ALLEGATO A

SPECIFICHE TECNICHE DELL'INFRASTRUTTURA TECNOLOGICA DEL DATA CENTER DELLA REGIONE EMILIA-ROMAGNA

1 PREMESSA

L'Amministrazione è dotata di una serie di procedure informatiche per l'automazione delle proprie attività. Ovvero, applicazioni e sistemi che hanno caratteristiche funzionali e tecnologiche diversificate. Conseguentemente negli ultimi anni hanno assunto un rilievo notevole le esigenze di integrazione e cooperazione tra applicazioni realizzate su sistemi diversi, nella logica di unificazione del sistema informativo dell'Ente.

Le attività di conduzione e di realizzazione dei progetti di sviluppo, come pure la manutenzione ordinaria ed evolutiva delle applicazioni in gestione, la gestione sistemistica del DataCenter e dei server in esso contenuti, la gestione della rete e delle postazioni di lavoro sono assicurate dalle funzioni regionali preposte, cui è affidato altresì il governo di risorse esterne per lo sviluppo e la manutenzione, acquisite sul mercato dei servizi, per migliorare l'operatività in settori di interesse dell'Amministrazione.

Nei prossimi paragrafi sono delineati il contesto tecnologico e le architetture applicative di infrastruttura nelle quali verrà integrata la piattaforma software offerta dal Fornitore.

2 CONTESTO TECNOLOGICO

Di seguito viene delineata la dotazione di infrastrutture informatiche e telematiche attualmente presenti presso l'Amministrazione.

2.1 Tecnologia Server e Storage

Presso il DataCenter dell'Amministrazione regionale sono presenti circa 480 server dipartimentali, mentre presso gli uffici regionali periferici sono distribuiti circa 40 server. I sistemi server sono tutti in tecnologia Intel, ad esclusione dei server DNS pubblici in tecnologia Itanium.

I sistemi operativi installati sono Microsoft Windows e distribuzioni Linux (RedHat e Ubuntu) oltre ad OpenVMS per i server DNS.

Tutti i server fisici del CED, ad esclusione del mirror dischi di sistema operativo, appoggiano i dati su Storage Area Network (SAN).

Dal 2007 è stata attivata la tecnologia di virtualizzazione sia sul fronte server sia sul fronte storage. La tecnologia adottata per la virtualizzazione server è VMware e la situazione attuale vede circa il 75% dei server virtualizzati su tale tecnologia.

Complessivamente quasi il 40% dei sistemi è basato su sistemi operativi Linux, il restante su sistemi operativi Microsoft Windows.

Tutti i server del DataCenter appoggiano i propri dati su SAN composta da una infrastruttura a fibra ottica, con SAN Switch e sottosistemi a disco di classe Midrange ed Enterprise: IBM DS5000, IDM DS8100, IBM v7000.

Le tipologie di meccaniche distribuite sugli Enclosure di dischi sono FC, SATA e SAS. Il 90% dello storage viene reso disponibile agli hosts tramite virtualizzatore costituito da due coppie di nodi specializzati del prodotto IBM (SVC, San Volume Controller).

Tutta l'infrastruttura VMware, tutti gli RDBMS, il DB ad oggetti di PLONE, SAS, i file server, Sharepoint e tutti i Landscape SAP sono allocati su SAN e tendenzialmente su dischi in tecnologia FC per garantire ottime prestazioni di I/O. Attualmente lo storage della SAN si attesta a circa 300 TB.

Di seguito si propone una tabella riassuntiva delle tecnologie HW server e storage con indicazione degli SLOTS disponibili in cui inserire nuove Blade:

SYSTEM SERVER		
Blade Chassis/Enclosure	**Server Blade**	**Free Slots**
HP BladeSystem Enclosure c7000, 403321-B22	HP BL460c G7, 603251-B21 HP BL460c G6, 507782-B21 HP BL680c G5, 443530-B21	2
HP BladeSystem Enclosure BLc7000, 507019-B21	HP BL460c G8, 641016-B21	20
IBM BladeCenter H, 8852	IBM Hx5, 7873 IBM HS22V, 7871 IBM HS22, 7870	30

SYSTEM STORAGE	
Controller/Expansion	**Disk**
IBM System Storage DS5300, 1818-53° IBM - Storage Enclosure EXP5000, 1818-D1A IBM - Storage Enclosure EXP810, 1812-81H	SATA 1TB, 2TB FC 146GB 15K, 450GB 15K
IBM - Storewize V7000 Control Enclosure, 2076-324 IBM - Storwize V7000 Expansion 24, 2076-224	450GB 2.5 INCH 10K HDD 300 GB 2.5INCH 15K RPM SAS HDD
System Storage Virtualization/VTL	
IBM - System Storage SVC, 2145-CF8	
IBM - System Storage TS7650G ProtecTIER Deduplication Gateway, 3958-DD5	
IBM - Storewize V7000 Control Enclosure, 2076-124 IBM - Storwize V7000 Expansion 24, 2076-224	600 GB 2.5INCH 10K RPM SAS HDD

2.2 Tecnologie Implementate sui sistemi dipartimentali

Le tecnologie, il software di base e di ambiente, nonché i principali servizi gestiti tramite questi server sono i seguenti:

Area	Tecnologie adottate
Sistemi Operativi	Microsoft Windows 2003 / 2008 / 2008 R2 – Linux RedHat 5/ 6 - Ubuntu LTS 12
Sistemi centralizzati distribuzione patching di S. O.	WSUS (Windows software Update Services) - Rhel Satellite
Web Server Internet/Intranet	Microsoft Internet Information Server 6.0/7.5 – Apache 2
Posta elettronica comunicazione unificata	Microsoft Exchange Server 2010 configurato in clustering; sistema antivirus/antispam; Lync 2013
File Server	Microsoft Windows 2008, Samba 3.3.x

DNS	Microsft, OpenVMS
Data Base Server	Oracle 10g / Oracle 11g configurato in Data Guard - Microsoft SQL Server 2005/2008/2012 configurato in clustering tramite Cluster Service. MySQL 5 e PostgreSQL 8/9 per i progetti OpenSource.
Application Server	IBM Websphere 6.1 , Tomcat 5/6, JBoss 4/5/7, per le applicazioni J2EE, Zope/Plone 3.3/4
Web Farm	Microsoft IIS 7.5 per servizi di web relativi alle applicazioni Microsoft ASP e .NET
Motore di ricerca	Solr
Motori Cartografici	ESRI ArcIMS, ESRI ArcGISserver, ESRI Image Server, Radex Server, GeoServer (Open source), MapServer
DBMS Cartografici	ArcSDE, PostGis, Oracle Spatial
Sistemi di monitoring e management sistemi Hw / Sw	HP System Insight Manager– IBM Director, ITcam,TPC – OpenSource Zabbix
Sistema Antivirus/antiSpam	TrendMicro Office Scan, Deep Security, IMSS, Network Reputation Services, McAfee AVD
Sistemi di sicurezza perimetrale e VPN SSL	Infrastruttura Firewall (Checkpoint) e VPN Connectra
Sistemi Proxy	Linux Rhel 5 – Squid
Sistemi di Backup	IBM Tivoli TSM
Motori Business Intelligence	SAS 9. 3 – Business Objects XI - SAP BW – SpagoBI
Sistemi di reportistica	Microsoft SQL server Reporting Services 2012
Sistemi di Groupware	Windows SharePoint Server 2010
Gestione Documentale	Doc-ER (Alfresco 4)
Adobe	Suite LifeCycle (PDF Generator), InDesign
Soluzioni Software acquisite da Fornitori esterni	Piattaforma Agenzie di Stampa Telpress, Rassegna Stampa Orazio Web (DataStampa), Rassegna Audio/Video Sipario (Telpress), Piattaforma Xerox FFWS 8 per Centro Stampa, Piattaforma Reitek URP
Statistiche Web	Piwik
Ambienti SAP	R/3 ECC 6.0 –CRM 7 –HR ECC 6.0– Mobile Infrastructure 7.0 – BW 7.0 – NWDI 7.0 – Solution Manager 7.0 – BPC 7.5
Sistemi di integrazione	Talend Open Studio, WebServices per integrazione applicativa, cooperazione applicativa con Porta di dominio ICAR (specifiche SPCCoop – DigitPA)
CMDB e Trouble Ticketing	CMDBuild, RT
Inventory	Microsoft SCCM 2012
Repository sorgenti	Redmine/SVN
Tecnologia virtualizzazione area desktop	Citrix XenApp 6.5, VDI con VMware View 5
Tecnologie di infrastruttura	Tecnologia VMware (Virtual Infrastructure 5) – Tecnologia Blade – Tecnologie SAN, virtualizzatore Storage IBM SVC
Domini di autenticazione	Microsoft Active Directory – SAP – IDM – FedERa
IAM	Soluzione SUN di Identity ed Access Management

Gateway e bilanciatori per servizi web	Apache, LBL Load Balancer 8
Sistemi di Storage	IBM DS5300, DS8100, V7000 – virtualizzatore storage IBM SVC - Automated TAPE Library 3584-L52, TS3310 (tecnologia LTO3, LTO4, LTO5)

2.3 Rete regionale

L'Amministrazione dispone di reti locali Fast Ethernet e Gigabit Ethernet nelle proprie sedi principali, e di una rete geografica che le raggiunge tutte. Alla rete sono collegate le sedi degli uffici e delle Agenzie e Istituti Regionali.

La rete utilizza come standard il protocollo TCP/IP, con indirizzi IP privati sulle postazioni di lavoro ed indirizzi IP pubblici per i principali sistemi server, l'interconnessione ad Internet e l'intercomunicazione con altri enti.

I collegamenti tra le sedi sono realizzati attraverso router e switch layer 3; le linee trasmissione dati che collegano le sedi fanno uso di tecnologie di telecomunicazione sia tradizionali sia innovative, ed hanno velocità fino ad 10 Gbps: si tratta di circuiti in fibra ottica di proprietà regionale, collegamenti affittati su VPN IP-MPLS, linee ADSL e HDSL, ecc.

Dal 2003 la Regione ha realizzato un'infrastruttura di rete a banda larga, chiamata Lepida, per collegare gli Enti Pubblici presenti sul territorio, ossia le Amministrazioni Provinciali, i Comuni e le Comunità Montane, le Aziende Sanitarie ed i propri uffici.

A partire dal 2007, la rete Lepida si è evoluta in modo coerente con le regole del Sistema Pubblico di Connettività (SPC), costituendo la Community Network dell'Emilia-Romagna (CN-ER); dal 2008 la CN-ER è collegata all'ambito SPC Infranet, in modo da assicurare il coordinamento informativo ed informatico tra amministrazioni centrali, regionali e locali.

A fine 2007, l'Amministrazione ha istituito la Società Lepida spa, a cui ha affidato la gestione tecnica della rete Lepida, delle connessioni ad Internet aggregate a servizio di tutti gli enti connessi su CN-ER, la registrazione dei domini Internet d'interesse proprio e degli altri enti locali, ecc.

I tecnici dell'Amministrazione conservano la responsabilità della gestione dei propri Domain Name Server pubblici, dei propri firewall, realizzati in tecnologia Checkpoint, e della rete locale e geografica a servizio dei propri uffici.

Sulla connessione dell'Amministrazione su CN-ER, che viene utilizzata per tutte le comunicazioni verso Internet e verso SPC Infranet, in orario d'ufficio viene generata una banda aggregata di circa 190 Mb/s in ingresso e circa 60 Mb/s in uscita.

2.4 Dominio regionale di accesso e certificazione

I server dipartimentali, insieme a tutti i client delle sedi principali della Regione, fanno riferimento a un dominio nativo Microsoft Windows 2008 R2 che certifica tutti gli utenti regionali.

Il dominio di rete regionale (Domain Controller, File Server, Print Server, Mail Server, DNS Server, piattaforma antivirus, IM Server, SharePoint Services) è internamente implementato su tecnologia Microsoft: Windows 2008, SQL Server 2005 e SQL Server 2012, Windows SharePoint Foundation 2010, Exchange Server 2010 Server, Lync 2013, WSUS (Windows Software Update Services).

Il dominio regionale conta oltre 5.700 account utente e 4.000 login giornalieri in media, circa 3.100 account di gruppo, oltre 5.000 computer account (tra server e workstation), circa 5.300 caselle di posta, 300 share di rete, 3.000 siti SharePoint personali e 700 siti SharePoint di gruppo.

Per le applicazioni che prevedono utenti non regionali è stato creato un dominio extraregionale che contiene oltre 10.000 account utente e circa 300 gruppi.

2.5 Sistema di Information & Event Management

L'amministrazione si è dotata di un sistema di Information & Event Management che ha il duplice scopo di:

- registrare gli accessi degli amministratori di sistema, secondo quanto richiesto dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008;
- registrare tutti gli eventi provenienti dai sistemi della rete regionale significativi dal punto di vista della sicurezza, permettendo di individuare la presenza di tentativi di intrusione o di malware.

Il logger centralizzato è costituito dai seguenti componenti:

- Arcsight logger L7200-SAN: appliance dedicato alla memorizzazione dei log in modalità sicura e non modificabile. Prevede strumenti di interrogazione e reportistica;
- Arcsight Express M7200-X-NOLOG: appliance dedicato alla correlazione dei log ricevuti attraverso il logger. Prevede strumenti di monitoraggio e reportistica basati sulla correlazione dei log provenienti da tutti i sistemi integrati;
- Arcsight connector C320: appliance che ospita i connettori che si occupano di prelevare i log da sistemi server, database, sistemi di sicurezza, apparati di rete e software complesso, di normalizzarli e inviarli al logger;

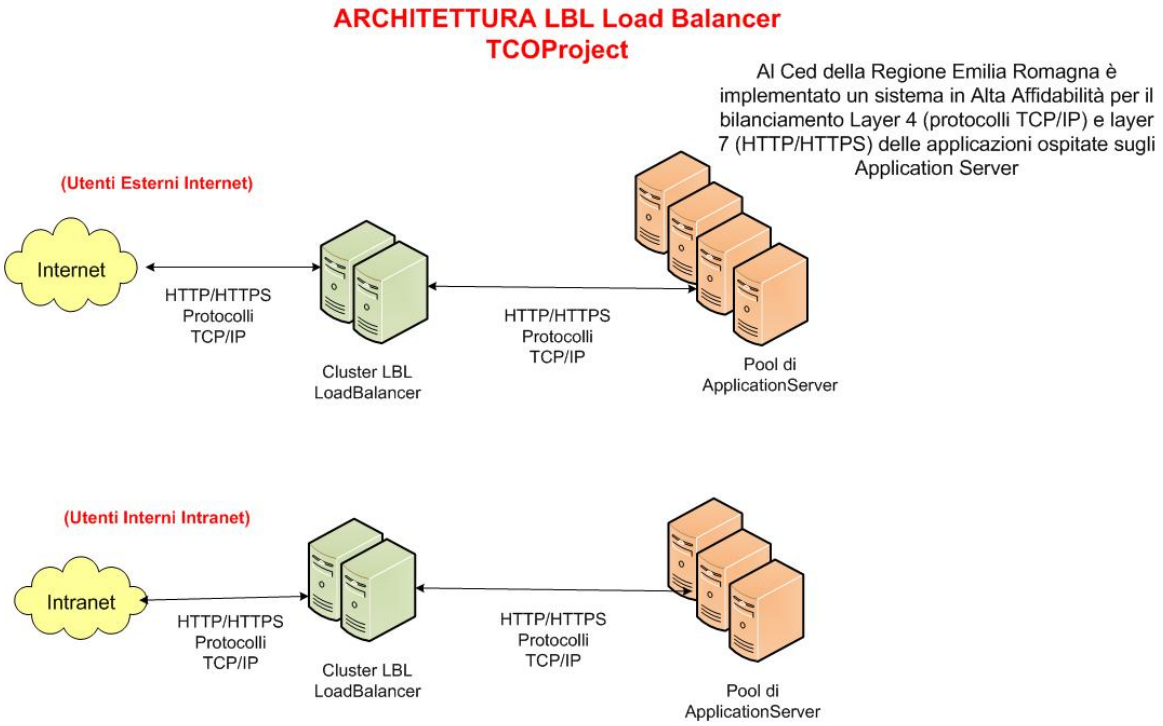
- connettori su server Windows: ospita quei connettori che hanno la necessità, per prelevare i log, di alcune personalizzazioni.

Il sistema è stato configurato per integrare i log di tutti i sistemi server, RDBMS, apparati di rete, dispositivi di sicurezza e applicazioni complesse. Mediamente durante l'orario lavorativo vengono generati circa 1200 eventi al secondo.

2.6 Sistema di bilanciatori di carico del traffico HTTP/S

L'Amministrazione ha intrapreso un progetto di consolidamento dei gateway Applicativi (Reverse Proxy) su un'architettura in Alta Affidabilità basata su TCOProject LBL LoadBalancer.

Si tratta di una soluzione software di bilanciamento del traffico di trasmissione dati a livello 4 OSI (port forwarding) e a livello applicativo 7 OSI (HTTP/S) con caratteristiche di session affinity e gestione della sessione. Di seguito si riporta lo schema di architettura implementata, da cui si evince la presenza di due cluster di bilanciamento, uno dedicato ai servizi Internet e l'altro dedicato ai servizi Intranet:



2.7 Sistema VMware vSphere 5 per virtualizzazione server

L'Amministrazione ha avviato nel 2008 un progetto di razionalizzazione, centralizzazione e consolidamento di servizi applicativi e server adottando la soluzione VMware. Oggi l'ambiente VMware implementato è vSphere (versione 5.1) e virtualizza oltre 350 Server Linux e Windows.

La piattaforma VMware si appoggia alla SAN.

Il processo di virtualizzazione server continua e la linea guida è quella di individuare prima una soluzione su piattaforma di virtualizzazione e solo nel caso ciò non sia possibile si adottano soluzioni su piattaforme fisiche.

3 ARCHITETTURE APPLICATIVE

Di seguito vengono delineate le filiere applicative supportate dall'Amministrazione regionale e le piattaforme applicative di infrastruttura disponibili per l'utilizzo da parte dei singoli sistemi informativi.

3.1 Sistema di Identity & Access Management

L'amministrazione dispone di un sistema di Identity & Access Management (IAM). Il sistema di IAM è finalizzato alla gestione razionale, scalabile ed omogenea delle utenze del Sistema Informativo della Regione, ottemperando al tempo stesso alle normative ed ai requisiti di legge in tema di sicurezza informatica e di protezione dei dati personali.

Il sistema di IAM è composto dalle seguenti componenti:

- un servizio di Directory per la gestione centralizzata delle utenze interne ed esterne, sul quale poggiano le funzioni di "profilatura" e "autenticazione" di sistemi e applicazioni integrati nello IAM;
- una soluzione di Identity Management, che, interfacciandosi a diversi repository utente, consente la gestione dell'intero ciclo di vita delle identità su specifici sistemi e applicazioni, la sincronizzazione delle password degli utenti e la delega ai referenti alla gestione delle loro utenze; consente inoltre l'automatizzazione del processo di provisioning degli account, integrato con i processi organizzativi mediante l'utilizzo di workflow;
- una soluzione di Access Management che permette l'accesso in Single Sign-On alle applicazioni web integrate, liberando le applicazioni stesse dalla gestione dell'autenticazione.

Il sistema di Access Management è inoltre integrato con il sistema di autenticazione federata della Regione Emilia-Romagna (FedERa), agendo sia come "Identity Provider", permettendo ai proprio

utenti di accedere con le proprie credenziali a servizi esposti da altri Enti del territorio regionale, che come "Service Provider", permettendo ad utenti di altri Enti l'uso di applicazioni integrate con l'Access Manager.

3.2 Sistema di autenticazione federata

La Regione Emilia-Romagna dispone di un **sistema di autenticazione federata** (FedERa) che permette a utenti e cittadini di un Ente di accedere ai servizi online erogati dagli Enti della Regione Emilia-Romagna, utilizzando le credenziali rilasciate dall'ente di appartenenza. FedERa orchestra il colloquio tra i gestori federati delle identità digitali dei cittadini: i portali web aderenti alla federazione che utilizzano tali contenitori di identità digitali garantiranno l'accesso ai propri servizi con l'introduzione di una sola credenziale di autenticazione, cioè di una coppia utente/password in modalità single sign-on.

I servizi offerti da FedERa sono:

- **Identity Manager**: gestisce la procedura di rilascio delle credenziali;
- **Identity Provider**: mette a disposizione un contenitore di identità digitali per i cittadini;
- **Identity Gateway**: consente la comunicazione tra diversi IdP e i vari servizi online aderenti alla federazione.

L'infrastruttura FedERa pone come requisito la possibilità di discriminare l'accesso ad un servizio da parte di un Service Provider basandosi su tre fattori complementari: in particolare richiede che sia possibile selezionare, a priori e nel modo più trasparente possibile, il livello di affidabilità dell'identità digitale e il livello minimo di password policy dell'utente (oltre ovviamente all'insieme di meccanismi di autenticazione considerati accettabili dallo specifico servizio), in modo da accettare risposte di autenticazione che garantiscono un certo livello di affidabilità complessiva dell'autenticazione dell'utente.

3.3 Cooperazione applicativa (PDD)

L'utilizzo della cooperazione applicativa nello sviluppo dei sistemi informativi è prescritto dal Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82 e successivi aggiornamenti) e deve avvenire secondo le specifiche del Sistema Pubblico di Connettività e Cooperazione (SPC-SPCoop), esplicitate in particolare nelle regole tecniche e di sicurezza SPC emanate con il DPCM del 1 aprile 2008.

DigitPA (ex CNIPA) ha definito, con una serie di documenti ufficiali, le specifiche tecniche e organizzative per la cooperazione applicativa fra le pubbliche amministrazioni (PA), in ottemperanza alle indicazioni normative.

La Regione Emilia-Romagna, nel contesto del Piano Telematico dell'Emilia-Romagna (PitER), ha promosso la realizzazione di una infrastruttura di cooperazione applicativa per il territorio regionale. Tale infrastruttura è stata denominata ICAR-ER, anche per evidenziare la sua "continuità" con le attività e i risultati ottenuti nel progetto interregionale ICAR.

Le principali componenti della infrastruttura ICAR-ER possono essere così sintetizzate:

1. un insieme di componenti detto Nodo di Interconnessione per la Cooperazione Applicativa (NICA), unico a livello regionale. I principali componenti del NICA sono:
    - una PDD conforme alle specifiche SPCoop per l'accesso ai servizi erogati;
    - un registro dei servizi erogati dagli enti regionali (che può eventualmente fungere da registro SICA di secondo livello), per la pubblicazione degli Accordi di Servizio SPCoop;
    - un Gestore Eventi in grado di supportare comunicazioni di tipo EDA (Event Driven Architecture – Cooperazione ad eventi) a livello regionale ed interregionale;
    - una componente che implementa gli strumenti necessari per il monitoraggio dei livelli di servizio (SLA) dei servizi erogati (modulo infrastrutturale sviluppato nel task INF2 del progetto ICAR).
2. la PDD conforme alle specifiche SPCoop e nativamente integrata con le componenti del NICA suddetto.

Il modello di gestione e manutenzione dell'infrastruttura ICAR-ER di cooperazione applicativa ha visto l'implementazione presso i sistemi del CED regionale della propria PDD su piattaforma OpenScource Linux / Jboss / Mysql configurata per colloquiare con il modulo NICA installato presso il DataCenter di Lepida SpA.

3.4 Firma digitale

È utilizzata un'infrastruttura di servizi di firma digitale, basata su un server per la centralizzazione delle funzioni di firma, verifica, cifratura, decifratura e time stamp. Questa infrastruttura è realizzata in ambiente di sviluppo Oracle e Java ed è interfacciabile dalle applicazioni attraverso web services.

La Regione si avvale di un Certificatore accreditato per i servizi di certificazione. Tutti i dirigenti e le Posizioni Organizzative sono in possesso di badge multifunzione contenenti certificati di firma digitale, per consentire l'implementazione di applicazioni con funzionalità di firma digitale.

3.5 Filiere applicative

I principali ambienti di sviluppo di applicazioni custom in uso presso l'Amministrazione regionale (basati su architettura applicativa a due e tre livelli) sono descritti nelle tabelle seguenti:

	Piattaforma **Microsoft** (**Windows 2003/2008/2008 R2)**	Piattaforma **Linux** **(Linux RHEL 5/6 – Ubuntu LTS)**
FILIERA A **Applicazioni su tecnologia JAVA (specifiche JEE)**	WS: **Microsoft IIS/LBL** AS: **IBM WebSphere** DB: **Oracle**	WS: **Apache/LBL** AS: **JBoss** DB: **PostgreSQL** **Oracle**
FILIERA B **Applicazioni su tecnologia Microsoft**	WS: **Microsoft IIS/LBL** AS: **Microsoft .NET** DB: MS **SQL Server**	-
FILIERA C **Applicazioni su tecnologia OpenSource**	-	WS: **Apache/LBL** AS: **PHP, Python, Perl Tomcat, Ruby Plone (Zope)** DB: **MySQL, PostgreSQL, Plone (Zeo)**
Legenda**: WS:** Web Server/Bilanciatore di carico – **AS:** Application Server – **DB:** Database Server		

In generale i possibili prodotti, linguaggi, ambienti di sviluppo e tecnologici sono: HTML, DHTML, CSS, XML, XSL, XHTML, WML, Perl, Python, PHP, Javascript, C, C++, SQL, PL/SQL, SOAP, WSDL, OpenLayers, Google Map API.

Le soluzioni per il repository e versioning dei sorgenti sono le seguenti: RedMine/SVN, Visual SourceSafe con netta prevalenza della soluzione SVN.

In particolare, si riportano a titolo indicativo le tecnologie sia di sviluppo che di runtime adottate per ogni filiera:

- filiera A: Oracle DB Server, PostgreSql, IBM WebSphere, JBoss-Tomcat, JEE, Java, EJB, Servlet, Jsp, Soap, Oracle Jdeveloper, Eclipse, IBM RAD, Jdbc, Javascript, Ajax, Axis, Spago, Spago BI, ecc.;
- filiera B: SQL Server, IIS, MS Visual Studio.NET, VBScript, Visual Basic, ASP, ODBC, OLEDB, Windows Scripting Host, .NET, C#, ASP.NET, ecc.;
- filiera C: MySql, PostgreSql, Tomcat, Apache, Eclipse, Php, Perl, Python, Plone, Zope, Zeo, Eclipse, Odbc, Jdbc, Javascript, Shibboleth, ecc.