SPECIFICHE IT ASUITS

Di seguito vengono definite le specifiche che i sistemi forniti dovranno rispettare relativamente ad aspetti della sfera dell'IT (Information Technology).
Il sistema nel suo complesso dovrà essere coerente con le politiche di sicurezza e di privacy dell'ASUITS e più in generale dovrà funzionare nel rispetto delle norme di buona tecnica, delle "best practice", dei regolamenti, delle norme tecniche e della legislazione vigente, in particolar modo in materia di sicurezza e privacy.
Il collaudo dell'intero sistema sarà condizionato alla redazione e sottoscrizione da parte del fornitore di un accordo di responsabilità (responsability agreement) redatto secondo i dettami della norma IEC 80001. Tale documento farà esplicito riferimento all'installazione ASUITS, nei modi e nei termini definiti dal presente documento e che verranno a presentarsi all'atto pratico dell'installazione e della manutenzione del sistema nel tempo. Il responsability agreement conterrà espliciti riferimenti alla "marcatura CE" dei sistemi offerti ed al fatto che i requisiti essenziali di sicurezza non verranno inficiati nella particolare installazione ASUITS, così come intesa sopra.

Specifiche di integrazione con l'infrastruttura IT

I sistemi oggetto di fornitura dovranno essere integrati ed interfacciati con l'infrastruttura informatica di rete e sistemistica dell'ASUITS, secondo quanto riportato nel seguito.
I dispositivi dotati di connettività di rete (host) che necessitano di collegamento alla rete dati per svolgere le funzioni richieste, potranno essere inseriti nella LAN ASUITS seguendo uno dei due scenari, mutuamente esclusivi, descritti nel seguito.

Scenario 1

Nel primo scenario, agli host oggetto di fornitura verrà assegnata una specifica classe di indirizzi IP statici coerente con il piano di indirizzamenti ASUITS. Tali dispositivi verranno inseriti in una VLAN dedicata, assegnata dall'ASUITS, dalla quale potranno effettuare solo il traffico necessario per svolgere le funzioni richieste e traffico relativo all'assistenza remota da parte del fornitore. La disciplina del traffico verrà garantita tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali, stilate per rete IP e per porta, sulla base delle sole effettive necessità di traffico. Il fornitore dovrà garantire piena collaborazione nella redazione di tali ACL e/o regole sui firewall, per una durata complessiva di almeno un giorno lavorativo uomo e comunque fino al raggiungimento del risultato atteso.

È attivo sulla LAN ASUITS un sistema di autenticazione degli host di rete basato su protocollo IEEE 802.1x e realizzato per mezzo di tecnologia Microsoft NPS. Tutti gli host forniti e collegati alla LAN ASUITS dovranno essere tali da consentire l'autenticazione di rete tramite MAC address (cosiddetta MAC authentication).

Per le eventuali attività di assistenza remota, effettuate nel corso della durata del contratto dal personale tecnico dell'aggiudicatario, la connettività agli host oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN aziendali ASUITS, a cui sarà dato accesso solo a seguito di domanda scritta rivolta all'ASUITS. La connessione VPN dovrà essere di tipo client-to-site ed effettuata per mezzo di credenziali personali; nel caso in cui l'aggiudicatario non fosse in condizione di garantire tale configurazione, sarà tenuto a redigere una relazione tecnica che giustifichi tale evenienza sulla base della quale l'ASUITS si riserverà di attivare connessioni di tipo site-to-site. Nel presente scenario, a

valle dell'instaurazione della connessione VPN, il collegamento ai singoli host oggetto di assistenza potrà avvenire con gli strumenti scelti dall'aggiudicatario, sempre e comunque con modalità rispondenti al quadro legislativo e normativo vigente, solo a valle di validazione degli strumenti stessi e della loro configurazione da parte dell'ASUITS.

Per quanto riguarda le eventuali attività di telemonitoraggio continuo degli strumenti e in generale degli host oggetto di fornitura, nel presente scenario, lo strumento messo a disposizione dall'ASUITS è il proxy di navigazione autenticata, gestito da Insiel e basato su tecnologia Blue Coat: gli host forniti dovranno essere tali da consentire la configurazione del proxy internet, tramite il quale, su specifiche porte di navigazione (80, 443, ecc.), potranno raggiungere specifici IP pubblici. Verranno effettuate specifiche eccezioni all'autenticazione basate su IP sorgente che consentiranno il traffico solo sulle porte necessarie e solo verso gli IP necessari. L'aggiudicatario dovrà fornire la massima collaborazione in tal senso all'ASUITS per la definizione delle suddette eccezioni.

Nel presente scenario l'aggiudicatario sarà responsabile in toto delle prescrizioni di ambito sicurezza informatica e privacy, secondo quanto previsto dal quadro legislativo e normativo vigente, nonché dal presente documento; in particolare per quanto riguarda le politiche: di autenticazione, autorizzazione e accounting (AAA), di backup e disaster recovery, sugli aggiornamenti di sicurezza di tutti i software installati sugli host oggetto di assistenza, di protezione antivirus e da altre tipologie di cyber attacco.

Scenario 2

Nel secondo scenario, in alternativa, l'aggiudicatario potrà integrare i sistemi oggetto di fornitura con l'infrastruttura sistemistica dell'ASUITS. Di seguito vengono riportate, in prima istanza, alcune caratteristiche peculiari dell'infrastruttura informatica dell'ASUITS; successivamente vengono definite le specifiche di interfacciamento all'infrastruttura ASUITS che i sistemi oggetto di fornitura dovranno avere in caso di adesione al presente scenario. L'architettura generale e le caratteristiche dei singoli elementi dei sistemi forniti dovranno in ogni caso essere pienamente coerenti e allineati con le logiche di seguito descritte.

L'ASUITS è dotata di un dominio Active Directory (AD) 2008 R2 (aouts.it), che presto verrà migrato alla versione 2012. In ciascuno dei due principali siti AD (Ospedale di Cattinara e Ospedale Maggiore) è presente almeno un domain controller global catalog ed un file server. Ogni account del directory service aziendale è associato ad almeno un gruppo di dominio (gruppi locali al dominio, domain local) corrispondente alla struttura amministrativa ASUITS di appartenenza.
La default domain policy impone l'utilizzo di password complesse di almeno 12 caratteri, con password history a 24 e cambio password obbligatorio ogni 90 giorni. 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 ASUITS (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 Core Due Duo 1,8 GHz o equivalente
- memoria RAM DDR2 1 GB
- hard disk da 250 GB

a

- CPU Intel Pentium G3420 3,2 GHz o equivalente
- memoria DDR3 4 GB
- 2 hard disk da 500 GB

Tutte le postazioni di lavoro ASUITS sono dotate di connettività di rete 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 ASUITS è realizzata in modo che tutti i servizi sono raggruppati nel datacenter (CED) ASUITS del sito di pertinenza; in particolare i server virtualizzati appartengono ad una VLAN dedicata.
In generale la LAN ASUITS 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. Il traffico è suddiviso in VLAN separate, a cui corrispondono specifiche sottoreti IP, sulla base della tipologia di host e del traffico dati che effettuano, ovvero nell'intento di isolare il traffico dati stesso sulla base dei servizi e dei domini di competenza degli amministratori degli host. Il traffico dati tra apparati di periferia appartenenti a differenti VLAN non è in generale consentito, in quanto i flussi funzionali sono sempre dal data center (CED) ASUITS alla periferia e viceversa.
È attivo sulla LAN ASUITS 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) e degli host con IP statico.
Come precedentemente riportato, è attivo sulla LAN ASUITS un sistema di autenticazione degli host di rete basato su protocollo IEEE 802.1x e su tecnologia Microsoft NPS. L'autenticazione è basata, a seconda delle caratteristiche dell'host, su uno dei seguenti criteri (ordinati per livello di sicurezza e quindi per preferenza di implementazione):

- account macchina Microsoft Active Directory, se l'host è dotato di client AD;
- nome utente e password, se l'host non è dotato di client AD ma è dotato di client IEEE 802.1x;
- MAC address, solo se l'host non è dotato di client IEEE 802.1x.

La struttura di backup ASUITS 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 ASUITS, della configurazione dei DB ASUITS, dei dati (presenti sui NAS e sui file server), delle macchine virtuali, dei registri di log dei sistemi.
In ciascuno dei due presidi ospedalieri (Cattinara e Maggiore) è presente un server Microsoft SQL 2008 R2 64 bit; tutti i database delle applicazioni aziendali basati su tale tecnologia vengono ivi istanziati. Tali server supportano solo l'autenticazione nativa (Native Mode o Windows Integrated) e l'istanza di default non viene utilizzata.
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 CA Unicenter Remote Control v11.x, che consente l'accesso interattivo alle sessioni utente per fini di assistenza tecnica.

Nel presente scenario, gli eventuali server forniti dovranno essere virtualizzati nel sistema ASUITS VMware vSphere v5.x del sito che verrà indicato dall'ASUITS (Cattinara o Maggiore) e seguirne le politiche di gestione, comprese quelle di indirizzamento IP, di aggiornamento, 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 ASUITS.
Tutte le licenze Windows Server necessarie al funzionamento del sistema, non sono da intendersi a carico del fornitore e non saranno in alcun caso di tipo OEM, bensì licenze Retail intestate all'ASUITS e comunque in ogni caso compatibili con l'ambiente di virtualizzazione dell'ASUITS descritto precedentemente.
Allo scopo di uniformare i sistemi forniti agli standard ASUITS, compresi quelli di sicurezza e autorizzazione (authorization), tali macchine server verranno inserite in una Organizational Unit (OU) generica dedicata ai server ASUITS oppure in una OU dedicata al fine di definire ed applicare su di esse specifiche Group Policy concordate con l'ASUITS; 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.
Nel presente scenario, i dati acquisiti e generati dal sistema e/o i loro riferimenti, nonché tutti quelli direttamente o indirettamente necessari al funzionamento degli applicativi forniti, dovranno essere organizzati in uno o più RDBMS, che potranno essere istanziati sui server Microsoft SQL ASUITS a discrezione dell'aggiudicatario; in tal caso dovranno seguirne le politiche di gestione, comprese quelle di backup e disaster recovery. In particolare potranno essere dedicati ai sistemi forniti una o più istanze oppure uno o più database in accordo con l'ASUITS.
In base alla specifiche scelte progettuali e di infrastruttura, l'aggiudicatario dovrà usufruire della struttura di backup ASUITS per i sistemi operativi di tutti i server e per la configurazione dei database. Dovrà essere fornito all'ASUITS supporto per il loro inserimento nel sistema di backup dell'ASUITS, nonché per la redazione delle procedure di backup e disaster recovery.

Nel presente scenario, lato utente, ovvero lato postazione ASUITS (PC client), gli applicativi eventualmente forniti potranno essere basati su tecnologia client/server o web.
Gli eventuali applicativi client forniti nell'ambito della presente fornitura, necessari all'espletamento di una o più funzionalità dei sistemi forniti, verranno installati sulle postazioni ASUITS – senza limitazioni in termini di numero di postazioni – 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 ASUITS. La distribuzione sulle postazioni di lavoro ASUITS di tali applicativi, nonché degli aggiornamenti, verrà eseguita per mezzo del sistema di software distribution di Microsoft AD, cioè tramite pacchetti MSI (Microsoft Installer), in alternativa l'installazione verrà effettuata – con analoghe caratteristiche qualitative e di risultato – da parte dell'aggiudicatario.
Gli eventuali applicativi web forniti nell'ambito della presente fornitura, dovranno essere compatibili con il browser web IE8, attualmente installato sulle postazioni ASUITS.
Eventuali PC oggetto di fornitura potranno essere inseriti nel dominio aouts.it a condizione di seguire le policy e caratteristiche dei PC ASUITS, così come descritte nel presente documento.

Nel presente scenario, tutte le funzionalità dei sistemi forniti dovranno essere garantite con il sistema di indirizzamento IP dinamico (DHCP) attivo sulle postazioni ASUITS. Nel caso in cui l'architettura e le caratteristiche tecniche dei sistemi forniti impedissero tale configurazione, l'aggiudicatario sarà tenuto a redigere una relazione tecnica che giustifichi tale evenienza e sulla base della quale l'ASUITS si riserva di create sul servizio DHCP opportune e specifiche configurazioni (reservation).
Nel presente scenario, tutte le funzionalità dei sistemi fornito dovranno essere garantite con il client antivirus aziendale ESET NOD32 v4.x di cui ogni postazione ASUITS è dotata, in considerazione del fatto che verranno applicate le politiche di aggiornamento/scansione standard dell'ASUITS, a meno di eccezioni concordate con l'ASUITS. Inoltre, tutte le funzionalità dei sistemi forniti dovranno essere garantite con l'agente CA Unicenter Remote Control v11.x di cui ogni postazione ASUITS è dotata.

Nel presente scenario, eventuali host (di tipologia non server) oggetto di fornitura che non siano dotati di client AD e che necessitano di connettività con la rete dati ASUITS, verranno connessi alla stessa con una specifica classe di indirizzi IP statici assegnata dall'ASUITS. Tali dispositivi verranno inseriti in una VLAN dedicata, assegnata dall'ASUITS, dalla quale potranno solo effettuare traffico specifico da e verso gli eventuali applicativi server forniti e installati nella virtualizzazione ASUITS e traffico relativo all'assistenza remota da parte del fornitore. La disciplina del traffico verrà garantita tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali, stilate per rete IP e per porta, sulla base delle sole effettive necessità di traffico. In ogni caso, gli host non dotati di client AD non avranno visibilità di rete sugli applicativi client/web installati sulle postazioni ASUITS. Il fornitore dovrà garantire piena collaborazione nella redazione di tali ACL e/o regole sul firewall, per una durata complessiva di almeno un giorno lavorativo uomo e comunque fino al raggiungimento del risultato atteso.

Nel presente scenario, 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'ASUITS patch contrassegnate come "non applicabili", solo se di natura non critica; per tali patch "non applicabili" verranno generate dall'ASUITS delle eccezioni in WSUS, che avranno una durata limitata di 6 mesi entro cui l'aggiudicatario dovrà provvedere alla risoluzione del problema di compatibilità.

Nel presente scenario, tutti i dispositivi forniti collegati alla LAN ASUITS dovranno autenticarsi in rete secondo il protocollo 802.1x, con uno dei tre criteri sopra esposti. In particolare:

- tutti i client tramite account macchina;
- tutti gli host non dotati di client AD, dovranno autenticarsi per mezzo di nome utente e password o di MAC address.

Per le eventuali attività di assistenza remota, effettuate nel corso della durata del contratto dal personale tecnico dell'aggiudicatario, la connettività agli host oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN aziendali ASUITS, a cui sarà dato accesso solo a seguito di domanda scritta rivolta all'ASUITS. La connessione VPN dovrà essere di tipo client-to-site ed effettuata per mezzo di credenziali personali; nel caso in cui l'aggiudicatario non fosse in condizione di garantire tale configurazione, sarà tenuto a redigere una relazione tecnica che giustifichi tale evenienza sulla base della quale l'ASUITS si riserverà di attivare connessioni di tipo site-to-site. Nel presente scenario, a valle dell'instaurazione della connessione VPN, il collegamento ai singoli host oggetto di assistenza: dovrà avvenire esclusivamente con gli strumenti aziendali ASUITS CA

Unicenter Remote Control v11.x e Microsoft Windows RDP, nel caso di host dotati di client AD; potrà avvenire con gli strumenti scelti dall'aggiudicatario, sempre e comunque con modalità rispondenti al quadro legislativo e normativo vigente, solo a valle di validazione degli strumenti stessi e della loro configurazione da parte dell'ASUITS, nel caso di host non dotati di client AD.

Per quanto riguarda le eventuali attività di telemonitoraggio continuo degli strumenti e in generale degli host oggetto di fornitura, nel presente scenario, lo strumento messo a disposizione dall'ASUITS è il proxy di navigazione autenticata, gestito da Insiel e basato su tecnologia Blue Coat: gli host forniti dovranno essere tali da consentire la configurazione del proxy internet, tramite il quale, su specifiche porte di navigazione (80, 443, ecc.), potranno raggiungere specifici IP pubblici.

È in uso presso l'ASUITS una soluzione di single sign-on (SSO) per l'autenticazione (authentication) ed il conseguente accesso alle risorse informatiche. Di seguito vengono riportate, in prima istanza, le caratteristiche peculiari del SSO ASUITS e successivamente vengono definite le specifiche dei sistemi da fornire in tal senso, nell'ambito del presente scenario.
Il SSO ASUITS permette al singolo account di autenticarsi una sola volta e di essere successivamente autenticato automaticamente – ovvero in maniera trasparente e senza dover reinserire le proprie credenziali – ogni volta che tenta di accedere ad una risorsa di rete di rete a cui è abilitato. Gli account possono essere associati sia a credenziali personali (ad uso esclusivo di una persona fisica, ovvero di un operatore) che impersonali (ad uso non esclusivo di una sola persona fisica, ovvero di un operatore), nonché account digitali (a titolo di esempio non esaustivo, un'applicazione che deve autenticarsi verso un'altra applicazione, un servizio, ecc.). Per risorsa di rete si intende un qualsiasi servizio erogato su qualsiasi sistema operativo (a titolo di esempio non esaustivo, l'accesso: ad un applicativo web o client/server, interattivo ssh, a file, a stampanti, ecc.).
La soluzione SSO ASUITS prevede un repository centrale realizzato attraverso il protocollo Lightweight Directory Access Protocol (LDAP), che contiene gli account e la configurazione delle macchine e dei servizi correlati; tale repository è il directory service aziendale Microsoft AD 2008 R2 (aouts.it) e non accetta bind anonimi. Per quanto riguarda l'autenticazione degli account, questa si basa sul protocollo kerberos versione 5 (in seguito anche v.5) e viene effettuata dal dominio aouts.it. Il SSO ASUITS ricalca quanto trova nome in letteratura come "Windows Integrated Single Sign-On" o "Windows Integrated Authentication". Le credenziali utilizzate sono ad oggi "nome utente" e "password", e seguono le politiche descritte precedentemente; in futuro verranno adottati sistemi basati su certificati digitali.
I sistemi forniti dovranno essere coerenti ed integrati con la soluzione di SSO ASUITS. Le modalità operative di accesso agli applicativi ed ai sistemi forniti da parte degli operatori dovranno essere personali, avverranno cioè per mezzo di credenziali informatiche personali; a queste potranno inoltre essere associati uno o più ruoli.
Come suddetto, l'unico repository di account ASUITS (personali e impersonali) è il directory service Active Directory e a ciascun account di dominio sono associate le rispettive credenziali informatiche. In tal senso tutte le credenziali personali, previste negli applicativi e nei sistemi forniti, dovranno essere quelle del dominio aouts.it; gli account associati a credenziali personali si autenticheranno in maniera automatica (e trasparente agli operatori) a tali applicativi/servizi, in base al proprio livello di autorizzazione (definito in base al ruolo) e a seguito dell'accesso alla sessione di lavoro. Tutte le credenziali impersonali, eventualmente presenti negli applicativi e nei sistemi forniti, dovranno essere opportunamente create e configurate nel dominio aouts.it; gli account AD associati a

credenziali impersonali si autenticheranno in maniera automatica (e trasparente agli operatori) a tali applicativi/servizi in base al proprio livello di autorizzazione minimo necessario e a seguito di auto log-on (in ogni caso senza l'immissione delle credenziali impersonali da parte degli operatori).
In ogni caso l'autenticazione degli account personali e impersonali dovrà avvenire tramite protocollo kerberos v.5. Ciò significa in particolare che, nell'architettura kerberos, i domain controller del dominio aouts.it svolgeranno il ruolo di KDC (Key Distribution Center), mentre gli applicativi/sistemi forniti assolveranno i ruoli di Client e SS (Service Server); a titolo di esempio non esaustivo, i Service Server forniti dovranno essere in grado di interpretare e validare correttamente i Service Ticket inviati dai Client, nonché instaurare successivamente le Client/Server Session (sia in caso di architetture fornite tipo client/server che web).
L'autorizzazione (authorization) è intesa in questo contesto come profilatura dell'account e gestione dei ruoli e delle abilitazioni ad esso associati. In particolare gli applicativi/servizi forniti dovranno importare gli account da abilitare dal repository LDAP ASUITS (dominio aouts.it), sulla base di un Gruppo AD specifico che verrà realizzato ad hoc, e circoscrivere la profilatura e l'attribuzione dei ruoli all'interno degli applicativi/servizi stessi solo per gli account appartenenti a quello specifico gruppo. In via propedeutica al collaudo dei sistemi forniti, l'aggiudicatario dovrà installare la consolle amministrativa su un client ASUITS afferente alla SC Informatica e Telecomunicazioni e dovrà formare una risorsa ASUITS alla profilatura degli account nei sistemi forniti, in modo da rendere l'ASUITS autonoma nelle procedure di abilitazione e successiva reinstallazione della consolle amministrativa.
Non dovrà essere possibile creare, configurare e profilare altri account non appartenenti ad AD, ad eccezione di specifiche situazioni opportunamente motivate ed in ogni caso concordate con l'ASUITS. La profilatura e l'attribuzione dei ruoli degli applicativi/servizi forniti dovrà essere tale da garantire il massimo livello di dettaglio di configurazione, ed in ogni caso dovrà garantire tutto quanto descritto nel presente documento.
Altre soluzioni di SSO, autenticazione e account/identity management non saranno consentiti.

Specifiche tecniche sicurezza informatica

Di seguito vengono definite le specifiche che i sistemi forniti dovranno rispettare, sia nello Scenario 1 che nello Scenario 2, relativamente ad aspetti generali della sfera dell'IT (Information Technology) con particolare riferimento alla sicurezza informatica (security).
Vale in ogni caso il principio generale per cui la sicurezza informatica è un fattore intrinseco dell'architettura dei sistemi oggetto della presente fornitura e delle caratteristiche tecniche degli elementi che li compongono; perciò l'aggiudicatario dovrà garantire che, sia l'architettura che gli elementi, siano progettati, implementati e manutenuti nel tempo in modo da minimizzare il rischio informatico residuo (sia di "attacchi ai sistemi" che di "attacchi dai sistemi").

Inoltre i sistemi forniti dovranno rispettare le seguenti prescrizioni.
In generale, 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 dei sistemi.
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, 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 dei sistemi;
- 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 dei sistemi;
- installati e configurati per essere utilizzati, in condizioni di massima sicurezza e funzionalità, nello specifico contesto dell’ASUITS, 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 su dispositivi collegati alla LAN ASUITS e inseriti nel dominio aouts.it, 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, 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 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, in tutti i software forniti che si configurano come “strumenti elettronici” che effettuano trattamento di dati personali, così come definito nel D.Lgs. 196/03 “Codice in materia di trattamento dei dati personali” e s.m.i., dovranno essere adottate:

- le “misure minime di sicurezza” previste dal suddetto codice e dal relativo disciplinare tecnico (Allegato B, D.Lgs. 196/03);
- le “idonee e preventive misure di sicurezza” previste dal medesimo codice all’art. 31 nell’ambito degli obblighi di sicurezza.

Dovranno essere rispettati tali obblighi in particolare in termini di:

- adozione di un “sistema di autenticazione informatica”, comunque nel rispetto di quanto riportato nel presente documento relativamente alle modalità di autenticazione (authentication) degli operatori per mezzo di account – e relative credenziali – personali;
- adozione di un “sistema di autorizzazione”, comunque nel rispetto di quanto riportato nel presente documento relativamente alle modalità di autorizzazione (authorization) degli account personali;
- “protezione degli strumenti elettronici e dei dati”, comunque nel rispetto di quanto riportato nel presente documento relativamente alla sicurezza informatica;
- “copie di sicurezza” e di “ripristino della disponibilità dei dati e dei sistemi”, comunque nel rispetto di quanto riportato nel presente documento relativamente alle politiche di backup e di disaster recovery.

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 ASUITS e dovrà inviare, nel rispetto delle procedure ASUITS, 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’ASUITS e a livello personale, 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’ASUITS, 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 ASUITS, 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 ASUITS, essere impersonali e dovranno essere tutti comunicati all’ASUITS, 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'ASUITS e dovranno essere impersonali, dovranno essere tutti comunicati all'ASUITS, 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'ASUITS, salvo esplicita autorizzazione da parte dell'ASUITS.