazione di una infrastruttura centralizzata che permetta, in modo efficace ed efficiente, di ottemperare alle richieste contingenti e, più in generale, ad una gestione organica degli strumenti hardware e software utilizzati.
La soluzione ipotizzata prevede:

- centralizzazione dei server DHCP, DNS (interno e forwardato verso DNS sapienza), VPN, LDAP (locale e forwardato verso ldap sapienza), Siti Web istituzionali di Facoltà e Dipartimento;
- armonizzazione dei siti web per la didattica, per la gestione degli spazi comuni e delle risorse.

La soluzione ipotizzata consentirà:

- di rispondere in modo adeguato alle richieste attuali;
- adattabilità alle future richieste previste dalla circolare AgID;
- scalabilità rispetto alle future esigenze delle strutture di Facoltà;
- di monitorare il software e l'hardware utilizzati con conseguente semplificazione delle procedure di programmazione degli acquisti.

Implementazione misure AgID - Studio di fattibilità per la rete di facoltà

Al fine di monitorare l'attività degli utenti nella rete e, soprattutto, per poter individuare i comportamenti *maliziosi* e risalire alla macchina da cui sono originati, è necessario disporre di una serie di apparati, tra cui i *firewall*, che permettano di tenere traccia della navigazione Internet.
In seguito ad una valutazione fatta sugli apparati *firewall* oggi presenti sul mercato e dopo aver verificato l'efficacia e l'efficienza di contatti pre e soprattutto post-vendita con il supporto tecnico

dei vari *brand*, abbiamo ritenuto opportuno acquistare gli apparati della società Fortinet (modello Fortigate 220D).
Sono stati acquistati due Fortigate in modo da avere una struttura ridondante che garantisca continuità di interconnessione anche in caso di guasto di uno dei due apparati.

Implementazione misure AgID - Studio di fattibilità per le postazioni di tipo client.

Le richieste relative ai criteri di sicurezza sulle macchine client sono molte ed hanno livelli di difficoltà di implementazione differenti. Nel seguito ci soffermeremo sulla descrizione di quei punti che hanno richiesto un'analisi più approfondita per la valutazione delle possibili alternative.

ABSC 1: Inventario dei software Autorizzati
L'AgID non si limita a chiedere un inventario dei software ma di monitorare costantemente le macchine per assicurarsi che non sia installato software non autorizzato. Ovviamente una possibilità è quella che i tecnici controllino regolarmente una ad una tutte le macchine della Facoltà con evidente dispendio di tempo. Esistono diversi modi di automatizzare e centralizzare questa operazione.
Considerando che il parco macchine di Facoltà è eterogeneo e comprende sia macchine Windows (la maggioranza) che macchine OSX e Linux sono state valutate le seguenti alternative:

Gestion Libre De Parque Informatique (GLPI) + Fusion Inventory
GLPI rappresenta lo standard open source per la gestione di un inventario hardware/software. Fusion Inventory rappresenta una estensione di GLPI che permette il *software deployment* ovvero l'installazione e rimozione remota di software.
Pro: Open source, gratuito, supporta tutti i sistemi operativi.
Contro: Documentazione incompleta in lingua inglese, richiede conoscenze specifiche non in possesso dei tecnici Informatici di Facoltà, in caso di necessità, il supporto tecnico, dovrà essere richiesto a società esterne.
Nonostante le potenzialità, la scelta di questa tecnologia richiederebbe tempi di realizzazione troppo lunghi e non in linea con le direttive AgID. Ci proponiamo comunque di testare il sistema su un insieme di prova di macchine per adottarlo in un successivo momento qualora risultasse idoneo.

Software IBM BigFix
E' un software proprietario sviluppato da IBM per l'identificazione e la gestione remota dei nodi in una rete. Permette di configurare macchine ed installare/rimuovere software in maniera centralizzata.
Pro: funziona con tutti i maggiori sistemi operativi, messa in opera rapida, utilizzo di base semplice, non richiede particolari conoscenze, supporto incluso nel prezzo.
Contro: la licenza di ciascun client è a pagamento, non è stato possibile testarlo direttamente.
Il software IBM risulta la scelta più efficace per le necessità della Facoltà.

ABSC 3: Configurazione sicura delle macchine.
La configurazione sicura richiede l'attuazione di varie misure, dalla gestione degli utenti che utilizzano la macchina (tipologia di account, criteri per la password, gestione dei dispositivi mobili connessi) fino alla creazione di immagini offline per il ripristino delle macchine in tempi brevi. Ad eccezione della creazione di immagini, tali configurazioni possono essere implementate utilizzando i tool messi a disposizione del sistema operativo. Occorre tuttavia considerare il particolare utilizzo della macchina per poter definire delle configurazioni adeguate. Sono state evidenziate le seguenti tipologie:

- PC totem ad accesso pubblico nelle biblioteche
- PC ad accesso pubblico nei laboratori
- PC ad uso esclusivo del personale TAB/Docente

Un primo intervento consiste nel definire una configurazione sicura di base per ciascuna tipologia e la conseguente messa in opera della stessa dai parte dei tecnici (o dell'effettivo responsabile della macchina).

Un approccio più efficace potrebbe essere l'utilizzo di un software che gestisca in maniera centralizzata le configurazioni di tutte le macchine della rete, come il software IBM *BigFix* (descritto al punto precedente).

ABSC 4: Analisi e correzione delle Vulnerabilità
Lo standard open source è rappresentato dal software *openvas* che richiede l'installazione del software su una macchina ad hoc. Inoltre l'analisi delle vulnerabilità necessità la regolare scansione di tutte le macchine e la verifica da parte di personale tecnico competente del risultato della scansione. La correzione delle vulnerabilità necessita l'installazione sulle macchine delle relative correzioni (patch). Un sistema centralizzato per l'installazione di patch garantisce un minore onere di intervento.

ABSC 10: Copie di sicurezza.
E' possibile effettuare le copie di sicurezza installando su ciascuna macchina un software che effettui un backup regolare su un dispositivo rimovibile. Tuttavia questo approccio presenta molti inconvenienti e sarebbe preferibile centralizzare il processo di Backup. Tra le soluzioni valutate la migliore risulta essere quella che prevede l'utilizzo del software opensource e gratuito *UrBackup*. L'adozione di questa soluzione centralizzata prevede necessariamente l'acquisto dell'hardware necessario ovvero un server per il software di backup ed un sistema di dischi (NAS) per la memorizzazione dei dati.

Implementazione misure AgID - Studio di fattibilità per macchine server.

Lo studio di fattibilità per le macchine client ha evidenziato la necessità di sviluppare una serie di servizi centralizzati per l'implementazione delle MMS. I principali servizi che si vogliono implementare sono:

1. *Backup e Imaging* delle macchine client e server:
   Hardware: server di gestione del software (Centos 7.x), NAS (Network Attached Storage) di circa 80Tb
   Software: *UrBackup*
2. *Deploying:* distribuzione sui client di immagini di sistema operativo comprensivo di applicazioni, sottoposte preventivamente a valutazione di sicurezza ed aderenza agli standard secondo le specifiche AgID:
   Hardware: server di gestione del software (Centos 7.x)
   Software: *IBM BigFix educationa*l per ciascuna postazione.
3. *Inventario Hardware e software dei client e dei server*:
   Hardware: server di gestione del software (Centos 7.x)
   Software: IBM BigFix educational per ciascuna postazione.

4. ProgettoAgID@Economia (#NonAgIDiamoci)

Ricognizione hardware e software, controllo remoto
Obiettivo dell'intervento è realizzare sistemi automatici di monitoraggio, verifica e gestione dei dispositivi attraverso l'installazione di un servizio centralizzato che
permetta la supervisione delle macchine del personale non in grado di amministrare in modo autonomo la propria postazione. Utilizzando le tecnologie elencate nello studio di fattibilità, in un'unica soluzione saranno integrate tutte le funzioni per la gestione delle P.D.L.:

inventario HW/SW dinamico, Distribuzione SW, Controllo Remoto, Gestione delle Configurazioni, Patch/SP Management, Risparmio Energetico e strumenti per la manutenzione ordinaria.

I template di configurazione delle macchine desktop potranno essere facilmente standardizzati in base alle policy aziendali: wallpaper, shortcuts, stampanti, local security policies, accesso alle periferiche USB, migliorando la sicurezza e l'efficienza dei PC.
Sarà inoltre agevole verificare il software installato e misurarne la frequenza d'uso al fine di ottimizzare l'assegnazione delle licenze.

Messa in sicurezza della Rete di Facoltà

1. Piano di indirizzamento
E' stato modificato il piano di indirizzamento di ogni singola struttura presente all'interno della Facoltà, passando ad indirizzi IP privati ed eliminando quasi complessivamente tutti gli indirizzi IP pubblici presenti. Nei casi in cui è stato necessario mantenere verso l'esterno un determinato IP pubblico si è applicata una operazione di mappatura tra l'IP privato e l'IP pubblico (metodo NAT, Network Address Translation). Ad ogni struttura è stata quindi riservata una classe di IP privati, in modo da isolarla logicamente e gestirne le policy per le esigenze richieste.

2. Assegnazione dinamica degli indirizzi (DHCP, Dynamic Host Configuration Protocol)
L'assegnazione degli indirizzi di rete ai vari *device* fino ad oggi è stata gestita manualmente attraverso l'assegnazione di un indirizzo statico. Questa operazione oltre ad essere molto dispendiosa in termini di tempo non porta ad un controllo puntuale, veloce e centralizzato.
E' stata implementata, tramite un server DHCP installato sul firewall di Facoltà, l'assegnazione dinamica degli indirizzi a tutti i device collegati alla rete.
Questa scelta consente la gestione centralizzata di ogni singolo apparato e, parallelamente, di avere una lista sempre aggiornata che permetta di intervenire prontamente nel momento in cui dovesse presentarsi un problema di sicurezza. A tal fine, per ogni *device*, è stato effettuato il *reservation* dell'indirizzo IP che permette di identificare in maniera univoca il possessore della macchina che sta utilizzando quel determinato IP.
3. User authentication e Captive Portal
Grazie alla tecnologia presente nei nuovi apparati, è stato possibile realizzare un unico sistema di autenticazione che utilizza le credenziali di posta elettronica per il personale strutturato e quelle del sistema INFOSTUD per gli studenti.
Per quanto riguarda gli utenti occasionali (prof. visitatori etc.) è stata implementata una procedura che, attraverso la richiesta di un docente, validata dal referente informatico della struttura di afferenza, fornisce le credenziali di autenticazione per un tempo limitato (utilizzando il sistema LDAP interno).
Alla prima richiesta di accesso ad una destinazione web, i sistemi re-indirizzeranno l'utente ad una pagina *intranet* dove sarà necessario inserire le proprie credenziali di accesso.
Questa tecnologia permette di creare un ambiente di rete in cui ciascun utilizzatore dei servizi è identificato: gli utenti che non eseguono il login, o che inseriscono credenziali errate, non avranno accesso ad alcun servizio di rete, oppure ad un ristretto insieme di servizi definito dagli operatori IT.
Per garantire la sicurezza della rete tutti i visitatori saranno dirottati su una VLAN ospiti, appositamente creata, che consentirà la navigazione Internet ma impedirà loro di utilizzare i *device ed i servizi* messi a disposizione delle strutture e del personale (stampanti, servizi web interni, etc ...).
4. Network policies
Attraverso l'autenticazione è possibile identificare in maniera univoca l'utente connesso all'infrastruttura e grazie a questo è possibile applicare per ciascun tipo di utilizzatore delle regole di connessione personalizzate.
Possiamo quindi assegnare per ogni classe di utente differenti privilegi, quali ad esempio:

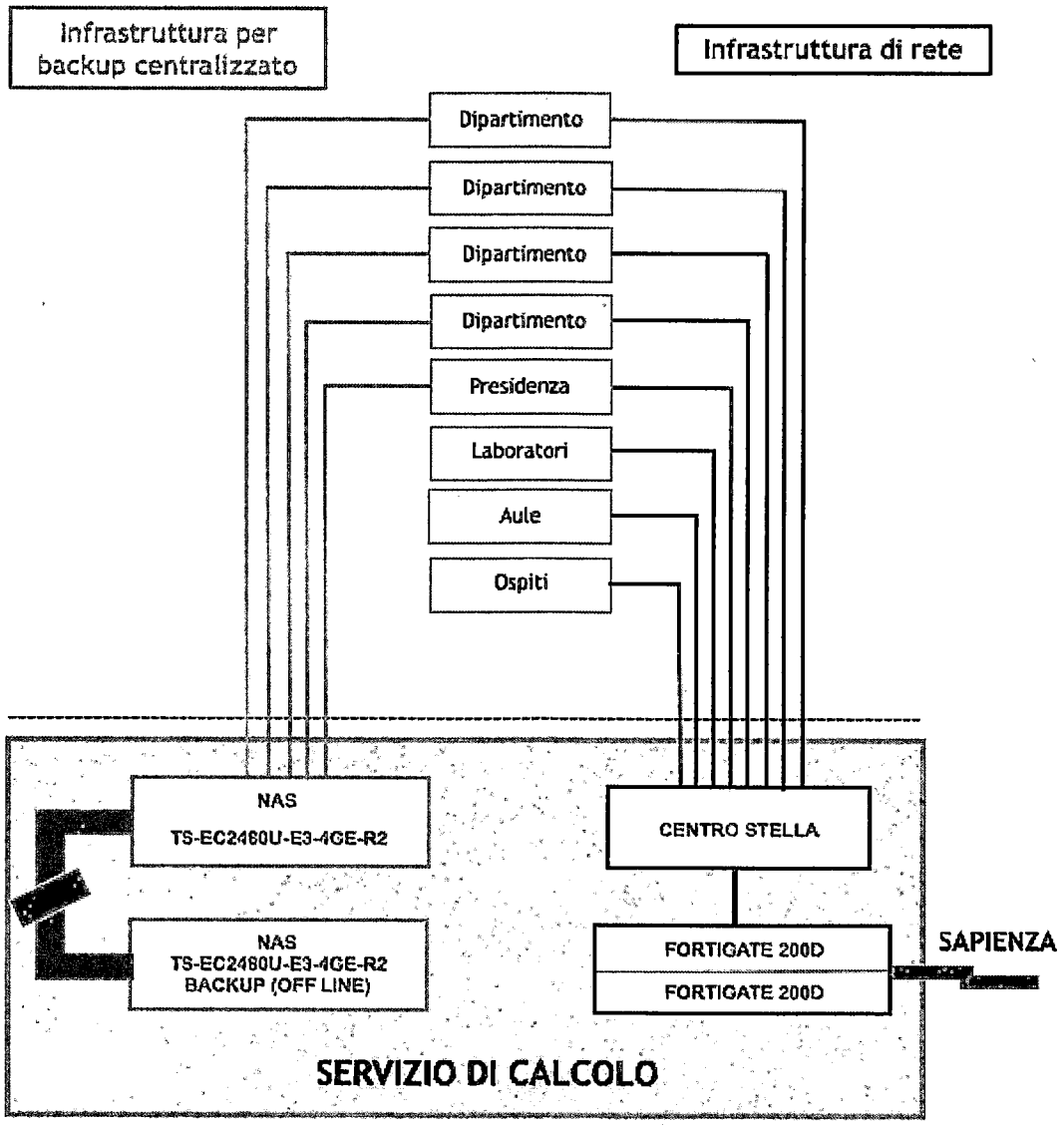
- Accesso ad internet
- Servizi abilitati (es. web, posta, vpn, p2p, etc...)
- Fasce orarie di validità dei privilegi

5. Log (registrazione) delle attività

Tutte le operazioni eseguite dai firewall sono storicizzate in un sistema di *log* estremamente dettagliato che viene poi copiato su supporti esterni per essere adeguatamente archiviato.

I *log*, oltre a fornire informazioni su eventi specifici, forniscono informazioni statistiche generali utili per comprendere l'utilizzo della rete permettendo così interventi specifici su eventuali anomalie riscontrate.

Schema tecnico del progetto di Rete



5. Gantt delle attività

	ATTIVITA'					
	gen-18	feb-18	mar-18	apr-18	mag-18	giu-18
Procedure amministrative						
Installazione						
Collaudo						

Il progetto è stato realizzato da:

Anna Mallamaci
Domenico D'Orazi
Enrico Mastrostefano
Luigi Basilici
Riccardo Sucapane
Stefano Sansone

Roma il 28.12.2017

Il Preside della Facoltà
Prof. Fabrizio D'Ascenzo