**CARATTERISTICHE DELL’INFRASTRUTTURA INFORMATICA AOUTS**

L’AOUTS è dotata di un dominio Active Directory (AD) 2008 R2 (aouts.it). In ciascuno dei due principali siti AD (Ospedale di Cattinara e Ospedale Maggiore) è presente almeno un domain controller global catalog.

Gli aggiornamenti di sistema per i client e per i server vengono distribuiti tramite il servizio Microsoft WSUS, su base mensile e appena rilasciati da Microsoft.

Le postazioni di lavoro AOUTS (PC) sono inserite nel dominio aouts.it. Esse sono dotate di sistema operativo Microsoft Windows XP Professional Italiano SP3 o Microsoft Windows 7 Professional Italiano e di browser Microsoft Internet Explorer 8 (nel seguito anche IE8); l’hardware di tali postazioni è eterogeneo e varia, nelle prestazioni e caratteristiche di base, da

* CPU Intel Pentium 4 2,4 GHz o equivalente
* memoria DDR-SDRAM 512 MB
* hard disk da 40 GB

a

* CPU Dual Core Intel Pentium G630 2,7 GHz o equivalente
* memoria DDR3 4 GB (in configurazione dual channel)
* hard disk 500 GB

Tutte le postazioni di lavoro AOUTS sono dotate di connettività di rete Fast Ethernet o Gigabit Ethernet (secondo quanto definito dagli standard IEEE 802.3). Tutti gli operatori aziendali accedono, nell’operatività quotidiana, alle postazioni di lavoro (PC) tramite account e relative credenziali personali con bassi privilegi; su tutte le postazioni è attivo il servizio Microsoft DEP (Data Execution Prevention).

Il protocollo di rete utilizzato è IPv4. La risoluzione dei nomi è basata esclusivamente sul servizio DNS (Domain Name Service), integrato in AD, che accetta solo registrazioni sicure. I server Microsoft aziendali appartengono a due subnet IP dedicate – una per ciascun sito AD – e sono virtualizzati tramite due sistemi VMware vSphere v5.x, uno installato presso l’Ospedale di Cattinara ed uno presso l’Ospedale Maggiore. L’architettura di rete AOUTS è realizzata in modo che tutti i servizi sono raggruppati nel data center (CED) AOUTS del sito di pertinenza; in particolare i server virtualizzati appartengono ad una VLAN dedicata.

In generale la LAN AOUTS è una rete layer 2-3 (pila ISO/OSI) a due livelli (core e periferia): per ciascun presidio, gli apparati di periferia sono collegati in layer 2 agli apparati di core; il data center è collegato direttamente agli apparati di core in layer 3. In tutta la LAN AOUTS il traffico è suddiviso in VLAN separate sulla base della tipologia di traffico dati e nell’intento di isolare il traffico dati stesso sulla base dei servizi. Il traffico dati tra gli apparati di periferia non è in generale consentito, in quanto i flussi funzionali sono sempre dal data center (CED) AOUTS alla periferia e viceversa. Gli host non inseriti nel dominio aouts.it sono suddivisi in un certo numero di VLAN/sottoreti IP, una per ciascuna classe di dispositivi; la disciplina del traffico tra queste VLAN/sottoreti ed il datacenter e la rete esterna avviene tramite opportune ACL (Access Control List) che consentono il solo traffico funzionale.

E’ attivo sulla LAN AOUTS un servizio DHCP (Dynamic Host Configuration Protocol) che in generale rilascia gli indirizzi IP a tutti gli host in rete ad esclusione dei server (per i quali sono previste specifiche configurazioni). Le postazioni AOUTS dotate del software DNA sono oggetto di opportune IP reservation.

Nel prossimo futuro sarà attivo sulla LAN AOUTS un sistema di autenticazione degli host di rete basato su protocollo IEEE 802.1x. L’autenticazione sarà basata, a seconda delle caratteristiche dell’host, su uno dei seguenti criteri (ordinati per livello di sicurezza e quindi per preferenza di implementazione):

* certificato macchina digitale erogato dalla certification authority (CA) AOUTS;
* account macchina Microsoft Active Directory, se non è possibile installare il certificato macchina sull’host;
* MAC address, solo se l’host non è dotato di client IEEE 802.1x.

L’infrastruttura PKI (public key infrastructure) in cui sarà inserita la CA AOUTS sarà basata su sistema Microsoft Windows Server 2008 R2 e strutturata su due livelli (“offline root CA” e “issuing CA”), rendendo disponibili le CRL (certificate revocation list) sia in Active Directory che tramite specifico sito intranet http. I certificati macchina rilasciati saranno basati su algoritmo SHA-256, di dimensione di 2 kB e di durata di 12 mesi; verranno inoltre distribuiti e rinnovati automaticamente ove possibile (client Microsoft) e manualmente negli altri casi. Quando il sistema di autenticazione su descritto sarà a regime, l’AOUTS avvierà l’implementazione di un sistema NAC (Network Access Control) di accesso alla rete, che sarà consentito solo agli host che rispetteranno un set di criteri minimi di sicurezza (a titolo di esempio non esaustivo, presenza del software antivirus, stato di aggiornamento del software antivirus, stato di aggiornamento delle patch di sistema, ecc.).

La struttura di backup AOUTS è basata su due tape library: una Sun Storage Tek SL500 posta nel data center dell’Ospedale di Cattinara ed una Sun Storage Tek SL48 posta nel data center dell’Ospedale Maggiore. Tramite il software Symantec Backup Exec 10d, le tape library effettuano – con periodicità variabile a seconda dei casi – le copie di sicurezza: dei sistemi operativi di tutti i server AOUTS, della configurazione dei DB AOUTS, dei dati (presenti sui NAS e sui file server), delle macchine virtuali, dei registri di log dei sistemi.

L’applicativo antivirus (AV) aziendale è l’ESET NOD32 v4.x distribuito su tutti i client e aggiornato automaticamente ogni tre ore.

Su tutti i client aziendali è presente l’agente Unicenter Remote Control v11.x, che consente l’accesso interattivo alle sessioni utente per fini di assistenza tecnica. E’ inoltre installato su tutti i client l’agente Altiris Asset Managentent v6.x per la gestione dell’inventario e per l’interfacciamento con il software di gestione del servizio di help desk (cosiddetta “gestione dei ticket”).

**SPECIFICHE IT RELATIVE ALL’OGGETTO DI FORNITURA**

I server forniti dovranno essere virtualizzati nel sistema AOUTS VMware vSphere v5.x del sito che verrà indicato dall’AOUTS (Cattinara o Maggiore) e seguirne le politiche di gestione, comprese quelle di indirizzamento IP, di backup e di disaster recovery. Potranno essere create una o più macchine virtuali a seconda delle necessità e dell’architettura proposte dall’aggiudicatario, ma in ogni caso tali macchine dovranno essere compatibili almeno con il sistema operativo Windows Server 2008 R2 Standard/Enterprise/Datacenter Edition ENG e inserite nel dominio aouts.it e conseguentemente nel sistema WSUS AOUTS. Tutte le licenze Windows Server necessarie al funzionamento del sistema, sono da intendersi a carico del fornitore e non saranno in alcun caso di tipo OEM, bensì licenze Retail intestate all’AOUTS e comunque in ogni caso compatibili con l’ambiente di virtualizzazione dell’AOUTS descritto precedentemente.

Allo scopo di uniformare i sistemi forniti agli standard AOUTS, compresi quelli di sicurezza, tali macchine server verranno inserite in una Organizational Unit (OU) generica dedicata ai server AOUTS oppure in una OU dedicata al fine di definire ed applicare su di esse specifiche Group Policy concordate con l’AOUTS; la default domain policy verrà applicata in ogni caso su tutte le OU.

Ai server verrà in ogni caso assegnata una opportuna classe di indirizzi IP fissi, che saranno oggetto di specifica configurazione sul servizio DHCP e concordati con l’AOUTS.

In base alla specifiche scelte progettuali e di infrastruttura, l’aggiudicatario dovrà usufruire della struttura di backup AOUTS per i sistemi operativi di tutti i server. Dovrà essere fornito all’AOUTS supporto per il loro inserimento nel sistema di backup dell’AOUTS, nonché per la redazione delle procedure di backup e disaster recovery.

Tutti gli eventuali applicativi client forniti, necessari all’espletamento di una o più funzionalità del sistema fornito, verranno installati sulle postazioni aziendali secondo le indicazioni di AOUTS e su proposta dell’aggiudicatario – senza limitazioni in termini di numero di postazioni e di numero di utenti connessi contemporaneamente – e dovranno essere adeguati alle caratteristiche software e hardware delle postazioni stesse, in particolare alle policy del dominio aouts.it e conseguentemente a quelle del sistema WSUS AOUTS. La distribuzione sulle postazioni di lavoro AOUTS di tali applicativi, nonché degli aggiornamenti, verrà eseguita per mezzo del sistema di software distribution di Microsoft AD, cioè tramite pacchetti MSI (Microsoft Installer), oppure con modalità alternative ma a carico dell’aggiudicatario, anche in caso di sostituzione delle postazioni AOUTS, per un numero illimitato di volte.

Tutti gli eventuali applicativi web forniti dovranno essere compatibili con il browser web IE8, attualmente installato sulle postazioni di lavoro AOUTS.

Tutte le funzionalità del sistema fornito dovranno essere garantite con il sistema di indirizzamento IP dinamico (DHCP) di cui le postazioni AOUTS sono parte.

Tutte le funzionalità del sistema fornito dovranno essere garantite con il client antivirus aziendale ESET NOD32 v4.x di cui ogni postazione AOUTS è dotata, in considerazione del fatto che verranno applicate le politiche di aggiornamento/scansione standard dell’AOUTS, a meno di eccezioni concordate con l’AOUTS.

Tutte le funzionalità del sistema fornito dovranno essere garantite con l’agente Unicenter Remote Control v11.x e con l’agente Altiris Asset Managentent v6.x di cui ogni postazione AOUTS è dotata.

In generale, sia lato server che lato client, se non diversamente comunicato dall’aggiudicatario, verranno installate tutte le patch rilasciate da Microsoft. Potranno essere segnalate all’AOUTS patch contrassegnate come “non applicabili”, solo se di natura non critica; per tali patch “non applicabili” verranno generate dall’AOUTS delle eccezioni in WSUS, che avranno una durata limitata di 6 mesi entro cui l’aggiudicatario dovrà provvedere alla risoluzione del problema di compatibilità.

I POCT forniti verranno collegati alla LAN AOUTS e inseriti in una specifica VLAN/sottorete. Su questa verranno configurate opportune ACL per consentire solo il traffico funzionale tra i POCT ed i server oggetto di fornitura e tra i POCT e la rete esterna per la sola assistenza remota. Per la redazione delle suddette ACL, l’aggiudicatario dovrà fornire tutta l’assistenza necessaria al raggiungimento degli obiettivi descritti.

Tutti gli elementi forniti non dovranno essere in alcun caso fuori supporto tecnico del fabbricante o a fine ciclo di vita (end-of-life) e comunque non dovranno trovarsi in tale stato ad un anno dal collaudo definitivo del sistema.

In ogni caso tutto quanto fornito dovrà essere coerente e compatibile con l’infrastruttura IT AOUTS descritta.

Per tutte le macchine appartenenti al dominio aouts.it, Unicenter Remote Control v11.x ed il programma integrato nei sistemi operativi Microsoft Windows (RDP) saranno gli unici strumenti consentiti per le attività di assistenza remota effettuate dal personale tecnico dell’aggiudicatario e da quelli dell’AOUTS. Per le macchine non appartenenti al dominio aouts.it, potranno essere utilizzati per le attività di assistenza remota effettuate dal personale tecnico dell’aggiudicatario altri strumenti purché segnalati puntualmente all’AOUTS. Tali attività potranno essere svolte per mezzo dei sistemi VPN Cisco aziendali e con credenziali personali di dominio rilasciate ad hoc, a seguito di presentazione di opportuna domanda rivolta all’AOUTS. In particolare per i server verranno rilasciate credenziali di amministratore e per i client AOUTS di user, se necessario.

In generale, tutti i software forniti dovranno essere:

* intuitivi e di facile utilizzo, ad ogni livello di accesso ed in ogni configurazione, per tutti gli operatori (a prescindere dal ruolo);
* dotati di labeling (GUI) in Italiano e tali che le impostazioni internazionali di Microsoft Windows (se presente) siano sempre IT standard (non sarà consentita alcuna modifica alle impostazioni di default IT sulle postazioni AOUTS), comprese le tastiere;
* stabili, in particolare che siano in grado di gestire le eccezioni;
* sicuri, sia dal punto di vista della sicurezza informatica che della qualità delle funzioni svolte;
* ottimizzati, in termini di rapporto tra uso delle risorse e prestazioni;
* sviluppati tenendo conto dei principi del “ciclo di vita del software” e dell’“analisi del rischio”, secondo le norme tecniche (o principi e metodologie almeno equivalenti) e le best practice internazionali; in ogni caso non dovranno utilizzare librerie deprecate e/o obsolete, né dovranno essere scritti e sviluppati con versioni del linguaggio di programmazione fuori supporto tecnico del fabbricante o a fine ciclo di vita (end-of-life) e comunque non dovranno trovarsi in tale stato ad un anno dal collaudo definitivo del sistema;
* pensati, progettati e realizzati nel rispetto del quadro legislativo vigente, nonché in modo da non mettere in alcun caso gli operatori in condizione di violare il quadro legislativo stesso nell’espletamento del normale utilizzo del sistema;
* installati e configurati per essere utilizzati, in condizioni di massima sicurezza e funzionalità, nello specifico contesto dell’AOUTS, così come descritto nel presente documento;
* manutenuti e gestiti in modo da conservare e mantenere stabili nel tempo tutte le caratteristiche possedute al momento del collaudo definitivo.

In particolare, tutti i software forniti che verranno installati o eseguiti su dispositivi collegati alla LAN AOUTS, dovranno essere eseguiti sempre:

* in un contesto user space per i client,
* come servizio per tutti i server,
* come servizio per i client se non è richiesta interazione con l’operatore,
* ed in ogni caso non dovranno essere modificati in alcun modo i permessi di default del file system e del registro di sistema Microsoft (ove presente).

In particolare, tutti i software forniti che verranno installati o eseguiti sulle postazioni di lavoro AOUTS, dovranno essere protetti da copia o distribuzione per mezzo di sistemi diversi da dispositivi hardware (a titolo di esempio non esaustivo, chiavi hardware USB).

In particolare, tutti i software forniti che verranno installati su sistema operativo Microsoft Windows Server 2008 o Microsoft Windows 7, dovranno essere compatibili con il sistema UAC (User Access Control).

In particolare, per quanto concerne le configurazioni:

* quelle degli applicativi server dovranno risiedere in database e comunque mai sui dischi locali dei PC client;
* quelle globali degli applicativi client (ovvero non riferite alle personalizzazioni dei singoli account) dovranno risiedere in un file xml (eXtensible Markup Language) nella cartella di installazione dell’applicativo (a cui quindi avranno accesso solo gli utenti con ruolo Amministratore) oppure nel registro di sistema (ove presente) nella sottochiave appositamente creata in fase di installazione in HKEY\_LOCAL\_MACHINE\SOFTWARE, ed in ogni caso informazioni critiche in termini di sicurezza e funzionalità (a titolo di esempio non esaustivo: le stringhe di connessione ai database, le credenziali necessarie per instaurare eventuali altre connessioni client/server, ecc.) dovranno essere cifrate almeno con algoritmo AES256;
* quelle personali degli applicativi client (ovvero riferite alle personalizzazioni dei singoli account) dovranno risiedere nel profilo dell’account a cui si riferiscono (ove presente).

Ovvero, in ogni caso non dovranno risiedere configurazioni globali degli applicativi client nei profili degli account, né altresì configurazioni personali degli applicativi client fuori dai profili degli account.

In particolare, i software forniti dovranno essere dotati di:

* un sistema di autenticazione informatica degli operatori per mezzo di account – e relative credenziali – personali;
* un sistema di autorizzazione degli account personali.

In via propedeutica al collaudo del sistema fornito, l’aggiudicatario dovrà installare la consolle amministrativa, che consente di gestire il sistema di autorizzazione, su un client AOUTS afferente alla SC Informatica e Telecomunicazioni o al Laboratorio e dovrà formare una risorsa AOUTS alla profilatura degli account nei sistemi forniti, in modo da rendere l’AOUTS autonoma nelle procedure di abilitazione e successiva re installazione della consolle amministrativa (se necessaria).

L’aggiudicatario dovrà individuare, all’interno della sua organizzazione, un “Responsabile per la privacy”. Questi verrà in tal senso nominato dal titolare del trattamento dei dati personali AOUTS e dovrà inviare, nel rispetto delle procedure AOUTS, le richieste di abilitazione degli incaricati e degli amministratori afferenti all’aggiudicatario (anche quelle necessarie per lo svolgimento delle attività di assistenza remota). I relativi account e le relative autorizzazioni verranno sempre erogate dall’AOUTS e a livello personale (tranne quelle relative all’account VPN Cisco che saranno aziendali), secondo le proprie procedure ed in ogni caso con i privilegi necessari e sufficienti allo svolgimento delle mansioni di competenza.

Per quanto concerne gli “account amministrativi” (ovvero ogni account a cui è associato un ruolo Amministratore o che è dotato di privilegi amministrativi o che consenta di svolgere funzioni di amministratore su qualunque macchina, sistema o applicativo fornito), questi:

* potranno, nel caso di account amministrativi locali di default (a titolo di esempio non esaustivo: “admin”, “administrator”, “root”, ecc.), essere impersonali e dovranno essere tutti comunicati all’AOUTS, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza; in ogni caso non dovranno essere configurati account amministrativi locali ulteriori rispetto a quelli di default;
* dovranno, nel caso di account amministrativi non locali che consentano l’accesso interattivo a macchine/sistemi/applicativi collegati alla LAN AOUTS, essere sempre personali e rispettare quanto riportato nel presente documento relativamente alle modalità di autenticazione (authentication) degli operatori per mezzo di account – e relative credenziali – personali;
* potranno, nel caso di account amministrativi di macchine/sistemi/applicativi non collegati alla LAN AOUTS, essere impersonali e dovranno essere tutti comunicati all’AOUTS, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza; in ogni caso non dovranno essere configurati account amministrativi in numero maggiore dello stretto necessario;
* potranno, nel caso di account digitali amministrativi, essere configurati dall’aggiudicatario solo in accordo con l’AOUTS e dovranno essere impersonali, dovranno essere tutti comunicati all’AOUTS, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza;
* non dovranno, nel caso di account amministrativi impersonali, essere in alcun caso presenti.

Per quanto concerne gli account impersonali, consentiti solo secondo quanto riportato nel presente documento, questi non dovranno in alcun caso permettere:

* di modificare le configurazioni, impostazioni e settaggi di macchine/sistemi/applicativi;
* di visualizzare, modificare o cancellare dati personali diversi da quelli eventualmente trattati contestualmente all’uso dell’account stesso.

Eventuali dati personali salvati in ulteriori archivi, diversi da quelli descritti nel presente documento, saranno ammessi solo con funzioni di “archivi provvisori”, ovvero di passaggio intermedio dei dati prima dell’invio agli archivi definitivi. I dati personali devono permanere negli archivi provvisori il minor tempo possibile, ovvero per un tempo massimo che sia configurabile e che in ogni caso non superi le 24 ore naturali, con l’implementazione di opportune procedure di cancellazione automatica che non consentano il recupero locale dei dati.

In ogni caso l’accesso agli archivi di dati personali (anche provvisori) dovrà avvenire solo da parte degli account personali e degli account digitali autorizzati, sulla base di opportuni permessi settati in modo che il livello dei privilegi di accesso sia il più basso possibile e preferibilmente che l’accesso ai dati avvenga sempre per tramite dell’applicativo e non direttamente da parte dell’account.

Non è consentita l’archiviazione, anche temporanea ed anche in forma anonima, dei dati su macchine situate esternamente rispetto alla rete dati dell’AOUTS.

Sono oggetto di fornitura i servizi di manutenzione ordinaria preventiva e ordinaria correttiva su tutte le forniture di ambito IT, comprensive di:

* esecuzione, con cadenza almeno semestrale, di tutte le operazioni necessarie a prevenire eventuali anomalie sull’hardware e sul software (comprese tutte le cosiddette “minor release”, che devono in ogni caso essere installate subito dopo il loro rilascio); in occasione di tali attività, l’aggiudicatario dovrà eseguire un backup (anche in assistenza remota) delle macchine oggetto di intervento, in modo da garantirne il ripristino in caso di problemi al riavvio;
* numero illimitato di interventi di manutenzione ordinaria correttiva su tutto quanto oggetto di fornitura (hardware e software); in caso di guasto bloccante, la presa in carico deve essere effettuata entro 1 ora lavorativa dalla chiamata, la risoluzione provvisoria entro 8 ore lavorative dalla chiamata (per esempio con cosiddetti “muletti” che consentano però tutte le funzionalità ordinarie) e la risoluzione definitiva entro 15 giorni lavorativi dalla chiamata; in caso di guasto non bloccante, la presa in carico deve essere effettuata entro 4 ore lavorative dalla chiamata, la risoluzione provvisoria entro 16 ore lavorative dalla chiamata (per esempio con cosiddetti “muletti” che consentano però tutte le funzionalità ordinarie) e la risoluzione definitiva entro 15 giorni lavorativi dalla chiamata; le chiamate verranno aperte telefonicamente, via fax o per email ai riferimenti che verranno comunicati all’AOUTS; i termini temporali indicati sopra si riferiscono ad una giornata lavorativa tipo almeno con orario dalle 8:00 alle 16:00 e dal lunedì al venerdì.

Il collaudo dell’intero sistema sarà condizionato alla redazione e sottoscrizione da parte del fornitore di un responsability agreement. Tale documento farà esplicito riferimento all’installazione AOUTS, nei modi e nei termini definiti dal presente capitolato e che verranno a presentarsi all’atto pratico dell’installazione e della manutenzione del sistema nel tempo. Il responsability agreement conterrà espliciti riferimenti al fatto che i requisiti funzionali e prestazionali non verranno inficiati nella particolare installazione AOUTS, così come intesa sopra.