UNIVERSITÀ DEGLI STUDI DELL'INSUBRIA

Nome del documento	Endpoint e attrezzature individuali.docx
Redatto da	Dott. Luca Mondini
Revisionato da	Dott. Federico Raos
Data ultima revisione	26/03/2026 14:44:00
Numero di pagine	4

Endpoint e attrezzature individuali

Contesto e finalità

La gestione degli endpoint e delle attrezzature individuali rappresenta un ambito di investimento strategico per l'Ateneo, come documentato anche **nelle Relazioni PIAO degli ultimi tre anni**, che evidenziano una progressiva maturazione dei modelli di governo ICT, con particolare attenzione ai temi di sicurezza, affidabilità operativa e continuità del servizio.

Contenuti ed evidenze

Perimetro e dotazioni

Tutto il personale PTAB della amministrazione centrale a tempo determinato è dotato di **computer portatile istituzionale**, configurato secondo standard di sicurezza e gestione centralizzati.
Il modello adottato prevede:

- Cifratura sistematica del disco per tutti i dispositivi assegnati;
- Possibilità di cancellazione remota del dispositivo in caso di furto o smarrimento, con una significativa riduzione del rischio di data breach;
- Gestione unificata delle configurazioni di sistema e degli applicativi.

Le medesime piattaforme e criteri di gestione sono applicati anche ai:

- calcolatori dei laboratori didattici;
- calcolatori della didattica in aula (postazioni di cattedra).

Questo consente uniformità di configurazione, semplificazione della manutenzione e maggiore controllo complessivo del parco macchine.

Gestione centralizzata degli endpoint (Microsoft Intune)

La gestione degli endpoint è basata sull'utilizzo di Microsoft Intune, progressivamente esteso nel tempo:

- inizialmente adottato per i dispositivi dei laboratori informatici e per i calcolatori della didattica (i calcolatori presenti in ogni cattedra di Ateneo);

- successivamente esteso ai calcolatori del personale tecnico-amministrativo AC
- reso disponibile ai Dipartimenti su base volontaria, nel rispetto delle diverse sensibilità organizzative.

Alcuni Dipartimenti hanno scelto di conferire integralmente sotto Intune tutti i propri calcolatori, inclusi quelli dei docenti; altri hanno adottato il modello in modo parziale, in funzione delle specificità disciplinari o di esigenze particolari. Questo approccio flessibile ha favorito l'adesione progressiva, mantenendo al contempo standard di sicurezza elevati.

Sicurezza, aggiornamenti e riduzione della superficie di attacco

La funzione principale della piattaforma di gestione centralizzata riguarda:

- distribuzione e aggiornamento centralizzato dei sistemi operativi;
- gestione degli applicativi;
- applicazione di policy di sicurezza finalizzate alla riduzione della superficie di attacco (attack surface reduction).

Tali policy consentono di mitigare in modo sistematico i rischi legati a vulnerabilità note, configurazioni non conformi o software non aggiornato, contribuendo in modo sostanziale al miglioramento del profilo di sicurezza complessivo dell'infrastruttura endpoint.

Monitoraggio e prevenzione dei guasti

I dispositivi gestiti sono oggetto anche di monitoraggio continuo di metriche di performance, che permettono di:

- individuare degradi prestazionali;
- intercettare segnali precoci di possibile guasto hardware;
- pianificare interventi di manutenzione o sostituzione prima dell'interruzione del servizio.

Questo approccio proattivo riduce i tempi di fermo, migliora l'esperienza degli utenti e ottimizza l'impiego delle risorse ICT e contribuisce in modo diretto alla continuità delle attività didattiche e amministrative, riducendo i disservizi percepiti dagli utenti finali.

Gli indicatori sono utilizzati non solo a fini di controllo, ma anche per orientare le priorità di investimento e le politiche di rinnovo del parco macchine.

Processi e responsabilità

La gestione degli endpoint coinvolge:

- le strutture ICT centrali, responsabili della definizione degli standard, delle policy di sicurezza e della gestione della piattaforma;
- i Dipartimenti, che possono aderire al modello di gestione centralizzata secondo modalità concordate;
- il Service Desk, quale punto di contatto per il supporto operativo agli utenti.

Il coordinamento tra i diversi attori avviene attraverso processi strutturati di pianificazione, gestione operativa e miglioramento continuo, in coerenza con i sistemi di AQ dell'Ateneo.

Indicatori / monitoraggio

Tra gli indicatori e le modalità di monitoraggio adottate rientrano, a titolo esemplificativo:

- stato di conformità dei dispositivi alle policy definite;
- livello di aggiornamento dei sistemi operativi e degli applicativi;
- metriche di performance e affidabilità;
- numero e tipologia di interventi preventivi effettuati.

Tali indicatori sono utilizzati nel ciclo di miglioramento continuo per orientare le scelte tecnologiche e organizzative.

Evoluzioni e obiettivi di sviluppo (orizzonte 2026)

In continuità con gli investimenti già effettuati, l'Ateneo prevede per il 2026 un ulteriore rafforzamento della **gestione della sicurezza degli endpoint**, attraverso la progressiva introduzione di **strumenti avanzati e soluzioni basate su intelligenza artificiale** a supporto delle attività di prevenzione, rilevazione e risposta agli incidenti.

La piattaforma di gestione degli endpoint basata su **Microsoft Intune** è già **integrata nativamente con Microsoft Defender for Endpoint**, consentendo una gestione coordinata delle configurazioni di sicurezza, l'utilizzo dei segnali di rischio degli endpoint e il miglioramento complessivo della postura di sicurezza.

In un'ottica di **sicurezza integrata,** gli eventi e gli alert generati dagli endpoint possono essere correlati tramite **Microsoft Sentinel**, favorendo una visione unificata degli eventi di sicurezza e una maggiore capacità di individuare comportamenti anomali e **movimenti laterali**, che rappresentano una delle principali modalità di compromissione degli endpoint.

A partire dal **1° gennaio 2026**, il perimetro degli endpoint gestiti è stato inoltre esteso includendo anche dispositivi digitali a supporto della didattica e delle attività istituzionali, quali **DSP audio digitali Dante, microfoni radio e ambientali Dante, altoparlanti digitali**

Dante, telecamere con tracking automatic 4k e proiettori, gestiti tramite i rispettivi sistemi cloud di amministrazione.

Questa estensione consente una visione più completa e coerente dell'ecosistema tecnologico dell'Ateneo, in linea con un approccio evoluto alla gestione degli endpoint.

Riferimenti

- Relazioni PIAO (ultimi tre anni);
- policy di sicurezza ICT e linee guida operative