AOSP

La rete di trasporto dati e l'infrastruttura centrale

La rete informatica di AOSP è costituita da una rete capillare di distribuzione sia di tipo wired che di tipo wireless (in corso), caratterizzata da 2 centri stella di campus.

L'infrastruttura si sviluppa all'interno di un unico campus, connesso da un'unica lan, suddivisa in "aree"; un'area può corrispondere a un grosso padiglione o a un aggregato di alcuni padiglioni vicini più piccoli. L'architettura di rete è di tipo L3: ciascuna area ha una sua VLAN per i client, più altre VLAN per usi specifici (server decentrati, wifi, etc.); ogni VLAN è separata dalle altre e comprende sottoreti con indirizzi di classe B o C e default gateway distinti. Complessivamente sono presenti circa 23 aree e oltre 150 VLAN.
Gli apparati di rete sono di tipo Cisco e HP, con tecnologia di connessione switched-ethernet. Tutte le dorsali di rete dai centri stella agli armadi principali di area sono realizzate con collegamenti in fibra ottica ridondati a 1Gbps o 10Gbps; la distribuzione dall'armadio principale ai secondari di area è su collegamenti in fibra ottica ridondati a 1Gbps; l'utenza è servita da cavi a coppie UTP di cat.6 o cat.5e, secondo lo standard TIA/EIA 568, per la maggior parte collegati a switch con porte 10-100-1000.

La copertura wireless, realizzata secondo lo standard IEEE 802.1a/b/g/n/ac è in corso di implementazione e a breve sarà distribuita su tutto il campus, compresi i reparti sanitari. L'infrastruttura sarà di tipo centralizzato e governata da Wireless Control System (WLC) ridondato. L'autenticazione di rete è basata su una tecnologia EAP ovvero WPA2 e la crittografia dati è la AES, con certificato aziendale autofirmato lato server.

L'unico protocollo di rete ammesso è IP unicast.

Le connessioni verso Internet devono avvenire tramite proxy server aziendali, che gestiscono tutte le richieste di accesso a Internet con autenticazione NTLM.

Sistemi di firewall ridondati gestiscono i collegamenti dei client sia verso i server aziendali che verso le altre reti (Internet, Cup2000, Lepida, rete interaziendale, MAN AUSLBO, etc.).
In particolare, il collegamento tra AospBo e AuslBo è realizzato su infrastruttura Lepida Man in fibra ottica a doppia via a 1Gbps, con ulteriore ridondanza tramite collegamento su doppio Pal Lepida a 1Gbps.
Il collegamento verso i DataCenter regionali Lepida avvengono tramite PAL Lepida ridondato e in doppia via a 1Gbps. Il round trip time (RTT) su questo collegamento è tipicamente inferiore ai 10 ms e il packet loss è tipicamente inferiore a 1%.

L'infrastruttura server è distribuita su 2 siti: sala server presso Ospedale S.Orsola a Bologna e datacenter Lepida a Ravenna; in un prossimo futuro il datacenter Lepida a Parma si aggiungerà come ulteriore sito. L'instrastruttura tipicamente è realizzata sulla piattaforma di virtualizzazione VmWare su server blade; le database machine con particolari necessità di performance sono installate direttamente su blade fisici dedicati; i datastore VmWare e le LUN dei database sono tipicamente collegati in fiber channel o NFS. È in corso un progetto per la migrazione dei database principali su appliance Oracle Exadata con versione di Oracle 12 presente nel datacenter di Ravenna. Tipicamente gli applicativi web sono presentati ai client attraverso l'utilizzo di bilanciatori per suddivisione del carico e disponibilità del servizio.

L'autenticazione per le principali applicazioni web è implementata attraverso l'utilizzo del sistema Shibboleth che implementa il protocollo SAML2.0.

15/05/201715/05/2017La gestione delle abilitazioni e della profilazione degli utenti delle principali applicazioni è implementata attraverso l'integrazione di tali applicazioni con il software ACM gestito presso il servizio Tecnologie Informatiche.

La server farm è organizzata in zone di firewall e il traffico tra esse è soggetto a policy.

Tutte le macchine e i servizi sono monitorati via SNMP attraverso la piattaforma open source Sanet.

Si forniscono di seguito altri parametri utili per una valutazione complessiva delle attrezzature in uso:

1. Sistema operativo client: principalmente Windows in tutte le versioni (prevalentemente Windows10, Windows7 e XP, con residui 2000) e Mac (principalmente tra i PC universitari).
2. Numero di personal computer attivi: circa 3000 aziendali e circa 800 universitari.
3. I PC sono normalmente parte di un dominio Active Directory; gli utenti che vi accedono sono nello stesso dominio o in un dominio universitario in trust.
4. Browser in uso: ad oggi principalmente Internet Explorer v. 11, Internet Explorer v.8.0 e Mozilla Firefox v. 41.0.
5. Gli utenti non hanno diritti amministrativi o di power user sui PC in uso.
6. Sono inoltre in uso (in aumento) dispositivi mobile dotati di connessione wi-fi quali smartphone, tablet, ecc.
7. Applicativi standard presenti sulle postazioni client: Kaspersky Endpoint Security (con funzioni di antivirus, antispyware, webcontrol, mail control, firewall), UltraVNC, Adobe Acrobat Reader, Microsoft Office 2003 o superiori, Libre Office.

Non è consentito, se non su esplicita autorizzazione del servizio Tecnologie Informatiche e del servizio di Ingegneria Clinica e Informatica Medica, l'inserimento di alcun dispositivo di rete estraneo alla infrastruttura di rete aziendale.

Requisiti di base per la gestione dell'autenticazione e dell'abilitazione

L'autenticazione degli utenti aziendali ai software applicativi avviene tramite il sistema aziendale **openLdap.** Le utenze in uso hanno una *naming* standard del tipo "SOnnnnn" o "SPnnnnn".

Per le procedure in ambiente web, è stato implementato il Single Sign On mediante il prodotto open source **Shibboleth**, integrato all'openLdap aziendale.

Nelle procedure non web l'autenticazione viene gestita dalla procedura, che richiede le credenziali all'utente e le verifica collegandosi direttamente (via ldaps) all'LDAP.

L'autenticazione LDAP viene inoltre utilizzata in caso di procedure web che abbiano esigenze particolari quali ad esempio quella di effettuare un cambio rapido di utente senza uscire dalle maschere applicative.

Abilitazioni e Integrazione con sistema di gestione abilitazioni utente

La gestione dei profili di abilitazione è realizzata all'interno delle singole procedure; gli LDAP aziendali non sono utilizzabili ai fini della profilazione e delle abilitazioni.

Le procedure sono integrate con il sistema aziendale di gestione delle abilitazioni utente (ACM) secondo le specifiche che seguono.

1. La gestione delle abilitazioni e profilazioni degli utenti deve essere integrata con il sistema ACM di Aosp mediante realizzazione di **web service** per:

a) assegnare o rimuovere un profilo di abilitazione (es. reparti di competenza, funzioni) ad un utente (già presente o nuovo)

b) disattivare/riattivare un utente senza però togliere le profilazioni (metterlo offline/online)

c) clonare la profilazione di un utente su un altro

d) riassociare tutti gli utenti di un reparto ad un nuovo reparto (per chiusure/aperture reparti)

e) fornire gli elenchi, aggiornati in tempo reale, delle abilitazioni e dei profili attivi, compresi i superutenti (utenti con abilitazioni estese)

I web service utilizzano il protocollo SOAP o API REST su HTTPS; se esposti su Internet i web service sono configurati in un virtual host dedicato, raggiungibile solo da determinati indirizzi IP Aosp.

Le specifiche tecniche relative alle informazioni rese disponibili o scambiate via web service vanno definite nel dettaglio con i referenti aziendali del sistema ACM.

IOR

Contesto tecnologico e situazione attuale

Rete di telecomunicazione

La rete informatica dell'Istituto Ortopedico Rizzoli è costituita da una rete capillare di distribuzione sia di tipo wired che di tipo wireless, caratterizzata da un centro stella di piano a servizio del blocco operatorio al primo piano, 2 centri stella di campus ed un nodo di disaster recovery (nodo DR) sia per la parte rete dati e fonia che per la parte server infrastrutturali. La parte wired a servizio della periferia utente è realizzata con cavi a coppie UTP di cat.6 o cat.5e, secondo lo standard TIA/EIA 568 mentre i collegamenti di dorsale periferica, dei centri stella ed il collegamento tra ciascuna sala del blocco operatorio ed il relativo centro di piano sono realizzati in fibra ottica, sia di tipo multi che single mode. La rete è realizzata completamente in tecnologia switched ethernet, servita anche da dispositivi PoE+ e gli apparati sono del produttore HP. La connettività di dorsale dai rack periferici verso i due centri stella e il DR è ridondata in fibra ottica single mode a 1Gbps; la connettività tra ciascuna delle dieci sale operatorie del blocco operatorio e il relativo centro di piano è ridondata in fibra ottica multi mode a 1Gbps; la connettività di dorsale di campus tra i due centri stella e il nodo DR è ridondata in fibra ottica single mode a 10 Gbps; la connettività verso i client è a 100 Mpbs o 1 Gbps in rame, a 1 Gbps o 10 Gbps in rame o in fibra verso i server e storage nelle server farm locali; la connettività geografica verso il data center di Lepida SpA a Ravenna è ridondata in fibra ottica single mode a 1 Gpbs con latenza media pari a 5 ms.
L'unico protocollo di rete ammesso è il TCP/IP. L'architettura di rete è di tipo L3 e ogni rack periferico prevede una sottorete (subnet) separata e distinta dalle altre con indirizzi di classe A o di classe B definiti nella RFC 1918 e default gateway distinti. Gli indirizzi IP sono assegnati dinamicamente tramite il servizio DHCP alle postazioni di lavoro fisse e mobili e gli host sulla rete sono tutti registrati nel dns interno aziendale. Le connessioni

verso l'esterno/Internet sono su rete geografica di Lepida attraverso il Cesia/Garr e avvengono tramite proxy server e firewall perimetrali con autenticazione mediante il server LDAP aziendale; viene inoltre gestito il dns esterno per i domini registrati in ior.it
La copertura wireless è realizzata secondo lo standard IEEE 802.1a/b/g/n ed è distribuita su tutti i reparti sanitari e alcune zone dei laboratori di Ricerca e dell'area Generale e Amministrativa. L'infrastruttura wifi è di tipo centralizzato, governata da due wireless lan controller (WLC) in HA e access point di tipo PoE del produttore HP. I protocolli di sicurezza e l'autenticazione della rete wireless sono basati su WPA2, PEAP, EAP/TLS e la crittografia dati AES, con certificato SSL self signed di IOR. L'Ente intende rinnovare l'infrastruttura di rete wireless nel corso del 2018-2019 con ampliamento della copertura.
Sulla rete informatica sono installati anche altri impianti tecnici quali: IP PBX, telefoni SIP, impianto cercapersone, telecamere, totem per le prenotazioni, riscuotitrici, sonde e allarmi.
Non è consentito, se non su esplicita autorizzazione del servizio ICT interno, l'inserimento di alcun dispositivo di rete estraneo alla infrastruttura di rete aziendale, come dal Regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli.
L'Istituto ha una sede geografica, il Dipartimento Rizzoli Sicilia (DRS), ubicata presso la struttura di Villa Santa Teresa a Bagheria. La sede DRS è collegata con una linea dati MPLS tipo Intranet di Telecom a 10 Mbps, attestata a Bologna sul punto di accesso alla rete Lepida dell'Istituto. La connettività della sede DRS con il data center di Lepida a Ravenna è assicurata attraverso la linea dati MPLS di Telecom e attraverso la rete geografica di Lepida utilizzata dall'Istituto. La rete LAN wired e wireless del DRS, messa a disposizione dell'Istituto, è di proprietà ed in gestione della struttura di Villa Santa Teresa.

Datacenter e infrastruttura hardware dei sistemi

I sistemi dell'Ente sono ospitati in due server farm aziendali locali e in housing nel data center di Lepida SpA a Ravenna. Le due server farm locali sonoSi forniscono di seguito altri parametri utili per una valutazione complessiva delle attrezzature in uso:

8. Sistema operativo client: principalmente Windows in tutte le versioni (prevalentemente Windows10, Windows7 e XP, con residui 2000) e Mac (principalmente tra i PC universitari).
9. Numero di personal computer attivi: circa 3000 aziendali e circa 800 universitari.
10. I PC sono normalmente parte di un dominio Active Directory; gli utenti che vi accedono sono nello stesso dominio o in un dominio universitario in trust.
11. Browser in uso: ad oggi principalmente Internet Explorer v. 11, Internet Explorer v.8.0 e Mozilla Firefox v. 41.0.
12. Gli utenti non hanno diritti amministrativi o di power user sui PC in uso.
13. Sono inoltre in uso (in aumento) dispositivi mobile dotati di connessione wi-fi quali smartphone, tablet, ecc.

Applicativi standard presenti sulle postazioni client: Kaspersky Endpoint Security (con funzioni di antivirus, antispyware, webcontrol, mail control, firewall), UltraVNC, Adobe Acrobat Reader, Microsoft Office 2003 o superiori, Libre Office. poste rispettivamente nella palazzina ICT e nel nodo DR e ospitano alcuni server critici ridondati in HA, come ad esempio: l'IP PBX, il PACS, i server infrastrutturali della rete (dhcp, dns, ldap, radius, firewall etc). I server sono ospitati su due nodi VMware 5.5 in HA e sue due nodi Proxmox VE in HA.
Tutti gli altri sistemi e in particolare quelli di area sanitaria, come ad esempio i server dei DB Oracle e SQL, gli application server, il mail server e altri server per l'esecuzione di applicativi e sistemi dell'area della ricerca ed amministrativa, sono ospitati in housing nel data center di Lepida a Ravenna, su di una infrastruttura a due nodi VMware 6.0 in HA.

I server hanno in maggioranza sistema operativo Linux/Oracle linux, sono presenti VM con sistema operativo Windows Server.
Presso il data center di Lepida sono disponibili soluzioni in hosting ad alta affidabilità su macchine virtuali VMware 6.x, su host fisici e su piattaforma exadata per Oracle.
Il sistema di storage a due nodi in HA è basato sul software datacore SANsymphony. Il sistema di backup principale è installato su hardware (server e storage) in hosting nel data center di Lepida ed è basato sul software Simpana di Commvault; un secondo sistema Simpana per la copia secondaria del backup è nella server farm locale nella palazzina ICT, in una sede diversa rispetto al data center Lepida.

Postazioni di lavoro

La postazione di lavoro aziendale standard (PDL) viene installata da immagine con sistema operativo Windows 7 o Windows 10. Gli applicativi normalmente installati sulle PDL sono: Libre Office v. 5 o superiore, Antivirus Kaspersky, Adobe Acrobat Reader, WinZip/7Zip, Java versione 1.6 o superiore, browser Firefox/Chrome/IE 11. Sono ancora presenti alcune postazioni con sistema Windows XP, in via di sostituzione. MSOffice è installato esclusivamente in postazioni dedicate ad attività specifiche. Le nuove postazioni di lavoro fisse e mobili saranno acquisite tramite le convenzioni Consip e/o presso altri soggetti aggregatori.

AUSL

Contesto tecnologico e situazione attuale

RETE DATI E INFRASTRUTTURA

La rete informatica dell'AUSL Bologna è costituita da una rete capillare di distribuzione sia di tipo wired che di tipo wireless.

Le diverse sedi, geograficamente distribuite sul territorio della provincia, principalmente si articolano in:

9 ospedali (Maggiore, Bentivoglio, Bellaria, San Giovanni in Persiceto, Porretta Terme, Bazzano, Loiano, Budrio, Vergato), dei quali i primi 4 divisi in campus

36 poliambulatori (Anzola dell'Emilia, Baricella, Castel Maggiore, Castenaso, Castiglione dei Pepoli, Granarolo del'Emilia, Lizzano in Belvedere, Marzabotto, Molinella, Monghidoro, Monte San Pietro, Pianoro, Sala Bolognese, San Benedetto Val di Sambro, San Giorgio di Piano, San Giovanni in Persiceto, San Lazzaro di Savena, Sant'Agata Bolognese, Vergato, Byron, Carpaccio, Altedo, San Matteo della Decima, Vado, Lame, Montessori, Mazzacorati, Mengoli, Montebello, Pilastro, Porretta Terme, Reno, Saragozza, Tiarini, Zanolini)

14 case della salute (Budrio, Casalecchio di Reno, Loiano, Ozzano Emilia, Pieve di Cento, Sasso Marconi, Vergato, Borgo Reno, Crespellano, Terre d'acqua Barberini, Lavino

Samoggia, Navile, San Pietro in Casale e Galliera, San Donato).
3 sedi amministrative (Castiglione, Gramsci, S.Isaia)

Le sedi sono tra di loro interconnesse tramite diversi collegamenti: fibra ottica Lepida, GBE fibra ottica Telecom, MPLS rame telecom, ponti radio Lepida; il cablaggio strutturato nelle sedi utilizza cavi UTP di categoria 5E e 6, antifiamma ed a bassa emissione di fumi (LS0H); le dorsali in fibra ottica sono costituite da due cavi ottici di tipo diverso: uno ha capacità di 12 fibre ottiche tipo multimodale 62.5/125 µm e l'altro di 12 fibre ottiche di tipo monomodale 9/125 µm, ognuna dotata di rivestimento primario e secondario.

La rete è realizzata completamente in tecnologia switched ethernet, servita anche da dispositivi PoE+ e gli apparati sono dei produttori HP e Cisco; la connettività verso i client è a 100 Mpbs o 1 Gbps, a 1 Gbps verso i server e storage nelle server farm locali; la connettività geografica verso il data center di Lepida SpA a Ravenna è ridondata in fibra ottica single mode a 1 Gpbs con latenza media pari a 5 ms.

L'unico protocollo di rete ammesso è il TCP/IPv4, principalmente la comunicazione è di tipo unicast ma esistono isolate implementazioni di multicast per usi specifici.

L'architettura di rete è di tipo L2 e ogni sede periferica e blocco/piano prevede una sottorete (subnet) separata e distinta dalle altre e default gateway distinto. Gli indirizzi IP sono assegnati dinamicamente tramite il servizio DHCP alle postazioni di lavoro fisse e mobili e gli host sulla rete sono tutti registrati nel dns interno aziendale. Le connessioni verso l'esterno/Internet sono su rete geografica Lepida e Telecom e avvengono tramite proxy server e firewall perimetrali con autenticazione mediante i server LDAP aziendali; sono presenti inoltre diversi firewall periferici realizzati tramite appliance Fortigate, micro-computer Raspberry PI e routerboard Mikrotik per l'isolamente delle reti dedicate a MMG e apparati medicali.

Sempre sui server LDAP aziendali, opportunamente ridondati, insistono l'autenticazione tramite Radius sugli apparati di rete, l'accesso ai server, ai sistemi VPN (in fase di transizione da appliance Juniper a OpenVPN) e l'accesso alla rete wireless dedicata ai client.

La copertura wireless è realizzata secondo lo standard IEEE 802.1a/b/g/n ed è distribuita su tutti i reparti sanitari e alcune zone dei laboratori di Ricerca e dell'area Generale e Amministrativa. L'infrastruttura wifi è di tipo centralizzato, governata da 8 wireless lan controller (WLC) in HA e access point di tipo PoE del produttore Cisco.

I protocolli di sicurezza e l'autenticazione della rete wireless per i client sono basati su WPA2, PEAP, EAP/TLS e la crittografia dati AES; sono configurati poi diversi SSID, propagati sugli AP tramite l'uso di opportuni gruppi, per la copertura di diversi casi d'uso:

- reti universitarie con autenticazione inoltrata verso server Cesia
- reti guest a gestione interna, in fase di transizione verso la rete EmiliaRomagnaWifi gestita da Lepida

- reti fonia per apparati Voip
- reti tablet con accesso tramite certificato univoco
- reti per dispositivi datalogger in uso all'Ingegneria Clinica

Tutte le apparecchiature di rete ed i server che offrono servizi di infrastruttura sono monitorati via SNMP attraverso la piattaforma open source Sanet.

GESTIONE DI AUTENTICAZIONE E ABILITAZIONE

L'autenticazione degli utenti aziendali ai software applicativi avviene tramite il sistema aziendale openLdap. Le utenze in uso hanno una naming standard del tipo "n.cognome".

Per alcune procedure in ambiente web, è stato implementato il Single Sign On mediante il prodotto open source Shibboleth, integrato all'openLdap aziendale.

Nelle restanti procedure l'autenticazione viene gestita dalla procedura, che richiede le credenziali all'utente e le verifica collegandosi direttamente (via ldaps) alla directory.

L'interfaccia di gestione della directory OpenLDAP aziendale è di tipo web-based, l'inserimento/modifica/cancellazione degli attributi utenti e delle utenze stesse è profillata su diverse tipologie di accesso e privilegio che vengono demandate al personale interessato all'attività nei diversi settori.

Le azioni compiute dai suddetti operatori vengono notificate all'utenza finale via SMS/email.

Il tutto è integrato con il sitema di gestione del personale GRU per le dovute disabilitaizoni per fine rapporto previste dalla vigente normativa.

Per tutte le utenze "terze" ovvero per quelle non non comprese nelle banche dati della procedura del personale (GRU), viene definita una persona "referente di gruppo", tipicamente rappresentante dell'azienda esterna di riferimento, la quale sistematicamente a cadenze programmate, vene notificata dello stato delle utenze da lei gestite.

Datacenter e infrastruttura hardware dei sistemi

I sistemi dell'Ente sono ospitati in due server farm aziendali locali e in housing nel data center di Lepida SpA a Ravenna e nel datacenter di Acantho Spa a Imola. Le due server farm locali sono poste rispettivamente nella palazzina Corpo D presso l'Ospedale Maggiore e nella palazzina Padiglione B dell'Ospedale Bellaria, che ospita alcuni nodi DR e alcuni server critici ridondati. I server sono ospitati su due 5 nodi VMware 6.0 in HA e sue 4 nodi Proxmox VE in HA.
Tutti gli altri sistemi e in particolare quelli di area sanitaria, come ad esempio i server dei DB Oracle e SQL, gli application server, il mail server e altri server per l'esecuzione di applicativi e sistemi dell'area della ricerca ed amministrativa, sono ospitati in housing nel data center di Lepida a Ravenna e nel data center di Acantho, su di una infrastruttura a due nodi VMware 6.0 in HA per quanto riguarda gli application server e su server fisici per quanto riguarda i database Oracle.
I server hanno in maggioranza sistema operativo Linux/Oracle linux, sono presenti VM con sistema operativo Windows Server.
Presso il data center di Lepida sono disponibili soluzioni in hosting ad alta affidabilità su macchine virtuali VMware 6.x, su host fisici e su piattaforma exadata per Oracle.
Il sistema di storage a due nodi in HA è basato sul hardware IBM (V7000) e su hardware Huawei. Il sistema di backup principale è installato su hardware (server e storage) in hosting nel data center di Lepida ed è basato sul software Simpana di Commvault; un secondo sistema Simpana per la copia secondaria del backup è nella server farm locale nella palazzina ICT, in una sede diversa rispetto al data center Lepida.

Postazioni di lavoro

La postazione di lavoro aziendale standard (PDL) viene installata da immagine.
Di seguito si riportano le principali informazioni su numerosità e configurazione delle PDL:

- Sistema operativo client: principalmente Windows in tutte le versioni (prevalentemente Windows10, Windows7 e XP, con residui 2000) e Mac (principalmente tra i PC universitari).
- Numero di personal computer attivi: circa 6000 aziendali e circa 200 universitari.
- Gli utenti non hanno diritti amministrativi ma di power user sui PC in uso in migrazione verso diritti di user.
- Applicativi standard presenti sulle postazioni client: UltraVNC, Adobe Acrobat Reader, Microsoft Office 2003 o superiori, Libre Office.

Gli applicativi di base installati sono:

#	**Applicativi di base**	**Note**
AB1	Kaspersky antivirus	10.2.6.3733 - 10.3.0.6294
AB2	UltraVnc	1.0.9.5
AB3	Oracle 8.1.7 ADS/9/10g/11g	Oracle 8.1.7/9/10g/11gR2
AB4	Java Runtime Environment	La versione dipende dal tipo di applicativi installati

	1.6 update 25 o 1.7 update 09	
AB5	.Net Framework 3.5 Sp3	Su Windows 10 .Net framework 4.0
AB6	Oracle Jinitiator	1.3.1.22
AB7	Adobe Reader	7 – 8 – 9 – 10 - 11
AB8	PdfCreator	8.2.0
AB9	Peazip	3.1
AB10	CdburnerXp	4.5.8
AB11	Vlc	2.2.4
AB12	LibreOffice	4.4.2
AB13	Open VPN	2.4.3
AB15	Mozilla Firefox 41 o superiore	41.0.2
AB16	Google Chrome	65
AB17	Bomgar	17.1.3

- Kaspersky Endpoint Security viene configurato con funzioni di antivirus, antispyware, webcontrol, mail control, firewall;
- MSOffice è installato su richiesta e in base alla disponibilità di licenze;
- Le postazioni di lavoro fisse e mobili vengono di norma acquisite tramite le convenzioni Intercent-ER, Consip, e/o presso altri soggetti aggregatori.