SI PREGA DI PRENDERE VISIONE DELL’ALLEGATO O “Vincoli Infrastrutturali aopd”, non pubblicato prima per mero errore materiale ma facente parte integrante e sostanziale della documentazione di gara.

Vincoli infrastrutturali

LINEE GUIDA REQUISITI PER APPLICAZIONI

Al fine di assicurare la piena compatibilità delle applicazioni sviluppata/ offerte con l'infrastruttura IT dell'Azienda si richiede la stretta osservanza delle seguenti linee guida :

1. L'Azienda richiede che le applicazioni sviluppate siano esclusivamente di tipo web-based, accessibili da browser di tipo standard, senza la necessità di installare software aggiuntivo sulle postazioni client.

2. L'Azienda richiede una rigida separazione, sia logica che topologica, tra :

2.1. Motore applicativo (applicazione e relativo application server)

2.2. Dati non strutturati (file server)

2.3. Dati strutturati (database server)

3. Le applicazioni devono supportare l'utilizzo di sistemi reverse proxy e di load balancing per mediare l'accesso degli utenti, sia per ragioni legate all'ottimizzazione delle performance sia per questioni legate alla sicurezza e alla disponibilità dei servizi.

4. L'applicazione deve essere pienamente compatibile con i protocolli standard di cifratura quali SSL/TLS.

5. Le applicazioni potranno comunicare fra loro solo in modalità **Web service** utilizzando il protocollo HTTPS

6. L'Azienda ha da tempo centralizzato il proprio sistema di autenticazione in un'infrastruttura basata su protocollo LDAPS e ha inoltre sviluppato un sistema di SSO basato su protocollo CAS. L'applicazione deve obbligatoriamente utilizzare il sistema aziendale di autenticazione e opzionalmente il sistema aziendale di SSO.

7. I sistemi firewall dell'Azienda utilizzano uno rigido controllo sui protocolli applicativi utilizzati, e quindi è vietato utilizzare modalità di tunneling di protocolli proprietari all'interno di protocolli standard (es. SQLNET over HTTP).

8. In un sistema IT complesso, come quello implementato dall'Azienda, l'integrazione tra le diverse applicazioni costituisce un elemento fondamentale del sistema stesso. L'Azienda richiede che tali integrazioni sia basati su un modello di tipo SOA (Service-Oriented Architecture) e in particolare su un'implementazione di tipo ESB (Enterprise Service Bus). Sono pertanto considerate non accettabili integrazione di tipo file-sharing based, DB-DB link, multi DB access, etc.

9. Le applicazioni proposte devono essere sviluppate tenendo conto dei principali principi di sicurezza, solidità e stabilità applicativa. In tale senso vanno tenute in considerazione linee guida quali "OWASP Top 10 Proactive Controls 2018".

10. I server destinati ad ospitare le applicazioni, sia in test, collaudo o produzione, sono deployati su infrastruttura virtuale VmWare, le applicazioni devono essere pienamente compatibili con tale soluzione, inoltre non devono essere previste :

    Chiavi hardware;
    licenze legate a componenti hardware;
    specifiche riferite a clock di CPU, velocità dei dischi;
    richieste riferite a specifiche schede video o in generale hardware particolari.

11. I sistemi operativi adottati dall'Azienda per i propri server (tutti obbligatoriamente 64bits), e uniche opzioni disponibili, sono :

    Windows 2016 R2 o superiore.
    RedHat Enterprise Linux 8 o superiore.
    CentOS 7 o superiore (esclusivamente per gli ambienti di test).

12. Qualora l'applicazione richieda l'utilizzo di JDK/JRE, valgono rigorosamente le seguenti restrizioni :

    Il JDK è installato a livello di sistema.
    Le versioni di JDK adottate sono basate sul progetto openJDK che, diversamente da quanto imposto da Oracle per la propria distribuzione ufficiale, non prevede alcun licensing in ambito di produzione
    Le versioni al momento adottate sono :
    - openJDK 8 (jdk 1.8.0.251 o superiore)
    - openJDK 11 (jdk 1.11.0.16 o superiore)
    - openJDK 17

13. L'Azienda predilige applicazioni deployate su application server quali Apache Tomcat, JBoss/WildFly, Apache PHP, IIS ASP, dotnet framework. L'utilizzo di altri application server

sebbene non vietato a priori deve essere esplicitamente evidenziato nel progetto applicativo in modo da consentire un'adeguata valutazione.

14. L'Azienda mette a disposizione, all'interno della propria infrastruttura, alcune tipologie di server database. L'applicazione dovrà essere compatibile con almeno uno dei seguenti database :

    Oracle 19.15.0.0 (in configurazione RAC)
    MariaDB 10.x
    SQL Server 2014 o superiore.
    PostgreSQL 9.x,14.x

15. Per gli ambienti Linux, l'Azienda adotta una rigida segmentazione dei profili utente :

    Utenti di manutenzione applicativi: dotato di accesso SSH e specifici grant SUDO per la gestione dell'applicazione.
    Utenti applicativi: destinati esclusivamente all'esecuzione di una o più applicazioni; non dotata di alcun accesso remoto.
    Utenti di amministrazione: riservati esclusivamente al personale dell'Azienda.

16. Per gli ambienti Windows, l'Azienda adotta una rigida segmentazione dei profili utente :

    Utenti di manutenzione applicativi: dotato di accesso RDS e specifiche autorizzazioni per la gestione dell'applicazione.
    Utenti applicativi: destinati esclusivamente all'esecuzione di una o più applicazioni/servizi; non dotata di alcun accesso remoto.
    Utenti di amministrazione: riservati esclusivamente al personale dell'Azienda.

17. L'Azienda adotta una rigida politica di aggiornamento dei sistemi operativi, il Fornitore dovrà adeguare il proprio software nel caso di inadeguatezze dello stesso rispetto ai vincoli che potrebbero essere posti dagli aggiornamenti messi in atto.

18. Nel caso vengano segnalate vulnerabilità di componenti software usati, il fornitore dovrà a norma di legge segnalare all'Azienda e mettere in atto le dovute strategie per la rimozione di tali vulnerabilità.

19. Riferimenti Normativi.

Per quanto non citato si rimanda a:

AGID Determinazione n. 628/2021 del 15 dicembre 2021 - Adozione del "Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione".

Direttive AGID denominate "Misure minime di sicurezza ICT per le pubbliche amministrazioni" (dettagliate nella Circolare 18 aprile 2017, n. 2/2017 e pubblicate sulla Gazzetta Ufficiale n. 103 del 5/5/2017).

Decreto legislativo 30 giugno 2003, n. 196

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

aggiornato in base ai seguenti provvedimenti:

• decreto legislativo 14 settembre 2015, n. 151.
• decreto legge 18 febbraio 2015, n. 7,
convertito, con modificazioni, dalla Legge 17 aprile 2015, n. 43;
• legge 27 dicembre 2013, n. 147;
• decreto legislativo 14 marzo 2013, n. 33;
• decreto legislativo 28 maggio 2012, n. 69;
• decreto legge 9 febbraio 2012, n. 5,
convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35;
• decreto legge 6 dicembre 2011, n. 201,
convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214;
• decreto legge 13 maggio 2011, n. 70
convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106;
• legge 4 novembre 2010, n. 183;
• legge 29 luglio 2010, n. 120;
• decreto-legge del 25 settembre 2009, n. 135
convertito, con modificazioni, dalla legge 20 novembre 2009, n. 166;
• legge 4 marzo 2009, n. 15;
• decreto-legge del 30 dicembre 2008, n. 207
convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14;
• decreto-legge 25 giugno 2008, n. 112
convertito, con modificazioni, dalla legge 6 agosto 2008 n. 133;
• decreto legislativo 30 maggio 2008, n. 109;
• legge 18 marzo 2008, n. 48, ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno
• decreto-legge 28 dicembre 2006, n. 300
convertito, con modificazioni, dalla legge 26 febbraio 2007, n. 17;
• decreto-legge 12 maggio 2006, n. 173
convertito, con modificazioni, dalla legge 12 luglio 2006, n. 228;
• decreto-legge 30 dicembre 2005, n. 273
convertito, con modificazioni, dalla legge 23 febbraio 2006, n. 51;
• decreto legge 30 novembre 2005, n. 245
convertito, con modificazioni, dalla legge 27 gennaio 2006, n. 21;
• decreto legislativo 7 settembre 2005, n. 209;
• decreto-legge 27 luglio 2005, n. 144
convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155;
• decreto-legge 30 dicembre 2004, n. 314
convertito, con modificazioni, dalla legge 1 marzo 2005, n. 26;
• decreto-legge 9 novembre 2004, n. 66
convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 306;
• decreto-legge 24 giugno 2004, n. 158
convertito, con modificazioni, dalla legge 27 luglio 2004, n. 188;
• decreto-legge 29 marzo 2004, n. 81
convertito, con modificazioni, dalla legge 26 maggio 2004, n. 138;
• decreto legislativo 22 gennaio 2004, n. 42;

• decreto-legge 24 dicembre 2003, n. 354
convertito, con modificazioni, dalla legge 26 febbraio 2004, n. 45