Aeroporto di Pescara

Rinnovamento Tecnologico S.A.G.A.

SOMMARIO

1. EXECUTIVE SUMMARY

Il presente documento si propone di analizzare nel dettaglio l'infrastruttura hardware, software e l'organizzazione dei processi di business del sistema informativo S.A.G.A. al fine di proporre alcune soluzioni atte al miglioramento dei servizi di gestione aeroportuale in vista dell… [Ristrutturazione aeroporto/Tratte].

A tale scopo sono stati portati a termine una serie di interventi conoscitivi dell'infrastruttura informatica aeroportuale.

A valle del assessment effettuato e dell'esame della documentazione fornita si propongono le seguenti aeree di intervento.

- **Rete Dati** – Rete LAN e la connessione ad internet
- **Sistemi di elaborazione e memorizzazione dati** – Infrastruttura CED dell'aeroporto, server, storage e sistema di backup. Comprende il sistema di virtualizzazione e la riorganizzazione dei server di gestione di Back-Office, contabilità ecc.
- **Gestione dei processi di business** – Analisi e proposta di ottimizzazione nella gestione dei processi relativi al business dell'aeroporto. Quali:
  - Sistemi di gestione voli / passeggeri
  - Sistema Gestione bagagli
  - Gestione avvisi al pubblico
  - Fatturazione voli… ecc.
- **Applicazioni per la gestione aeroportuale** – Strettamente connesse alla riorganizzazione dei processi di business aeroportuale, l'ottimizzazione e l'aggiornamento dei software di piattaforma per il business dell'aeroporto.
- **Sistema di controllo accessi e sicurezza**. Creazione di un sistema automatizzato di controllo ai varchi basato su tornelli e/o postazioni digitali di scansione badge per gestire in modo granulare la sicurezza delle aeree protette, memorizzare e storicizzare gli accessi.
- **Sistema di videosorveglianza**. In grado di gestire il controllo delle aeree aeroportuali, tramite l'utilizzo di tecnologie di rilevamento del movimento, autoregistrazione ecc.
- **Sistema di gestione del parcheggio** – Razionalizzazione dei sistemi di gestione parcheggio al fine di limitare le violazioni, aumentare il fatturato e connettere il sistema parcheggio a processi interni di CRM che prevedono la gestione del passeggero a 360 gradi.

Formattato: Non Evidenziato

2. INFRASTRUTTURA DI ELABORAZIONE E RETE DATI

2.1. SITUAZIONE ATTUALE

Al termine dell'assessment dell'infrastruttura di rete e del CED sono stati raccolti e riorganizzati I dati e gli schemi forniti, si delinea la seguente situazione, descritta per aree tematiche quali: Rete Dati, Sistema di Elaborazione, conservazione e salvataggio dei dati, stazioni PC utente.

2.1.1. RETE DATI

La rete dati fisica è strutturata in modalità piatta senza la creazione di subnet IP ne VLAN, Poggia su switch di rete HP e Cisco singoli (non ridondati) connessi in cascata.
Sono definiti 3 segmenti di rete totalmente isolati fra loro:

1. Rete di Office-automation: include I server e le applicazioni dell'amministrazione aeroportuale. Tale rete include:
    a. **CED.** Nel quale sono dislocati gli apparti connessi ai server, e alcuni switch di centro stella.
    b. **Uffici di piano.** Connessi attraverso switch in cascata su rete flat Layer2.
    c. **Biglietteria.** Connessa attraverso switch in armadio di distribuzione posto nei pressi della stessa.
2. Rete di Reparto Operativo
    a. Accesso remoto Sistema CUTE / SITA (Firewall, DCE e Router Fastweb)
    b. Connessione remota RayanAir
3. Voli in tempo reale
    a. Software Design: voli in tempo reale, Display Unit gestite centralmente e sito web con aggiornamento dati voli.

2.1.1.1. RETE DI CED

La rete di CED è composta da switch di classe top-of-rack con porte di accesso rame e alcune porte di uplink fibra SX 1Gbit, modelli Cisco 3750G, HP Procurve 2810-24G e 2810-48G, Netgear 4572DP per l'accesso ethernet degli access point del sistema di riconcigliazione bagagli. Gli switch sono basati su configurazione a singolo oggetto logico/fisico non ridondati, di tipo standalone.
Il cablaggio è effettuato tramite cavi 1Gbit rame per tutti gli elaboratori connessi.
Le porte di uplink in fibra ottica 1Gbit SX trasportano la rete verso i piani e gli altri armadi di distribuzione presenti.

2.1.1.2. LAN DI PIANO

Le LAN di piano sono gestite da apparati L2 di HP, posizionate in armadi di distribuzione, connessi a stella dagli switch di CED descritti. Non sono definite VLAN.

2.1.1.3. PUNTI DI ACCESSO WIRELESS

A bordo pista sono presenti 8 Access Point obsoleti Cisco Aironet previsti per il sistema riconciliazione bagagli.

2.1.1.4. CONNESSIONE A INTERNET

La connessione ad internet per la rete Office Automation è realizzata tramite una linea Telecom 4Mbit/256 Kbit, dotata di 4 inidirizzi IP pubblici.

Il sistema di protezione internet (firewall) è realizzato attraverso una virtual appliance Kerio Control/Proxy.

Il firewall è configurato per fungere anche da proxy server per gli utenti/PC client interni dell'amministrazione aeroportuale. Il sistema Kerio è fuori manutenzione e fuori supporto.

2.1.2. INFRASTRUTTURA DI ELABORAZIONE

1. **Server e client**

Attualmente i servizi di back-office sono ospitati su un'unico server che esegue l'HyperVisor VSphere 4.0, con hardware di generazione precedente, non di proprietà dell'amministrazione, che non dispone di supporto e manutenzione.
E' inoltre in funzione 1 domain controller Active Directory aggiuntivo basato su hardware fisico di vecchia generazione.
Sono in funzione circa 30 PC obsoleti per l'accesso ai dipendenti di S.A.G.A., connessi al dominio specificato.

Servizi eseguiti su Server e PC Standalone obsoleti:

- Il server del sistema biglietteria che gestisce la bigliettazione per Ryanair.
- Il server di gestione del sistema di condizionamento.
- Il server per la gestione degli accessi con software di riconoscimento biometrico (WINGAEP).
- Il server FAAC che gestisce il sistema parcheggio.
- File Sharing di backup dell'ambiente virtuale.
- Server fisici e PC per sistemi SITA / CUTE e ARCO (Registrazione passeggeri), basati su hardware totalmente obsoleto e fuori supporto.

Relativamente al reparto operativo sono in funzione:

- I 2 server obsoleti "Voli in tempo reale" e Display Unit, della Software Design, che gesiscono inoltre un sito web dedicato per l'accesso alle informazioni sui voli da internet. I sistemi citati non sono configurati in alta affidabilità e non è garantito il salvataggio della configurazione degli stessi. Sono presenti 13 Dispay Unit di precedente generazione: 8 posizionate sopra i banchi Check-in, 4 nella Hall, 1 dopo varco.
- E' presente nel CED 1 Server Novell eseguito su hardware IBM Netfinity obsoleto (Nome: "Server SAGA") con Software di fatturazione voli Team System ORUS.

Non è presente un sistema che offra l'alta affidabilità per i servizi elencati.

2.1.3. AMBIENTE VIRTUALE

I servizi di back-office si SAGA sono eseguiti all'interno di 6 virtual machine, all'interno di un'unico host VSphere 4.0, con Hardware appena sufficiente all'esecuzione del parco attuale; il server non è di proprietà dell'azienda. Non è prevista Vmware HA (Alta affidabilità).

Virtual Machines rilevanti:

- Il server della contabilità interna è eseguito su una Virtual Machine SQL Server interna all'host ESX citato che gestisce la piattaforma Team System Gamma.
- Una appliance di backup "Acronis" che gestisce "immagini disco" è presente sotto forma di Virtual Machine, ed effettua il backup delle virtual machine su un piccolo NAS esterno di tipo casalingo.
- Server Antivirus
- Servers Domain Controller Active Directory

2.1.4. IMPIANTI DATACENTER

All'interno del datacenter è disponibile un condizionatore standard per il raffreddamento del locale, un gruppo UPS APC Smart-ups 15.000 per il backup di emergenza dell'alimentazione elettrica dei sistemi.

Tutti i dispositivi sono dislocati su 2 Rack da 19", 1 rack ospita gli apparati di rete, l'altro ospita gli elaboratori, tra i quali 2 server risultano spenti/guasti.

Inoltre sono presenti 1 UPS che gestisce la rete privilegiata ed 1 gruppo elettrogeno da 350KVA che fornisce alimentazione di emergenza all'intero aeroporto.

2.1.5. IMPIANTI DI SICUREZZA FISICA

Gli impianti di Security attualmente presenti sono o assenti o obsoleti, comunque non più adeguati alle attuali esigenze.

2.1.5.1. VIDEOSORVEGLIANZA

Attualmente l'impianto di videosorveglianza è costituito da un numero limitato di telecamere che non riescono a fornire una copertura completa delle aree sensibili. Inoltre la tecnologia delle telecamere è obsoleta tale da non garantire supporto tecnico in caso di guasti e non permette l'applicazione delle attuali tecniche di videosorveglianza.

2.1.5.2. CONTROLLO ACCESSI

Attualmente l'accesso alle aree dell'aeroporto è consentito alle persone autorizzate soltanto esibendo il tesserino al personale di sicurezza. La modalità di controllo non permette di conoscere in tempo reale lo stato degli accessi e non consente un controllo dello storico.

2.1.5.3. ANTINTRUSIONE

Attualmente non è presente nessun impianto di antintrusione. Un tentativo di effrazione ed intrusione di malviventi all'interno dell'aeroporto non potrà essere rilevato automaticamente. Non potranno essere informate in modo tempestivo le autorità di polizia locale ne i responsabili di SAGA.

2.2. LIMITAZIONI E CRITICITÀ DELL'ARCHITETTURA ATTUALE

A valle dell'analisi presentata si riassumono le limitazioni e i possibili rischi dell'attuale implementazione in termini di infrastruttura informatica.

L'elaborazione tiene in considerazione i desiderata del cliente stesso nelle aree in cui ha espresso le maggiori preoccupazioni o la volontà di migliorare ed aggiornare i sistemi al fine di ottenere una risposta più reattiva e coerente con il futuro business dell'aeroporto.

Relativamente ai servizi operativi e di back-office, rete e sistemi server / virtualizzazione si evincono le seguenti criticità:

1. **Nessuna forma di alta affidabilità** è implementata fra i sistemi presenti. In caso di guasto al server Hyper-Visor o ad un server di qualunque applicazione, i servizi saranno interrotti fino alla riparazione dello stesso, che potrebbe risultare di difficile esecuzione e con importante latenza temporale, vista l'assenza della garanzia sull'hardware. L'impatto sul business è due tipi:
    a. Inaccessibilità dei servizi IT per personale di Back-office, con conseguente calo della produttività aziendale.
    b. Inaccessibilità dei servizi di core business dell'aeroporto, con danni di immagine, problemi operativi e di gestione, quali ritardi e mancato rispetto di impegni/contratti.

2. **Sicurezza dei dati**. A livello di sicurezza (certezza ed affidabilità del dato) e protezione fisica dei dati, i sistemi di supporto e memorizzazione fanno affidamento su server locali stand-alone con sistemi RAID di vecchia generazione, basati su hardware fuori supporto e manutenzione. L'impatto sul business è legato al rischio di perdita dei dati con conseguente costo sul valore dei dati stessi, sull'esercizio dei sistemi che sarebbe immediatamente arrestato con conseguente arresto dell'operatività. Minore è l'affidabilità dei supporti di memorizzazione maggiore è il rischio di perdita dei dati, interruzione del servizio e ricorso al backup, che impatta notevolmente sui tempi di riprsitino dell'operatività.
3. **Software di virtualizzazione obsoleto e fuori supporto**. La piattaforma virtuale implementata attualmente non è più in grado di garantire l'esecuzione di nuove virtual machine ne servizi compatibili con le nuove versioni dei sistemi operativi attuali. L'impatto sul business è il seguente:
    a. Impossibilità di adeguarsi a nuove piattaforme software in grado di erogare servizi in modo più efficiente, con maggior time-to-market e minor risorse (costi) impegnati.
    b. Impossibilità di adeguarsi a software e sistemi che gestiscono nuove regolamentazioni, nuovi sistemi di condivisione delle informazioni ed accesso a servizi esterni che siano conformi al business aeroportuale, con gli stessi livelli di servizio, compatibilità ed efficienza delle strutture aeroportuali internazionali comparabili.
    c. Scarsa flessibilità della piattaforma comporta maggiori tempi (costi) per attività di adeguamento, migrazione, amministrazione ed erogazione delle risorse; il tutto conduce ad un maggior time-to-market e dunque comporta uno scollamento fra decisioni strategiche e capacità stessa di attuarle, dunque diminuisce l'efficacia della piattaforma IT rispetto alle scelte del business.
4. **Il sistema di backup è inefficiente**, si basa su una tecnologia che non è in grado di garantire la conservazione dei dati ne di medio ne di lungo periodo. Il sistema attuale presenta performance di basso livello, Inoltre un sistema di backup solo locale non consente di ripristinare i dati in caso di disastro del datacenter. L'impatto sul business è il seguente:
    a. In caso di corruzione logica delle informazioni e dunque di necessità di ripristino di dati risalenti a periodi precedenti, il sistema mostra limiti tali da non consentire tale attività con conseguente rischio di perdita di informazioni o necessità di ricostruzione manuale del dato. La fattispecie conduce a maggiori tempi (costi) di gestione e rallentamento delle rispettive attività di business connesse con la gestione del dato stesso.
    b. In caso di disastro (incendio, furto, sabotaggio, calamità naturale) che impatti il CED, tutti i dati di tutti i servizi (Back-office e produzione) gestiti da SAGA andrebbero perduti senza alcuna possibilità di ripristino. La fattispecie ha impatto soprattutto per i dati che hanno un valore storico e devono essere riutilizzati per le attività di amministrazione e gestione futura, quali i dati contabili e commericali (fatture verso fornitori, fatture attive, fatturazione voli, interventi ed attività di società collegate ecc.); I dati operativi quali la gestione degli interventi effettuati da società connesse al SAGA, i dati di programmazione attività di produzione quali orari dei voli e scheduling delle attività correlate, programmazione carburanti, attività del personale ecc.; Informazioni di controllo (registrazione accessi ed autorizzazioni, configurazioni dei sistemi di antiintrusione, controllo del personale, gestione telecamere, regitrazioni del sistema di videosorveglianza ecc.). Relativamente all'ambiente virtuale che contiene i sistemi operativi che eseguono tutte le applicazioni ed i servizi di business, anche tale assetto andrebbe perduto per sempre, dunque in caso di ricostruzione del CED a seguito di un disastro parziale, l'attività di ripristino dei sistemi sarebbe notevolmente più lunga a livello temporale, impattando così su:

i. Forte slittamento delle Operatività e produzione (aeroporto non fruibile e forte OpEx)
ii. Costi e tempi di implementazione del ripristino dei sistemi (forte CapEX)

c. Inoltre le performance previste attualmente per il sistema di backup non consentono di effettuare ripristini dei dati con prestazioni adeguate. Ciò ha un impatto sui tempi (costi) di ripristino e relativi ritardi dell'operatività, i quali dovrebbero essere invece minimizzati così da consentire rapidamente il riutilizzo del dato perduto per dare continuità alle attività operative, di gestione e di amministrazione di SAGA.

5. **Hardware obsoleto**. I server delle applicazioni aeroportuali, di biglietteria, del sistema parking, di gestione accessi ecc. sono eseguiti su hardware server e PC obsoleti, senza alcuna forma di tolleranza al guasto. In caso di guasti hardware può risultare difficoltoso e temporalmente inefficiente la riparazione ed il ripristino del servizio. L'assenza della garanzia spesso non consente affatto la sostituzione delle parti danneggiate, che potrebbero non essere reperibili. L'impatto sul business è relativo alla cessazione per periodi di tempo intollerabili di servizi essenziali per l'operatività dell'aeroporto.
6. **Difficoltà nell'amministrazione dei sistemi**. Sistemi di gestione aeroportuale e di supporto ai servizi SAGA eseguiti su posizioni differenti, su piattaforme non uniformi, spesso su semplici PC obsoleti e non amministrabili centralmente. Questo conduce ad una elevata difficoltà di gestione e rende impossibile la centralizzazione del management conducendo a zone oscure dell'infrastruttura parzialmente fuori controllo. L'impatto sul business è centrato sui costi operativi e sull'inefficienza delle risorse umane impiegate nella gestione e nell'amministrazione dei servizi.
7. **Disegno Rete LAN errato**. La rete di piano e di dipartimento è interconnessa attraverso patch panel non etichettati e il cablaggio è confusionario, comportando un'ulteriore difficoltà di intervento in caso di modifica della configurazione o inserimento di nuovi host/pc in rete. La rete fisica non è certificata e non è disponibile alcun libro di permutazione fra porte di rete e patch panel. Inoltre alcuni armadi di accesso rete sono dislocati in aree non idonee (zone passeggero o promiscue) comportando rischi per la sicurezza informatica e per la gestione. L'impatto sul business è centrato sulla scarsa sicurezza informatica che espone i sistemi a furto di dati, violazione della confidenzialità dei sistemi, possibilità di sabotaggio con relatva interruzione dei servizi, danneggiamento delle informazioni ecc.
8. **Sistema di firewall instabile**. Il sistema di firewall presente eseguito in una Virtual Appliance non è più supportato (manutenzione non rinnovata), di conseguenza non è più aggiornabile a livello di criteri di sicurezza, anti-intrusione, antispam, antivirus.
9. **Rete di CED inaffidabile.** La rete di Datacenter (CED) che interconnette fra loro servizi e sistemi pensati per High-performance e alta affidabilità è attualmente costituita da soli apparati standalone (singoli). Con tale configurazione non è possibile garantire la connettività fra le piattaforme "core" in caso di guasto ad uno dei componenti di networking. L'impatto sul business è relativo al rischio di guasto non recuperabile in tempi adeguati, con conseguente interruzione delle attività di business e dunque costi imprevisti.
10. **Sistema Riconciliazione Bagagli fermo.** L'utilizzo degli access point Cisco Aironet per il sistema di riconciliazione bagagli presenta il problema dell'interferenza degli aeromobili fra gli access-point e gli apparati wireless in pista. L'impatto sul business è il seguente:
    a. Le procedure di riconciliazione bagagli sono meno efficienti e meno certe con conseguente consumo eccessivo di risorse (costi) e relativo rischio di smarrimento.

b. Il sistema di gestione bagagli in pista non può essere automatizzato tramite l'infrastruttura in essere a causa delle ragioni di cui sopra ed andrebbe ri-ingegnerizzato attraverso tecnologie differenti.

11. **Nessun sistema di monitoraggio** è presente all'interno della rete, dunque in caso di guasti prevedibili o situazioni di grave rischio per i dati e per i servizi l'amministrazione SAGA o il team IT non possono venirne a conoscenza in tempi adeguati, ma solo a guasto avvenuto. L'impatto sul business consiste nell'impossibilità di prevenire un guasto e dunque aumentare il rischio che esso si verifichi con relative conseguenze sull'operatività (costi).
12. **PC utente obsoleti** sia livello hardware che software (Sistema operativo e applicazioni). Tale situazione rende difficoltosa l'attività giornaliera dell'amministrazione e impossibile l'adozione di recenti versioni di applicazioni strategiche. Inoltre i modelli dei PC e dei sistemi operativi e software installati sono disomogenei, questo rende complesse le attività di gestione ed amministrazione del parco PC, quali allineamento delle versioni applicative, gestione policy centralizzate, distribuzione applicazioni, allinemento del livello di sicurezza dei PC utente ecc. Inoltre il sistema operativo Windows XP non è più supportato da Microsoft, con la conseguenza che aggiornamenti e fix non vengono più rilasciati lasciando così i computer sotto continua minaccia di Virus, Trojan, SpyBot e in genere software pericoloso e non conforme alle policy aziendali, che può compromettere l'operatività e danneggiare i dati condivisi, persino rappresentare un rischio per i servizi di dominio. L'impatto sul business è relativo alla minore efficienza delle attività di amministrazione e gestione del personale aeroportuale e alla difficoltà di adeguarsi a nuove piattaforme, al passo con l'evoluzione tecnologica globale.
13. **Sistema anti-intrusione:** Non essendo presente alcun sistema di antiintrusione, nella fattispecie il rischio di sabotaggio, danno ai sistemi o furto di informazioni sensibili è molto più elevato rispetto agli standard aeroportuali internazionali, vista l'assenza di procedure automatiche di allarmistica. L'impatto sul business è il seguente:
    a. Rischio di furto con relativi costi pari al valore dei beni.
    b. Rischio di sabotaggio con rischio di interruzione dell'operatività.
    c. Oltre al chiaro rischio a livello di salute e sicurezza personale; esiste un impatto relativo a danni a persone o cose che può comportare l'instaurazione di procedure penali o civili contro SAGA.
14. **Il sistema di videosorveglianza** è ormai obsoleto, sottodimensionato, carente a livello funzionale ed attualmente non operativo viste le precedenti considerazioni. In caso di richiesta da parte dell'autorità giudiziaria di materiale per indagini a seguito di eventi sospetti o criminosi nell'area aeroportuale SAGA risulterebbe impreparata a fornire il necessario supporto. L'impatto sul business è simile al punto precedente:
    a. Rischio che si verifichino eventi che impattano sulla sicurezza personale.
    b. Rischio di sabotaggio con rischio di interruzione dell'operatività.
    c. Impatto relativo a danni a persone o cose che può comportare l'instaurazione di procedure penali o civili contro SAGA.
    d. Rischio che si verifichino, con maggiore probabilità eventi quali incendi o allagamenti, poiché non possono essere prevenuti.

    Inoltre, nel caso in cui si verificasse l'accesso non autorizzato di personale di terra o di volo a determinate aree dell'aeroporto, il personale vigilante non sarebbe in grado di prendere le opportune contromisure. Un sistema di videosorveglianza adeguato è essenziale al fine di determinare in tempo reale situazioni di pericolo, possibili focolai di atti vandalici, cortocircuiti, attività sospette, effrazioni effettuate in aree interne all'aeroporto ecc.

15. **Software di controllo accessi inesistente**; non è attiva alcuna automazione per il controllo ai varchi, di conseguenza qualunque individuo dotato di tesserino aeroportuale può avere accesso all'aeroporto senza alcuno screening su orari consentiti, autorizzazioni specifiche ecc. Questa carenza può aumentare rischi legati ad atti criminosi, furti, sabotaggi, trasporto e passaggio di merci illegali ecc., con conseguente impatto sui costi e sull'immagine dell'aeroporto, nonché avere conseguenze penali e civili.

3. ESIGENZE

3.1. VISIONE GENERALE DELLA CRESCITA E RELATIVI IMPATTI

Effettuando un benchmarking generale dei sistemi IT aziendali in comparazione fra l'attuale infrastruttura tecnologica di SAGA ed infrastrutture aeroportuali confrontabili emerge che le aree sopra trattate risultano essenziali per realizzare un adeguamento allo standard del settore.

In vista di eventuali estensioni dei contratti con le compagnie aeree gestite da SAGA e dell'aumento del numero di voli e relativi passeggeri, tutte le aree trattate nel presente documento sono da considerare estremamente sensibili. Si consideri infatti che dato l'aumento consistente del numero di voli annui e dei relaviti passeggeri, si verificherà di conseguenza:

1. Un aumento della probabilità di atti vandalici, tentativi di accesso non autorizzato, di effrazione, di furto o sabotaggio, di pericolo alla sicurezza pubblica o di rischi penali connessi al trasporto di oggetti illegali ecc.. In tale area ricadono gli interventi sui sistemi di sicurezza quali controllo accessi automatizzato, sistema di videosorveglianza, anti-intrusione. Tutti gli eventi di cui sopra inoltre conducono alla necessità di interagire con le forze di polizia e con le autorità giudiziarie, ciò rende essenziale ottimizzare la collaborazione fornendo in tempo reale i dati degli accessi, le registrazioni delle telecamere ecc.. Tale reattività non è utile solo al fine di scongiurare altri possibili eventi di questo tipo in futuro ma anche al fine di non ricadere in lacune ed impreparazione tali da rappresentare un rischio penale o civile (monetario) per SAGA stessa.
2. Aumento del numero di processi e di transazioni per minuto sui sistemi informatici. In presenza di un numero maggiore di utenti e di processi, il numero di transazioni informatiche nell'unità di tempo viene di conseguenza impattato richiedendo sistemi IT che siano reattivi al business. In tale area ricade l'intervento di adeguamento dei server, del sistema di storage, dei PC, della rete al fine di garantire un supporto di lungo periodo.
3. Maggiore impatto economico in caso di interruzione dei processi di business e dei servizi erogati, connesso con un aumento di costo per unità di Rischio relativo alla scarsa sicurezza e all'inaffidabilità dei sistemi IT. In tale area ricadono gli interventi su sistemi informatici (HW e SW) ad alta affidabilità, e ricade nell'intervento sulla realizzazione di una architettura IT di nuova generazione, con elevati standard di sicurezza che scongiurino sabotaggi o manomissioni. Inoltre collaterlamente è coinvolto l'intervento sul sistema di backup, che minimizza l'impatto sul business nel caso di perdita accidentale o volontaria (manomissione, sabotaggio) di dati essenziali per le attività operative o di gestione/amministrazione.
4. Maggior impatto economico in caso di interruzione dei processi di gestione/amministrazione del personale interno di SAGA. In tale ambito ricadono gli interventi che saranno suggeriti sia per l'alta affidabilità sia per il sistema di salvataggio dei dati, e per il rinnovamento del parco PC.
5. Maggior impatto economico in caso di inefficienza, rallentamento dei processi operativi, rallentamento delle attività di gestione ed amministrazione. In tale ambito ricadono gli interventi che sono suggeriti per l'aumento dell'efficienza dei sistemi informatici e della flessibilità che accelera il tempo di fornitura (provisioning) di risorse e servizi IT in risposta alle mutate esigenze del business o di fronte a rapidi cambiamenti o riassetti che ottimizzino le attività operative. Tale aumento dell'efficacia dei sistemi, risponde alla richiesta di efficacia dei processi di business ed è strettamente legato alla reattività dell'intera infrastruttura.
6. Forte impatto economico in caso di perdita irrecuperabile di tutti i dati su cui poggiano tutti i processi operativi e gestionali, con rispettiva interruzione di tutte le attività operative e gestionali (fermo di tutti i servizi). In tale area ricadono gli interventi sul sistema di storage e di backup suggeriti.

7. Maggiore impatto sulle attività di governance di tutti i processi e sistemi, nonché di monitoraggio delle risorse IT. In tale ambito ricadono tutti gli interventi atti a realizzare una infrastruttura gestibile centralmente con vista sinottica dell'intero environment, monitorabile sia a livello di corretta operatività e funzionalità dei sistemi, sia a livello di utilizzo delle risorse / performance in grado di prevenire in tempi adeguati eventuali sovraccarichi futuri dovuti alla crescita, avendo chiari i tempi e le modalità di crescita. Tali interventi sono finalizzati anche alla predisposizione di una architettura in grado di scalare le risorse in base alle esigenze in modo trasparente e non impattante sull'operatività. Il disegno proposto è tale da scongiurare "lock-in" ovvero blocchi dovuti ad esaurimento di risorse dovute a "gabbie" hardware a risorse finite, che non consentono l'espandibilità in tempo reale, ma richiedono il fermo servizi e il ridisegno architetturale ogni qual volta si superi il carico massimo del singolo elemento fisico. Il disegno architetturale a "Silos" verticale di risorse finite della vecchia generazione informatica dovrebbe essere superato da una architettura aperta tale da espandersi e comprimersi flessibilmente in base alle esigenze operative, senza che l'attività di reazione al business richieda fermi del servizio o migrazioni totali di piattaforma.

3.2. SICUREZZA DEI DATI

Al fine di garantire la custodia dei dati, l'integrità e la usabilità degli stessi si rende necessaria l'adozione di componenti informatiche in grado di proteggere i dati attraverso sistemi di memorizzazione centralizzati di tipo dipartimentale quali storage array SAN/NAS. Tali sistemi dovranno possedere funzionalità di resilienza dei dati quali sistemi di parità tipo "RAID" in grado di scongiurare guasti parziali improvvisi dei supporti di memorizzazione; alimentazioni ridondate con almeno 2 accessi a diverse linee elettriche in grado di sopravvivere ad un black-out di una linea, sistemi di ventilazione dei componenti elettronici ridondati in grado di continuare a raffreddare il sistema in caso di guasto ad una o più ventole; sottosistemi disco accessibili almeno tramite 2 percorsi separati e alternativi, in grado di conservare inalterate le operazioni di scrittura/salvataggio dei dati anche in caso di guasto ad un percorso.

La sicurezza dei dati da accesso di terzi non consentito (confidenzialità ed integrità) riguarda anche la configurazione della rete dati, che dovrà essere conforme agli standard di isolamento (VLAN). Così tutti I sistemi di gestione (management) degli apparati richiesti dovranno rispettare degli standard di sicurezza informatica quali confidenzialità e cifratura dei dati ottenuta tramite standard de facto: SSL/HTTPS/SSH/VPN ecc.

3.3. AFFIDABILITÀ DEI SISTEMI

Per scongiurare l'interruzione di servizio in caso di guasto di un componente hardware o di errore logico di un componente software si richiede di porre tutta la pila di sistema (dagli strati applicativi o logici più alti fino all'hardware fisico) in una modalità detta HA (High Availability) o alta affidabilità.

A livello di sistemi di Server o di HyperVisor di virualizzazione si richiede dunque la presenza di almeno un componente aggiuntivo rispetto al minimo indispensabile, configurato in HA, così da tollerare il guasto di uno

dei componenti, riavviando nel modo più rapido possibile le applicazioni sul nodo gemello, in modo automatico.

A livello di storage system si richiede un sistema completamente ridondato dove non esista un singolo punto di guasto che causi l'arresto del servizio.

Si richiedono sistemi server e storage in grado di poter essere aggiornati a livello software senza che l'aggiornamento richieda alcun disservizio applicativo.

Per scongiurare che le applicazioni ed i sistemi operativi che condividono lo stesso hardware in un sistema di virtualizzazione possano accedere reciprocamente, volontariamente o accidentalmente ai rispettivi dati residenti in memoria e nei microprocessori, si richiedono soluzioni di virtualizzazione che siano in grado di garantire un'isolamento certo ed adeguato dei domini di virtualizzazione.

Al fine di scongiurare il fermo servizio per i sistemi vitali dell'aeroporto, si suggerisce di importare nell'ambiente virtuale (P2V: Physical To Virtual) gli OS Server eseguiti su PC o Elaboratori obsoleti e senza supporto/manutenzione. In tal modo i servizi automaticamente potranno servirisi dei meccanismi di alta affidabilità garantiti dall'architettura virtuale suggerita.

3.4. CRITERI DI EFFICACIA ED EFFICIENZA

Per aumentare l'efficienza nell'utilizzo delle risorse si richiede di implementare sistemi di virtualizzazione dei server, al fine di eseguire un elevato numero di server virtuali su uno stesso hardware fisico, risparmiando così in termini relativi sul costo d'acquisto (CapEX), sul costo di gestione (OpEX) che contiene la manutenzione e supporto, il raffreddamento, l'alimentazione ecc..

Allo stesso modo per quanto riguarda la memorizzazione dei dati si richiede di implementare sistemi che consentano di sfruttare efficientemente lo spazio attraverso algoritmi di compressione logica, in modo tale da poter rappresentare una quantità di dati molto più elevata di quella effettivamente fornita fisicamente.

A tale scopo si richiede di implementare sistemi di memorizzazione di massa centralizzati ed affidabili che supportino le funzionalità di Thin provisioning, AutoTiering con accelerazione SSD, compressione dei dati, clonazione efficiente a spazio zero, snapshot.

Per soddisfare il criterio di efficacia delle soluzioni richieste, a livello informatico è necessario confrontare l'attuale sistema informatico di supporto al business dell'azienda con la rispettiva soluzione realizzata dall'eventuale fornitore, che dovrà far corrispondere l'investimento richiesto con l'erogazione del livello di servizio desiderato.

I livelli di servizio non possono prescindere dalla velocità e flessibilità nella gestione dei sistemi, vantaggio che aumenta il time-to-market, ovvero il tempo che decorre da una decisione del management, al momento in cui si implementa in produzione la soluzione relativa. Più breve sarà il time-to-market, maggiore sarà la corrispondenza fra le decisioni del management e la loro applicazione pratica. Gli ambienti virtuali di nuova generazione garantiscono la possibilità di massimizzare i risultati in termini di fornitura di risorse elaborative ed applicazioni rispetto al tempo impiegato per gestire il processo di implementazione stesso, ottimizzando al massimo i costi, e rispettando il criterio della flessibilità che è alla base dell'efficacia stessa di un sistema IT nel rispondere alle esigenze di business.

Non ultimo dovrà essere soddisfatto il livello di servizio previsto dalle infrastrutture fondamentali, quali sistema di riconciliazione bagagli, sistema di controllo accessi, sistema di videosorveglianza ecc, servizi che attualmente mostrano carenze gravi o difficoltà di implementazione.

3.5. SCALABILITÀ RICHIESTA DELLA SOLUZIONE

L'amministrazione ha l'obbligo di fornire un adeguato supporto informatico alle applicazioni aeroportuali, alle attività dei propri dipendenti e ai dati di produzione, garantendo il supporto per gli asset attualmente in produzione e/o necessari durante la gestione societaria corrente. Allo stesso tempo ha la responsabilità di garantire un adeguato supporto all'evoluzione del business dell'aeroporto, la capacità dell'aerostazione di affrontare un'aumento imprevisto del traffico aereo e dei servizi offerti, negli anni, potendo gestire rapidamente i cambiamenti necessari a soddisfare tale crescita, senza che la relativa espansione tecnologica causi disservizi.

Per tali ragioni, ed in ultimo per preservare nel tempo l'investimento che si intende affrontare, i sistemi informatici a supporto del business dovranno soddisfare:

1. Richieste di rapida espandibilità in termini di spazio di archiviazione.
2. Richieste di rapida espandibilità in termini di carico elaborativo e memoria applicativa.
3. Richieste di rapida espandibilità in termini di ospitalità di nuovi clienti e sistemi (Rete, storage e server).
4. In generale: Richieste di ampliamento di risorse senza richiedere la minima interruzione dei servizi applicativi in produzione ("A caldo")

Queste richieste non dovrebbero richiedere cambiamenti o sostituzioni totali, nel breve/medio termine, del Tipo/Modello dei seguenti sistemi forniti, per il rispetto del rapporto fra capitale investito ed il tempo complessivo di sfruttamento delle risorse:

1. Storage System (capacità di espandere la sola capacità disco anche con tipologie differenti e possibilità di attivare licenze per nuove funzionalità sulla stessa piattaforma)
2. Sistemi di elaborazione (possibilità di scalare la potenza dello stesso server o il numero di server "a caldo" senza modificare sostanzialmente l'architettura prevista)
3. Sistema di backup Server e Software relativi (possibilità di scalare le risorse del server o le funzionalità della piattaforma di backup, senza interruzione del servizio di salvataggio dati).

3.6. CRITERI DI SICUREZZA FISICA

Per adeguare il livello di sicurezza ad un ambiente di tipo aeroportuale è necessario videosorvegliare le aree sensibili e controllare l'accesso alle stesse aree alle sole persone autorizzare.

L'impianto di videosorveglianza deve poter registrare immagini di qualità elevata (tipo Full HD – 1080p@30fps) in qualsiasi condizione di luminosità, in modo di permettere il riconoscimento di persone e oggetti in seguito di segnalazioni.

Il software di gestione della videosorveglianza deve essere scalabile, flessibile e ampliabile con app add-on di analisi video (tipo lettura targhe, oggetto non rimosso, ecc) L'installazione deve supportare la

virtualizzazione per poter essere integrato all'interno dell'infrastruttura DC dell'aeroporto. Il software deve permettere di effettuare ricerche a posteriori in maniera semplice tramite ora e data e generare allarmi in caso di eventi particolari (motion detection, ecc).

Il software di controllo accessi dovrà permettere la profilazione degli utenti assegnando privilegi a seconda del ruolo e alla responsabilità.

L'impianto di controllo accessi deve poter profilare gli utenti muniti di badge da un'unica interfaccia amministratore in maniera semplice. Inoltre si dovrà poter conoscere la situazione degli accessi in tempo reale oltre che analizzare lo storico. L'installazione deve supportare la virtualizzazione per poter essere integrato all'interno dell'infrastruttura DC dell'aeroporto.

4. SOLUZIONE SUGGERITA

Al fine di soddisfare le esigenze espresse dall'ente si suggerisce alla S.A.G.A. di prevedere i beni e servizi descritti in seguito.

Le esigenze per la fornitura sono organizzate in 2 sezioni:

1. Fornitura di hardware, software e servizi di implementazione per l'infrastruttura CED.
2. Fornitura di software e servizi per il ridisegno e l'aggiornamento delle applicazioni di gestione aeroportuale.

Formattato: Non Evidenziato

4.1. SISTEMA DI MEMORIZZAZIONE DATI

Al fine di memorizzare i dischi dei server fisici e delle Virtual Machine VMware preesistenti e le future (ovvero dei server che eseguono ed eseguiranno tutte i servizi aeroportuali interni), contenenti i dati delle applicazioni di back-office e di gestione aeroportuale, nonchè il NAS di produzione e tutti i sistemi di supporto, si rende necessario, per le considerazioni di cui sopra, l'approvvigionamento di un sistema di storage di marca primaria e classe di mercato tecnologico "midrange".

Un sistema di storage di classe midrange, prevede una serie di funzionalità di base, quali sicurezza, ridondanza, scalabilità, performance e numero di oggetti logici gestibili simultaneamente. Tali funzionalità minime consentono di garantire a S.A.G.A. l'approvvigionamento di un sistema che si ponga in una classe di prodotto adeguata alle esigenze e che garantisca il raggiungimento degli obiettivi stabiliti.

Il motivo che guida la scelta di un sistema di classe midrange e di marca primaria è che il sistema di storage protegge e gestisce gli asset fondamentali dell'azienda. Un sistema della classe prevista è stato tipicamente distribuito dal produttore a centinaia di migliaia di clienti e dunque presente sul mercato in numerosissime unità. Ciò garantisce la **qualità** intriseca del prodotto, ed in particolare:

1. Presenza di un microcodice del sistema fortemente stabile.
2. Rapida produzione di patch e aggiornamenti per qualunque BUG software (malfunzionamento che potrebbe compromettere i dati e/o i servizi) e continuo miglioramento del sistema operativo / microcodice.
3. Vasta presenza del supporto del produttore sul territorio, che garantisce riparazione di guasti o risoluzione di problemi in breve tempo senza prolungamento di disservizi.
4. Garanzia che non sia dismesso il supporto stesso per scomparsa del produttore dal mercato.

Per le ragioni sopra esposte, il sistema di storage richiesto dovrà avere le seguenti caratteristiche minime necessarie:

REQUISITO	OBIETTIVO	VALORE RICHIESTO
Sistema di marca primaria valutato come leader nel settore.	Garantire che non siano forniti sistemi "compatibili", con qualità di funzionamento incerta e senza adeguato supporto enterprise.	Prodotto da una delle Industrie rappresentate nel sub-quadrante dei "Leaders" all'interno del "Gartner 2014 Magic Quadrant for General-Purpose Disk Arrays"
Gestione Block Level (SAN) convergente (FC/FCoE)	Richiesto dall'architettura globale per motivi economici.	Sì – Licenza attiva
Numero di Storage Controller in High Availability (HA)	Alta affidabilità	Minimo 2
Nessuna interruzione di servizio in caso di "fail" di un controller	Alta affidabilità	Sì – presente
Mirroring della write cache fra gli Storage Controller	Alta affidabilità ed integrità dei dati	Sì – Licenza attiva

Multipath verso i dischi dati: Almeno 2 path di accesso da ciascuno Storage Controller verso ciascun disco	Alta affidabilità	Sì – Licenza attiva
Funzionalità “Hot-swap” per tutti i dischi appartenenti allo storage – sostituibili a caldo senza interruzione di servizio.	Alta affidabilità	Sì – presente
Dual Power Supply – ridondanza degli alimentatori per ciascun componente dotato di alimentazione elettrica.	Alta affidabilità	Sì – presente
Ridondanza del sistema di raffreddamento – nessuna interruzione di servizio in caso di “fail” di una ventola.	Alta affidabilità	Sì – presente
Automatic On-line RAID parity rebuild – ricostruzione automatica della parità su disco spare in caso di “fail” inatteso di un disco di qualunque raid group.	Integrità dei dati	Sì – Licenza attiva
Numero Spare Disk richiesti per ciascun raid-group configurato nel sistema rilasciato dal fornitore, al fine di soddisfare la capacità netta richiesta nella presente tabella.	Integrità dei dati	Almeno 1
Ridondanza generale dei componenti elettronici	Alta affidabilità	Assenza di SpoF (Single Point of Failure) , Ogni componente elettronico deputato al servizio di “data storage e data access” deve essere ridondato.
Protezione e conservazione della write cache in caso di interruzione completa dell’alimentazione elettrica nel sito, loading della write cache al riavvio del sistema di storage e finalizzazione delle scritture dal buffer sui dischi fisici.	Integrità dei dati	Sì – necessario, attraverso qualunque forma di conservazione della write cache in caso di interruzione dell’attività di entrambi i controller (in NVRAM protetta da batteria, destaging della cache/cache-vaulting su disco rotativo o flash ecc.).
Numero richiesto di porte FC Target 16Gbit/s (front-end verso gli Host) richieste	Alta affidabilità, Bilanciamento e performance	Almeno 4
Supporto Multipath per gli Host connessi via FC	Alta affidabilità, Bilanciamento e performance	Sì - necessario e attivo nello storage fornito
Quantita massima di porte FC Target 16Gbit supportate	Alta affidabilità, Bilanciamento e performance	Almeno 10
Quantità massima di porte Ethernet 10Gbit supportate	Alta affidabilità, Bilanciamento e performance	Almeno 4
Quantità massima di porte FCoE 10Gbit supportate	Alta affidabilità, Bilanciamento e performance	Almeno 4
Thin Provisioning Nativo	Efficienza dei dati,	Sì – necessario e incluso

	basso TCO relativo.	
Cloni di volumi/LUN in thin provisioning – effettuati on-line senza interruzione di servizio.	Efficienza e flessibilità, risparmio sui tempi e sui costi di gestione, miglior time-to-market.	Sì – Licenza attiva
Numero di LUN supportate	Scalabilità e dimostrazione di performance, gestione di carichi simmetrici ed elaborazione parallela.	Almeno 8000
Numero di host/initiators supportati	Scalabilità e dimostrazione di performance, supporto al carico simmetrico ed elaborazione parallela.	Minimo 512
Numero minimo di dischi collegabili direttamente ai controller dello storage (NON external array virtualization)	Scalabilità e dimostrazione di performance, supporto al carico simmetrico ed elaborazione parallela.	Almeno 200
Scalabilità massima (TB raw)	Requisito per Scalabilità futura, per l'ospitalità dei dati, per eventuali esigenze future.	Almeno 700TB
Aggiunta di dischi e/o shelf allo storage array "a caldo" senza interruzione del servizio per le applicazioni.	Affidabilità e livello di servizio per le applicazioni.	Sì – presente
Espansione a caldo dei volumi e delle LUN – senza interruzione del servizio per le applicaizoni.	Affidabilità e livello di servizio per le applicazioni.	Sì – presente
Espansione a caldo dei pool di storage, dei volumi e delle LUN sui dischi e shelf aggiuntivi in caso di futura espansione dello spazio raw – senza interruzione del servizio per le applicaizoni.	Affidabilità e livello di servizio per le applicazioni.	Sì – Licenza attiva
Capacità minima netta utilizzabile fornita inizialmente – protetta in RAID5 con capacità spare (al netto di deduplica e compressione).	Richiesta iniziale di spazio disco per le esigenze minime + spazio per importazione sistemi fisici (P2V) + spazio spare di crescita a breve termine.	**>3TB netti con l'utilizzo di 2 Tier: 1° Tier SSD con almeno 1,5TB netti/usabili. 2° Tier SAS con almeno 2TB netti/usabili.** NOTA: Si può installare maggiore capacità ed eventualmente aggiungere anche diversi Tier disco, fatto salvo il requisito minimo necessario.

Capacità del microcodice dello Storage array di ottimizzare le scritture su dischi SSD in modo tale da minimizzare la "write-amplification".	Affidabilità del sistema e integrità dei dati delle applicazioni	Sì – necessario
Capacità del microcodice dello Storage Array di computare in tempo reale il numero di scritture su ciascun disco SSD o la percentuale di scritture massima supportata da ciascun disco, ed avvisare proattivamente l'amministratore del sistema sul raggiungimento di "end-of-life" del/dei dischi.	Affidabilità del sistema e integrità dei dati delle applicazioni	Preferibile
Supporto tipologia dischi nei loop di back-end	Supporto per scalare in modo eterogeneo, dimostrazione di supporto di livello/classe midrange, possibilità di supporto tecnologico futuro nel medio termine senza necessità di ri-acquisto dell'intero sistema.	SAS, SSD/FLASH,NL-SAS
Possibilità di supportare negli stessi loop di dischi Back-end diverse tipologie di disco simultaneamente	Supporto esteso per scalare in modo eterogeneo, dimostrazione di supporto di livello/classe midrange	Sì – tipologie in intermix supportate: SSD/FLASH, SAS, NL-SAS
Supporto dischi SAS ad elevata densità	Efficienza, risparmio di spazio e relativi costi. Dimostrazione di supporto di livello/classe midrange, possibilità di supporto tecnologico futuro nel medio termine senza necessità di ri-acquisto dell'intero sistema.	Sì – necessario: SFF SAS.
Dimensione dischi supportati dal sistema – direttamente connessi ai controller (NON tramite storage virtualization)	Supporto esteso per dischi di nuova generazione.	Minimo necessario: SSD fino a 3,5 TB, SAS fino 1.800GB, SATA o NL-SAS fino a 6TB
Velocità di rotazione massima richiesta per tipologia disco rotativo	Prestazioni richieste per I profili di Input/output utilizzati dalle applicazioni.	SAS: 15.000, NL-SAS: 7200
Livelli di parità richiesti	Criteri di affidabilità ed	RAID 0, 1, 5, 6 o equivalenti.

	integrità/protezione dei dati.	
Cache Memory minima globale nei controller sotto forma di NVRAM/DRAM	Performance ed efficienza	Almeno 64GB.
Dimensione massima supportata della Cache all'interno del SAN controller sotto forma di Flash Memory.	Performance ed efficienza, dimostrazione di livello/classe midrange.	Almeno 700GB
Auto-Tiering (spostamento automatico a caldo dei dati sui vari tier disponibili in base alla frequenza di accesso ai dati ed alla tipologia di I/O)	Possibilità di allocare dischi ad elevata capienza e basse prestazioni, ottenendo elevati livelli prestazionali tramite l'accelerazione della cache (su tier più pregiati)	Sì – supportato dallo storage fornito, e attivabile su richiesta.
Funzionalità SnapShot	Protezione, Backup, Efficienza, flessibilità, time-to-market.	Opzionale/Preferibile – se inclusa: licenza illimitata per tutto lo spazio storage fornito e per tutti I volumi/LUN del sistema.
Numero minimo di snapshot attivabili per LUN/Volume o sistema	Dimostrazione di livello/classe midrange.	Se inclusa licenza Snapshot: almeno 8000 per sistema.
IOPS Massimo supportato dal sistema entro 1 millisecondo di latenza (100% del carico)	Dimostrazione di livello/classe midrange.	Almeno 300.000 IOPS dichiarato ufficialmente dal produttore.
IOPS Massimo del sistema fornito nella configurazione richiesta (misurabile con profilo di I/O: 100% random read – con block size 4K oppure 8K)	Dimostrazione di livello/classe midrange.	Almeno 200.000 IOPS Burst - dichiarati ufficialmente dal produttore.
Ottimizzazione delle performance per volumi/LUN sotto Snapshot.	Prestazioni identiche anche in modalità protezione dati.	A meno di tecnologie snapshot di tipo "Copy-Out", per tutte le tipologie "Copy-on-write" è necessario un algoritmo di ottimizzazione delle prestazioni in scrittura su un volume/LUN protetto da snapshot.
Supporto iSCSI su 10Gigabit Ethernet	Supporto per tecnologia di accesso ai dati in grande espansione sul mercato e nei modelli tecnici più diffusi.	Sì – attivabile on-the-fly su licenza nel sistema fornito senza aggiunta di engine esterni – supportato nel microcodice degli storage controller forniti.
Supporto NAS interno – Architettura convergente	Per imminente o futura richiesta di condivisione di file integrata totalmente nell'investimento effettuato, nessuna	Opzionale/Preferibile. Situazione Ottimale: Storage array che consenta di attivare il supporto NAS in caso di necessità aggiungendo solo licenze interne al microcodice

	richiesta aggiuntiva di spazio, nessuna richiesta di modifica del layout del rack, massima efficienza.	ed eventuali porte ethernet, senza alcuna interruzione delle operazioni dello storage, ne disservizio applicativo, ne aggiunta di Gateway NAS esterni.
Tipologia del supporto NAS previsto – se attivabile.	Tecnologie di mercato (vasto utilizzo) richieste per l'accesso ai file.	NFS V3, NFS V4.1, CIFS SMB 1,2,3.
Protocolli supportati dal sistema senza l'aggiunta di gateway esterni.	Specifica finale dei protocolli supportati dal sistema (tecnologie di mercato)	Opzionale/Preferibile: FCP, FcoE, iSCSI, NFS, CIFS
Tipologia di interfacce previste per il supporto NAS futuro	Specifiche di mercato per l'accesso ai file.	10 Gigabit Ethernet/FCoE Fiber – 10GBase-SR o SFP+
Upgrade del firmware/microcodice/storage-OS a caldo senza interruzione del servizio per le applicazioni.	Alta Affidabilità e livello di servizio minimo richiesto, integrità del servizio applicativo. Dimostrazione della classe di prodotto.	Sì – necessario e incluso
Sistemi operativi supportati (minimo)	Supporto per I sistemi operativi che possono essere richiesti per applicazioni aeroportuali. Dimostrazione della classe di prodotto.	Microsoft Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2012 R2, MS Hyper-V, HP-UX, Oracle Linux, Oracle Unbreakable Linux, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESX/ESXi/VSphere, IBM AIX, Solaris, Citrix XenServer, HP OpenVMS, Apple OS X
Supporto per VSphere richiesto	Supporto richiesto per il sistema di virtualizzazione necessario per la migrazione e l'esecuzione dei sistemi operativi, già in esecuzione presso SAGA.	Vmware VAAI, VASA e "Site Recovery Manager" Plug-in/integration, sotto forma di software sviluppato direttamente dal produttore dello storage system fornito, integrato con il microcodice degli storage controller.
Supporto per Mirroring/Replica remoti dei dati	Supporto per Protezione e disaster recovery; per usi nel breve/medio termine.	Sì – supportato nel microcodice dello storage system.
Supporto per soluzioni ufficiali di "Stretched SAN" / Metro-storage per business continuity e disaster recovery.	Supporto per Protezione, Business Continuity, disaster recovery; per usi nel breve/medio termine. Dimostrazione di	Sì – supportato per il modello di sistema fornito, offerto direttamente dal produttore dello storage system fornito ed integrato nel microcodice degli storage controller.

	Classe e livello di prodotto.	
Supporto per Integrazione Applicativa e Backup basato sugli snapshot per Vmware Vsphere.	Protezione dati, integrità dei dati e sicurezza per le applicazioni	Sì – supportato e sviluppato ufficialmente dal produttore dello storage system.
Sistema di management integrato fruibile via rete TCP-IP per la configurazione di raid-group, storage pool, tiering, volumi e LUN, masking, gestione snapshot, cloni e replica, visualizzazione e monitoring dei dischi.	Modalità minime di gestione del sistema.	Sì – incluso – sviluppato ufficialmente dal produttore dello storage system.
Connettori, cavi di interconnessione fra I controller, cavi di interconnessione loop dischi in multipath, cavi fibre channel.	Cavi e connettori richiesti per il funzionamento.	Componenti necessari per la messa in produzione del sistema e delle sue funzionalità come specificato nella presente tabella. In particolare: "SFP FC 8Gbit/s LC" necessari a popolare tutte le porte FC Target minime richieste/fornite; "SFP 10Gbase-SR LC" necessari a popolare le tutte porte 10GBE eventualmente fornite. Eventuali cavi di interconnessione fra I controller per il mirroring dell'NVRAM/CACHE, per la connessione fra I nodi NUMA, per la connessione fra Host directors, controllers, data directors ecc. Tutti i cavi necessari per il funzionamento in multipath di tutti i loop disco dello storage system. Cavi Fibra ottica OM2/3 (o superiore) in grado di soddisfare il trasferimento "line-rate" (8Gbit/sec, 10Git/sec) per tutte le interfacce dati richieste/fornite almeno fino a 5 metri di distanza tra Initiator e Target o tra DTE e DCE, per la connessione fra lo storage e le porte dei server richiesti.
N. 2 SAN Switch di FC Fabric	Supporto per accesso alla fabric degli host connessi alla SAN.	Sì. Richiesto/Necessario. Caratteristiche minime per ciascuno switch: n.8 porte FCP 8Gbit/s Full-Duplex, almeno 4 porte FCP licenziate per switch inclusi relativi SFP 8Gbit/s; Supporto Trunking attivabile, inclusa funzione di Aliasing e

		Zoning (hardware e software Zoning), Supporto attivabile per Extended Fabric (Trasporto traffico e zone su switch in cascata), interoperabilità con Brocade Fabric-OS; Throughput complessivo non bloccante; Interfaccia di gestione e configurazione switch e zoning via Web e via CLI (SSH).

Servizi di implementazione Storage necessari:

L'installazione e la configurazione dello storage system richiede una serie di attività professionali minime, che possono essere formalizzate in base alle richieste espresse nella seguente tabella.

REQUISITO	VALORE RICHIESTO
Installazione base	Installazione in rack 19" del sistema, cablaggio di tutti I moduli interni allo storage stesso. Upgrade del microcodice dei controller e del firmware dei dischi e moduli di switching / loop dischi all'ultima versione raccomandata dal produttore.
Configurazione base	Configurazione base del sistema; creazione dei raid groups e raggruppamento in poiché pool di storage. Se presenti diverse tipologie disco (es. SSD+SAS, SSD+SATA), è richiesta la creazione di un unico pool di AutoTiering, o comunque massimo di 1 pool per storage controller.
Connessione degli host connessi	Connessione dei cavi FC degli iniziatori alle porte target dello storage tramite cablaggio ordinato nel rack e "pettinatura" dei fasci di cavi. E' richiesta inizialmente la connessione degli Host alla SAN in Fabric sugli switch FC, con almeno 2 Path per Host verso ciascuna Target port del controller (tot. 4 path per host verso la SAN).
Creazione delle LUN	Il numero delle LUN definite deve essere commisurato al criterio di massima efficienza, dunque sarà richiesto il numero più basso possibile di unità di spazio per gli Host connessi (es. 2). Le LUN saranno utilizzate come datastore VSphere.
Presentazione delle LUN	Masking delle LUN agli Host tramite il sw di gestione della SAN fornito. I datastore Vsphere dovranno "essere visti" dall'HyperVisor in multipath, utilizzando il sistema di accesso ALUA.
Configurazione dell'efficienza dello storage	Attivazione del thin provisioning e di eventuali funzioni di compressione dati su volumi/LUN contenenti dischi virtuali.

4.1.1. SISTEMA NAS

Al fine di gestire l'accesso ai dati condivisi dell'azienda si suggerisce di realizzare inizialmente un cluster di Microsoft Windows Server 2012 eseguito in almeno 2 macchine virtuali con condivisione dello storage, configurato in HA. Il cluster realizzato dovrà gestire l'accesso ai dati condivisi secondo il seguente schema:

- **Profilo Utente**: \\NAS-DNS-NAME\Profiles\Username
- **Home Directories**: \\NAS-DNS-NAME\Home\Username …"\Documents" system folder tipicamente su C:\[Utenti\Documens].
- **Directory Condivise dipartimentali:** \\NAS-DNS-NAME\[root-folder]\Directory-dipartimentale

Codice campo modificato

Codice campo modificato

4.2. SISTEMI DI ELABORAZIONE

Al fine di garantire l'esecuzione delle applicazioni in un ambiente enterprise, si rende necessario utilizzare un sistema elaborativo in grado di supportare l'HyperVisor Vmware Vsphere 6.0, ultima versione della tecnologia già utilizzata in SAGA. In particolare è necessario l'approvvigionamento di almeno 2 (due) sistemi server enterprise con le seguenti caratteristiche minime:

Hardware richiesto	**Quantità e spefiche tecniche**
Form-factor	Server da rack (rackable) 19".
Occupazione spazio rack	Massimo 2 unità Rack
Alimentatori ridondati Hot swap	Minimo 2 alimentatori sostituibili a caldo senza interruzione operativa.
Sistema di raffreddamento ridondato	Almeno 2 ventole di raffreddamento globale atte a realizzare il flusso d'aria Front-Rear del server – sostituibili a caldo senza interruzione operativa.
Tipo processore	Minimo: N.2 CPU Intel Xeon serie E5 V3 oppure E7 V3
Frequenza minima processore	Frequenza base: 2.4 Ghz
Memoria	Minimo: 160GB RAM fornita con moduli da almeno 32GB l'uno
Espandibilità memoria	Almeno 768GB; Minimo 12 Slot memoria sulla motherboard
Tipo memoria	Almeno DDR4; ECC – Error Correction Code con possibilità di memory mirroring.
Controller Ethernet 10Gigabit	Minimo: N.2 porte 10Gigabit Ethernet SFP+ dotate di SFP 10Gbase-SR lc.
Controller Ethernet 1Gigabit	Minimo: N.4 porte 1Gigabit Ethernet rame 1GBase-T
Porta e sistema di gestione via TCP-IP	Minimo: 1 porta Ethernet 1Gbit rame dedicata alla gestione del sistema da remoto anche a sistema operativo spento. Il sistema deve consentire: accesso KVM (Keyboard/video/mouse) con interfaccia remota, accesso al POST del sistema, al BIOS e installazione remota del sistema operativo attraverso l'utilizzo della redirezione di un installation media del client connesso.
Controller Fiber-Channel	Minimo: 2 porte FC 8Gbit/s – Supporto protocollo FCP, FC-Tape support; Boot su SAN configurabile dal BIOS del controller stesso. N.2 SFP Fibre Channel 8Gbit/s LC inclusi.
Controller disco	Controller Raid SAS 6Gbit/s in grado di supportare almeno configurazione RAID-1
Dischi dati – Opzionale	Nessuno richiesto. Opzionale: Si potrà fornire opzionalmente 1 o più dischi SSD da utilizzare come dispositivo cache dell'Hypervisor.
SAN Boot	Attività Necessaria: il server dovrà essere configurato per effettuare il boot sul sistema di storage SAN fornito via FCP. Il server NON dovrà effettuare il boot su dischi locali.

Per i sistemi sopra elencati si rendono necessari i seguenti servizi minimi:

Servizio necessario	**Dettagli**
Installazione base	Installazione in rack, cablaggio dei cavi ethernet di gestione, dei cavi ethernet di accesso dati e delle interfacce fiber-channel; aggiornamento firmware dei server (componenti da aggiornare se presenti:

	BIOS, BMC, NIC, HBA, SCSI controller). Esecuzione e verifica di un POST completo del sistema senza errori.

4.2.1. SISTEMI ELABORATIVI PER ORACLE

Al fine di garantire l'esecuzione delle applicazioni di gestione voli "Software Design" in un ambiente enterprise, si rende necessario utilizzare un sistema elaborativo in grado di supportare l'esecuzione del Database Oracle in ambiente virtuale in alta affidabillità. A tal scopo sono state dimensionate le risorse dell'ambiente virtuale nel paragrafo relativo.

La scelta dell'ambiente virtuale è motivata da 2 ragioni:

1. Possibilità di ottimizzare il costo delle'hardware, poiché l'esecuzione in ambiente fisico richiederebbe l'aggiunta di due Host fisici all'environment. L'utilizzo del modello di licenza Oracle "per user" consente di non calcolare il numero di core fisici presenti nello strato elaborativo dell'hyper-visor.
2. Requisito di flessibilità ed alta affidabilità del server Oracle garantita dell'ambiente virtuale proposto nella configurazione suggerita.

Considerando che attualmente SAGA sfrutta le applicazioni di gestione voli di Software Design (SWDES), e che il design che definisce l'accesso al database è basato su numero di utenti (Named User) definito, il modello di licenza necessario, con la versione attuale del software, è "Per User License",ovvero quella già acquistata da SAGA. ~~La versione suggerita/sufficiente secondo gli sviluppatori e sistemisti SWDES è "Oracle Standard One".~~

Licenze Oracle richieste:

- "~~Oracle Stanard One": 5 User License + 1 Anno di supporto.~~
- Nessuna, al momento non saranno effettuate attività di upgrade della piattaforma esistente.

Licenze OS richieste:

- Nessuna. Licenza già coperta da Windows Server Datacenter Edition in esecuzione sugli Host VSphere.

Servizi necessari per l'implementazione dell'architettura Oracle:

- ~~Installazione OS nelle virtual machine richiesta per Oracle DB di SWDES, oppure~~ importazione (P2V) dell'host fisico preesistente nell'ambiente virtuale e necessarie attività di cleaning dei driver e software physical-hardware-related. ~~Clusterizzazione via Microsoft MSCS~~

~~*(Nota: La creazione delle istanze e degli schemi, ed il relativo popolamento dei DB sarà a a cura dei fornitori dell'applicazione di gestione voli SWDES)*~~

4.2.2. VIRTUALIZATIONE DEI SISTEMI OPERATIVI

Al fine di garantire continuità alle applicazioni attualmente in esercizio, e di consolidare nell'ambiente virtuale tutte le applicazioni attualmente ospitate su server fisici ~~(escluso Oracle Database)~~, si richiede l'approvvigionamento di:

Software richiesto	**Quantità e spefiche tecniche**	**Servizi necessari per l'implementazione**
Vmware Vsphere 6.0 Enterprise	N. 4 CPU-Socket + Vcenter	Installazione, configurazione e messa in esercizio dell'ambiente virtuale sui sistemi di server forniti dal fornitore per lo scopo.
Microsoft Windows Server 2012R2 Datacenter Edition	N. 4 CPU-Socket (2 server biprocessori)	Installazione e configurazione di Windows Server 2012 su 2 macchine virtuali – Upgrade a Windows server 2012 Active Directory di 2 domain controller, a partire da 2 domain controller Windows Server 2008 attuali.

Al fine di realizzare correttamente l'infrastruttura prevista è necessario configurare l'ambiente virtuale secondo I seguenti criteri:

Servizio professionale richiesto	**Dettagli**
Installazione Hypervisor	Installazione di Vmware Vsphere 6.0 sui server richiesti secondo specifiche concordate col personale tecnico nominato dall'amministrazione dell'aeroporto.
Configurazione Vsphere	Configurazione dei datastore, creazione di 1 template per ciascuno dei seguenti OS: Windows Server 2008R2, Windows 2012R2, Linux, configurazione dei virtual switch e delle relative VLAN (almeno tutte quelle richieste nel presente allegato tecnico), del Cluster Vsphere, dell'HA, del DRS, di tutte le regole necessarie, ottimizzazione delle performance.
Creazione delle virtual machine necessarie	Creazione delle virtual machine necessarie a migrare il dominio Active Directory da Windows Server 2008 a Windows Server 2012R2. Creazione delle virtual machine necessarie al funzionamento dell'infrastruttura, laddove il fornitore NON installi a proprie spese un server fisico

	aggiuntivo, la funzionalità Vcenter sarà configurato in una macchina virtuale.
Migrazione	Migrazione nel nuovo ambiente di tutte le virtual machine attualmente residenti sul server Vsphere 4.0 dell'amminstrazione. La migrazione prevede la conservazione dell'OS e della configurazione dei sistemi operativi importati, a meno delle necessaqrie modifiche di drivers ed eventuale espansione dei logical disk degli OS importati. La migrazione include l'upgrade all'ultima versione dell'hardware emulato nei computer virtuali e del software di supporto di VSphere residente nei Guest OS.
Importazione sistemi obsoleti	Si rende necessario importare in ambiente virtuale tutti i sistemi operativi Windows e Linux residenti su PC e server fisici standalone obsoleti, al fine di garantire il servizio e scongiurare fermi definitivi al collasso dell'hardware non manutenuto, presenti nel CED.

4.2.3. SISTEMA DI SALVATAGGIO DEI DATI

Al fine di supportare correttamente i processi di salvataggio dei dati dell'azienda, si rende necessario l'approvvigionamento dell' hardware, software e servizi necessari per la realizzazione di un sistema di backup automatico dei dati.

Dispositivo di memorizzazione dei dati di backup suggerito (sistema economico):

Bene richiesto	**Quantità e specifiche tecniche**	**Servizio di implementazione richiesto**
Server di backup	Tipo rackable – massimo 3 unità rack 19". Capacità di ospitare almeno 16 dischi SAS SFF hot swap.	Installazione in rack, upgrade firmware (BIOS, BMC, Controller rete e dischi); Installazione e configurazione del sistema operativo che ospiterà il sw di backup. Connessione cavi ethernet di gestione e dati, cablaggio porte FCP.
Alimentatori ridondati – hot swap	Minimo 2 alimentatori sostituibili a caldo senza interruzione operativa.	
Sistema di raffreddamento ridondato – hot swap	Almeno 2 ventole di raffreddamento globale atte a realizzare il flusso d'aria Front-Rear del server – sostituibili a caldo senza interruzione operativa.	
CPU del server di backup	Almeno 1 CPU Intel Xeon serie E5 V3 – min. 8 core – frequenza base 2,6Ghz	
Memoria del server di backup	Almeno 32Gbyte DDR4 ECC	
Controller Ethernet 10GBE	Almeno 2 porte 10Gigabit Ethernet dotate di SFP 10Gbase-SR LC.	

Controller Ethernet 1Gbit	Almeno 4 porte 1Gbit rame 1Gbase-T	
Porta e sistema di gestione via TCP-IP	Minimo: 1 porta Ethernet 1Gbit rame dedicata alla gestione del sistema da remoto anche a sistema operativo spento. Il sistema deve consentire: accesso KVM (Keyboard/video/mouse) con interfaccia remota, accesso al POST del sistema, al BIOS e installazione remota del sistema operativo attraverso l'utilizzo della redirezione di un installation media del client connesso.	Configurazione del sistema KVM remoto al fine di consentirne l'utilizzo immediato.
Controller disco di sistema	Controller SAS interno per dischi locali di sistema in grado di gestire almeno RAID-1.	Configurazione dei dischi del sistema operativo in RAID1
Unità a nastro	N.1 Drive Unit LTO-6. Tipologia: IBM, Quantum o HP, FH o HH. Interna al server o esterna (massimo 1 Rack unit).	Installazione e configurazione dell'unità sul server (se installato in fabbrica nel server l'installazione non è necessaria) e configurazione base del dispositivo, aggiornamento del firmware/patching.
Controller Tape per copia secondaria su nastro e retention di lungo periodo.	Controller SAS in grado di gestire il tape drive richiesto. Può corrispondere con il precedente controller SAS per i dischi di sistema, o essere fornito in aggiunta opzionalmente in base a criteri tecnici stabiliti dal fornitore.	
Controller dischi di backup	Controller SAS aggiuntivo dedicato con capacità di pilotare almeno 10 dischi SAS 15K o SSD. Supporto RAID 0,1,5,6. Tipologia minima: SAS 12Gbit/s.	Configurazione in RAID-6 dei dischi dati di backup.
Dischi di sistema operativo	Almeno N.2 dischi SAS 15K SFF o LFF. Dimensione minima: 144GB RAW. Funzionalità Hot-Swap attiva.	Dischi per installazione OS
Dischi dati di backup – copia primaria disk-based-backup	8 dischi 2TB oppure 12 dischi 1TB. Tipologia: NL-SAS SFF/SATA SFF su BUS SAS. Funzionalità Hot-Swap attiva.	Dischi per Backup repository
Sistema operativo	Microsoft Windows Server 2012R2 Standard – 1 CPU-Socket License	

Ambiente software di backup e relativi servizi richiesti.

Software richiesto	**Quantità e spefiche tecniche**	**Servizio richiesto per l'implementazione**
Veeam Backup & Replication Enterprise for Vmware Vsphere	Versione minima: V8. Licenza N. 4 CPU-Socket (2 Server biprocessori); opzioni richieste: • Veeam Explorer for Microsoft Active Directory • Veeam Explorer for	Installazione e configurazione del software per la realizzazione dell'ambiente di Backup Veeam; configurazione software del backup device; impostazione della protezione di tutte le virtual machine presenti, attraverso appropriati JOB di backup con tipologia e programmazione da

	Microsoft SQL • Opzione Veam Data Mover Service	definire in fase di redazione di progetto esecutivo di dettaglio. Minimo richiesto: 1 Job di backup Full + Incrementale su disco a bassa retention + 1 Job di backup FULL ciclico su nastro a retention elevata.

L'installazione, la configurazione e la messa in produzione dell'intera piattaforma di backup dovrebbe essere a cura del fonitore, come specificato nella precedente tabella.

4.2.4. STAZIONI ELABORATIVE UTENTE

Al fine di adeguare le stazioni PC utente a standard relativamente recenti si propone la seguente configurazione minima:

Sistema/Prodotto richiesto	**Quantità e spefiche tecniche**	**Servizio richiesto per l'implementazione**
PC nuovi, di marca primaria; con garanzia ufficiale del produttore di almeno 1 anno su tutti I componenti (da escludere PC assemblati su richiesta)	n.18 Stazioni utente (PC Desktop)	Installazione OS se non preinstallato; installazione applicazioni suite ufficio e sw minimo per produttività.
CPU	1 Intel Core i5/i7 frequenza base: minimo 3Ghz	
Memoria RAM	Almeno 4GB	
Hard disk	Almeno 1 HD 7200 rpm ~500GB	
Controller disco	SAS almeno 3Gbit/s	
Scheda di rete	Almeno 1 porta 1Gbit rame con Wake on LAN	
Porte USB	Almeno 2 frontali e Almeno 2 posteriori	
Accessori	Tastiera e mouse	
Sistema operativo	licenze Windows 8.1 Pro	
Pacchetto Office	Licenze Office 365 business (2 pc per C.A. e VMS senza Ms. Office)	

4.3. SICUREZZA E ACCESSIBILITÀ RICHIESTA

Per garantire la corrispondenza dell'infrastruttura prevista con le esigenze dell'ente, è di fondamentale importanza che i sistemi oggetto del presente studio consentano la gestione e l'amministrazione via rete attraverso protocolli di cifratura adeguati, tali da rispettare i criteri di sicurezza e la confidenzialità delle transazioni. Sarà necessario configurare ciascun servizio di gestione conformemente a tale requisito. Gli algoritmi di cifratura dovranno essere di ultima generazione, con chiavi di minimo 512bit, utilizzare sempre l'autenticazione asimmetrica con chiave pubblica + privata.

Al fine di garantire la massima sicurezza in termine di gestione dei sistemi, accesso ai dati per gli utenti, ed accesso alle applicazioni si richiede di suddividere la rete fisica in più partizioni logiche isolate, così da scongiurare sovrapposizione di flussi dati e di connessioni TCP/IP all'interno dello stesso segmento L2 e consentire a ciascuna area operativa l'accesso esclusivo alle proprie risorse.

La separazione logica della rete prevede almeno le seguenti aree di utilizzo attraverso il protocollo TCP-IP:

1. Gestione e amministrazione degli apparati di Storage System, Server fisici, telecamere videosorveglianza, sistemi di sicurezza fisica quali controllo accessi ed altri apparati fisici o automi. La rete è isolata e non deve effettuare routing verso l'esterno. Su tale rete è consentito l'atterraggio di una VPN di gestione configurata dal fornitore del sistema o al fornitore del supporto manutentivo ed evolutivo al fine di poter operare in emergenza da remoto, previa abilitazione del personale tecnico dell'aeroporto.
2. Gestione e amministrazione dei componenti di rete e firewall. LA rete è isolata e non deve effettuare routing verso altre reti. Su tale rete è consentito l'atterraggio di una VPN di gestione configurata dal fornitore al fine di operare in emergenza da remoto, previa abilitazione del personale tecnico dell'aeroporto.
3. Rete di gestione dell'Hyper-visor e di intercomunicazione Vsphere H.A. fra i nodi del cluster di risorse virtuali. La rete è routed e consentita solo da alcune postazioni di gestione definite all'interno dell'area aeroportuale. Tale rete è raggiungibile dalla VPN di servizio del fornitore del supporto.
4. Rete di accesso alle applicazioni aeroportuali. La rete è routed solo verso i client delle applicazioni specifiche.
5. Rete di dominio active directory per gli utenti dell'amministrazione aeroportuale e file-sharing. La rete è popolata dai client di back-office, dal NAS e dai domain controller, è ruotata verso le applicazioni che necessitano dell'autenticazione di dominio.
6. Rete dati sistema di videosorveglianza. La rete è isolata, non ruotata.

E' richiesto di configurare la separazione in VLAN su tutti gli apparati che saranno indicati dall'ente e di configurare il routing e le access-list necessarie a proteggere l'accesso delle risorse come minimo secondo lo schema indicato nel precedente punto elenco.

4.4. APPARATI DI RETE CED

Per l'attestazione dei server, dei sistemi virtuali (HyperVisor) e della rete di gestione del datacenter, si suggerisce necessario l'approvvigionamento di 2 switch di rete avanzati con adeguate prestazioni, funzionalità ed affidabilità, che saranno utilizzati come "Core" swtitch e datacenter core network.

Le caratteristiche mimine richieste dovrebbere essere:

Descrizione requisito	**Obiettivo**	**Dettaglio richiesto**
N. 2 Switch Ethernet con porte 10Gbit Fibra ed 1Gbit rame, ciascuno con le seguenti caratteristiche:	Due apparati per ridondanza globale	
Numero Porte 10GBE Fibra	Requisito per accesso rete	Almeno 4 porte attive 10Gbase-SR tutte dotate di sfp/sfp+ lc.
Numero Porte rame 1G	Requisito per accesso rete e uplink	Almeno 24 porte rame 1G-BaseT, 10/100/1000Mbit.
Supporto per Layer2 "single logical Object"	Requisito alta affidabilità	Sistema in grado di configurare 2 switch come fosse uno switch unico a livello Layer2 ed a livello Routing (Layer3). Con la possibilità di effettuare "Cross stack port-channels", ovvero di attestare un host ad entrambi gli switch e configurare una connessione LACP attiva su entrambi gli chassis, così da bilanciare il traffico Ethernet e garantire l'HA in caso di fail di uno switch fisico.
IP Routing attivo	Requisito per trasferimento dati su rete logica CED e applicazioni virtualizzate	"Layer3 license" attiva, con supporto Access-List e interVLAN routing.
Supporto per "Port-channel" / "Etherchannel"	Requisito per conformità alla soluzione tecnica, garanzia di ridondanza e continuità del servizio / bilanciamento dati.	LACP, PAGP, Trunk.
Supporto VLAN	Requisito conformità alla soluzione tencnica.	Supporto VLAN, InterVLAN Routing, 802.1Q Vlan Tagging e trunking su port-channel / logical channel.
Ampiezza di banda complessiva dello switch	Prestazione richiesta	120Gbit/s
Gestione tabella mac address	Prestazione richiesta	Almeno 16.000 mac address.
Numero frame/pacchetti al secondo switched	Prestazione richiesta	Minimo: 90 Milioni / Sec.

Latenza	Prestazione minima richiesta	Latenza massima “cut-through” o “store & forward”: 1,5 microsecondi.
Buffer porte di rete	Prestazione richiesta	Min. 1,5Mbyte
Supporto Jumbo Frames	Dettaglio tecnico richiesto	Sì: 9216 Bytes per frame.
Supporto QOS	Dettaglio tecnico richiesto	Supporto per traffic shaping, QoS e packet queuing.
Altre caratteristiche richieste	Dettagli tecnici necessari	Spanning Tree; IGMP
Supporto Virtual Router	Dettaglio tecnico richiesto	Supporto per virtual router, gestito da tutti i membri dello stack, con possibilità di failover automatico del virtual IP in caso di guasto all’apparato che effettua attivamente routing nello stack stesso.

4.4.1. FIREWALL AZIENDALE

Al fine di supportare la sicurezza perimetrale (Internet, DMZ, infranet) dei sistemi informatici con un prodotto di nuova generazione dotato di opportuno supporto, aggiornamenti delle definizioni e dei criteri di sicurezza ecc.; si richiede di implementare un firewall di livello enterprise, di fascia medio-bassa in termini di performance, adeguato alle prestazioni della rete internet o della connettività fra SILOS applicativi dei diversi fornitori o tenant. Il firewall dovrà essere coperto da adeguato contratto di supporto. Si suggerisce di implementare un Firewall in modalità Physical appliance al fine di rendere l’oggetto indipendente dall’ambiente virtuale e destinabile a tutti gli ambienti aeroportuali, sia fisici sia virtuali. La tipologia dovrà essere di tipo Unified Threat Management (UTM) ovvero gestione unificata delle minacce, che include Intrusion Detection, Antivirus, Antispam e firewalling standard.

Descrizione requisito	**Obiettivo**	**Dettaglio richiesto**
N. 1 Firewall Unified Threat Management	Sistema di livello enterprise fascia performance medio-bassa con supporto UTM	
Numero Porte 1GBE RAME	Requisito per accesso rete firewall e processing UTM	Almeno 6 porte attive utilizzabili per servizi UTM tipologia 1GBase-T
Numero Porte di gestione ethernet rame	Requisito per gestione via rete del firewall	Almeno 1 porta
Velocità max firewall	Supporto performance su rete gigabit ethernet interna, Internet, Infranet e DMZ.	Minimo 2 Gbit/sec
Velocità massima VPN AES128	Supporto performance VPN per collegamenti remoti o da altri fornitori / tenant	Almeno 200Mbit/sec con protocollodi cifratura AES 128

Velocità Massima Antivirus	Supporto performance Antivirus per scanzione on-line	1,5 Gbit/sec
Velocità massima IPS	Supporto performance Intrusion Prevention System - prevenzione degli attacchi/minacce; online scan speed	1,6 Gbit/sec
Velocità massima aggregata di tutti i servizi di scansione unificata – Unified Threat Management	Supporto performance aggregate IDS, IPS, AV, ANTISPAM, Firewall ecc. – livello di banda media supportata.	Almeno 800Mbit/sec
Supporto client/host locali	Supporto per numero PC, Server o device TCP-IP nella rete	Illimitato
Sessioni simultanee TCP-IP	Supporto per numero di sessioni TCP-IP simultanee gestite dal firewall nei confronti dei client, server, processi e device interni della rete fisica e virtuale, incluse le applicazioni.	Minimo 40.000
Velocità di creazione di creazione di connesisoni TCP-IP	Supporto per la creazione di nuove connessioni TCP-IP nell'unità di tempo.	Minimo 20.000 al secondo.
Supporto protocolli di trasporto	""	VLAN Tagging, Bridging (access mode)
Numero massimo di utenti locali definibili per autenticazione interna firewall	Supporto per coppie username/password gestite localmente all'interno del firewall stesso.	500
Utenti VPN mobili	Supporto simultaneo per utenti mobili, teleworkers, teleassistenza, clienti / fornitori e tenant.	60 Remote office. 70 Utenti Mobili, 60 utenti via tunnel SSL.
Supporto autenticazione integrata Active Directory	Possibilità di autenticare gli utenti attraverso il database con utenze (coppie username/password) illimitate via LDAP con pass-through Authentication ed automatic Single-Sign-On Active Directory integrated.	Sì Obbligatorio.
Caratteristiche Firewall incluse	Caratteristiche di sicurezza standard Firewall	Stateful packet inspection, deep application inspection, firewall proxy
Caratteristica Proxy Server	Caratteristiche di funzionamento del proxy – protocolli supportati.	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3
Protezione dalle minacce standard	Supporto per tipologia di minacce note gestite dal firewall in ingresso	Anti-spyware, attacchi DoS, pacchetti frammentati e malformati, minacce miste, Java Applet,

	/ uscita.	ActiveX.
Supporto protezione VOIP	Supporto per la protezione delle connessioni Voice Over IP per la telefonia digitale	Si, obbligatorio.
Supporto gestione minacce avanzate	Supporto per la protezione completa da minacce con rilevazione euristica e statistica.	Application Control, Gateway AntiVirus, Reputation Enabled Defense,WebBlocker, spamBlocker, Intrusion Prevention Service
Supporto L2TP/PPTP/SSL	Supporto per le tipologie standard i incapsulamento dei protocolli di trasporto nelle connessioni punto punto.	S,i Obbligatorio.
Protocolli di cifratura supportati	Supporto ai protocolli di sicurezza standard e a chiave forte.	DES, 3DES, AES a 128, 192 e 256 bit, IPSec SHA-1, MD5, codice precondiviso IKE, Supporto autorità di certificazione esterna.
Tipi di autenticazione supportati	Supporto per varie tipologie di autenticazione standard di mercato.	Radius, LDAP, Windows Active Directory, Autenticazioni utente VASCO, RSA SecurID, e web based auth.
Reporting	Supporto per Reporting sugli attacchi rilevati, le connessioni o gli indirizzi bloccati, il livello di sicurezza ecc.	Sì. Obbligatorio.
Interfaccia di gestione	Supporto per la tipologia di interfacce di gestione dell'apparato.	Minimo richiesto: Web Interface e Command Line Interface con funzionalità complete di configurazione e gestione.
Quality Of Service	Supporto per l'assegnazione di priorità al traffico con maggiore impatto sul business e sfruttamento ottimale delle linee internet (previene disservizi)	8 code di priorità, DiffServ, coda rigorosa modificata
Modalità di assegnazione inidirizzi di rete	Supporto per l'autoconfigurazione dei client di rete (PC e Device)	Statica, DynDNS, PPPoE, DHCP (server, client, relay)
Certificazioni minime richieste	Certificazioni minime rilasciate da enti preposti al rispetto dei criteri di sicurezza informatica e fisica.	ICSA Firewall, ICSA VPN, EAL4+, FIPS 140-2, NRTL/C, CB, RAEE, RoHS, REACH.

4.4.2. REQUISITI MINIMI DI CONNETTIVITA' NEL DATACENTER

Si richiede di realizzare la configurazione della rete di CED secondo i seguenti necessari criteri:

4.4.2.1. RETI DI CLUSTERING:

Si definiscono 2 tipi di reti di clustering, che si rende necessario configurare nell'infrastruttura di sistema oggetto del presente studio e sulla rete preesistente oggetto dell'espansione, laddove vi sia interazione:

- Rete di clustering di Guest OS (Sistemi operativi virtualizzati). La rete di clustering fra sistemi operativi virtuali sarà realizzata attraverso 2 VLAN minimo: 1 di intercluster communications, dedicata e isolata, più una rete pubblica di accesso client che potrà supportare le comunicazioni intercluster fra i nodi in caso di "fail" della rete dedicata.
- Rete di clustering HA di Vmware VSphere: per tale rete di clustering si prevede almeno 1 VLAN.

4.4.2.2. RETE INTERNA DI BACKUP:

Per il trasferimento dati tra il sistema di Backup e gli Host ESX / Virtual Machine / Host fisici è richiesto l'utilizzo di un segmento a 10GBE. Laddove possibile in base ai requisiti applicativi si rende necessario dedicare una VLAN al Backup.

Si richiede di trasportare la VLAN di backup e tutte le VLAN applicative che richiedono il servizio di backup attraverso trunk/link ridondati/bilanciati (es. LACP/Etherchannel ecc.) che prevedano connessioni "Cross-stack port-channel" verso gli switch di datacenter forniti.

A tale proposito si dovrà garantire per il sistema di backup, ed in genere per l'accesso ai dati fra apparati interni al datacenter, che l'accesso alla rete di tutti i sistemi virtuali NON sia interrotto in caso di "guasto" imprevisto ad uno degli switch ethernet 10G di CED forniti. A tale scopo dovrebbe essere onere del fornitore stesso di configurare gli switch forniti come una unica entità logica Layer2.

4.4.2.3. ACCESSO A INTERNET:

L'accesso a internet dovrà essere garantito a diverse VLAN anche se isolate fra loro. Se richiesto, il firewall dovrà consentire la segmentazione della rete effettuando il routing delle VLAN stabilite, con diverse subnet IP in modo tale da consentire il traffico dati fra loro attraverso ACL ed ispezione del traffico TCP/IP.

4.4.2.4. RETI DEDICATE FORNITORI DI APPLICAZIONI AEROPORTUALI

Per il trattamento di reti che necessitino di isolamento per motivi di sicurezza, la definizione dei segmenti relativi si rimanda alle raccomandazioni dei fornitori di applicazioni aeroportuali.

Ad ogni modo, data la compatibilità dei sistemi richiesti con gli standard VLAN e 802.1Q VLan tagging, sarà possibile separare o collegare in qualsiasi momento le reti applicative aeroportuali alle reti di dominio active directory o a Internet.

4.4.2.5. VERIFICA E ADEGUAMENTO DELLA RETE FISICA

Per sanare l'attuale indeterminatezza dello stato elettrico della rete fisica (cablaggi rame e fibra ecc.), si rende necessaria un'attività di certificazione delle tratte. Il risulatato sarà la misura del disturbo su ciascuna tratta e la rilevazione di relative eventuali violazioni delle specifiche Ethernet. I cablaggi errati comportano abbassamento della velocità di trasferimento dati, errori di trasmissione, possibile instabilità dei link con pregiudizio alle applicazioni e servizi che ne fanno uso ecc. Al termine delle misurazioni, sarà possibile comprendere le azioni necessarie per risolvere i relativi problemi di connessione, come ad esempio effettuare un cablaggio più adeguato, eventualmente adeguato ai più recenti standard di trasmissione dati.

4.5. INFRASTRUTTURE SPECIALI

Formattato: SpazioPrima: 1,2 linea

Il presente capitolo descrive alcune infrastrutture specifiche, a nostro avviso di fondamentale importanza in termini di sicurezza e di gestione e che, a livello di infrastruttura elaborativa, possono essere incluse nel modello architetturale suggerito.

4.5.1. ACCESSO AI VARCHI E ALLE AREE PROTETTE

Formattato: SpazioPrima: 1,2 linea, Dopo: 0,6 linea

Formattato: SpazioPrima: 1,2 linea

Per gestire l'accesso ai varchi protetti, superando le forti limitazioni della metodologia attuale, già citate nel presente documento, si suggerisce l'implementazione di un sistema di controllo accessi informatizzato, dotato come minimo delle seguenti caratteristiche minime. Il sistema, a livello della componente server (database degli accessi e delle autorizzazioni ecc.), dovrà essere virtualizzato e dunque deve supportare l'esecuzione in ambiente virtuale, certificata dal produttore.

In base alle esigenze rilevate dall'analisi della planimetria, sono state individuati i seguenti requisiti per il sistema di controllo accessi:

Requisito	Numero e/o dettagli	Obiettivo / Ruolo
Virtual Machine Server con almeno 2-4 VCPU – 6 GB RAM – 40GB spazio disco disponibile.	1	Server di raccolta dati accesso e configurazioni di sicurezza.
Terminale di controllo accessi per la gestione di 1 varco bidirezionale o 2 varchi monodirezionali,	16	Identificazione, autenticazione, verifica dell'autorizzazione e concessione / negazione dell'accesso.
Terminale di controllo accessi con connessione TCP-IP per scaricamento dati al server in almeno 1 posizione (proxy).	1	Identificazione, autenticazione, verifica dell'autorizzazione e concessione / negazione dell'accesso. Interfacciamento infrastruttura di C.A. su cavo bus con rete lan TCP/IP
Sensori smart-card installabili presso ciascun varco.	32	Lettore di tessere di riconoscimento
Software centrale con database di controllo accessi, con registrazioni degli accessi, configurazione del personale consentito e relativi orari, aree consentite ecc. Gestione della visualizzazione dello storico e dello stato attuale, allarmistica automatica remota. Gestione di 20 terminali.	1	Sistema centrale di gestione accessi.

Licenza per l'integrazione con software di supervisione terze parti.	1	Integrazione software di supervisione
Installazione e configurazione di terminali e sensori, collegamento al bus, installazione e configurazione del server di C.A. (infrastruttura CED) e del client di C.A.(Control Room)	1	Rilascio in produzione di tutto il sistema.

Formattato: SpazioPrima: 1,2 linea

Accanto al sistema di controllo accessi, un sistema anti-intrusione è fondamentale per garantire la sicurezza dell'aeroporto anche dal punto di vista della sicurezza da aggressioni esterne. Si suggerisce di dotarsi minimo dei seguenti componenti:

Requisito	**Numero**	**Obiettivo / Ruolo**
Centrale di allarme, almeno 8 zone e 4 uscite con batteria tampone inclusa.	1	Sistema centrale di antintrusione
Fornitura e configurazione della scheda ethernet per la comunicazione con il software di gestione della videosorveglianza	1	Integrazione con SW di supervisione
Tastiera	1	Configurazione ed inserimento di codici di blocco e sblocco
Batterie per il funzionamento e per autonomia elettrica della centrale	1	Autonomia e sicurezza elettrica
Sirena da esterno comprensiva di batteria	2	Segnalazione ottico acustica
Contatti magnetici per controllo effrazione con **grado di sicurezza 3**	11	Rilevamento intrusioni
Modulo di ingresso/uscita per il collegamento dei dispositivi in campo con il bus	3	Collegamento sensori
Installazione del sistema e messa in funzione	1	Rilascio in produzione di tutto il sistema

Formattato: SpazioPrima: 1,2 linea

4.5.2. SISTEMA DI VIDEOSORVEGLIANZA

Formattato: SpazioPrima: 1,2 linea, Dopo: 0,6 linea

Formattato: SpazioPrima: 1,2 linea

Al fine di ottenere un servizio di videosorveglianza efficace ed adeguato alle esigenze dell'aeroporto, si suggerisce l'implementazione di un sistema di videosorveglianza digitale, dotato come minimo delle seguenti caratteristiche minime. Il sistema, a livello della componente server (Sistema di registrazione in tempo reale delle immagini, gestione telecamere, configurazione ecc.), dovrà essere virtualizzato e dunque deve supportare l'esecuzione in ambiente virtuale, certificata dal produttore.

Per mantenere memorizzata 1 settimana di storico di registrazioni digitali delle telecamere previste, in alta risoluzione, sono necessari 3 TB di spazio sul sistema di storage, già previsti nel dimensionamento complessivo.

In base alle esigenze rilevate dall'analisi della planimetria, sono state individuati i seguenti requisiti per il sistema di videosorveglianza (VMS – Video Management System):

Requisito	**Numero e/o dettagli**	**Obiettivo / Ruolo**
Virtual Machine Server con almeno 4 VCPU – 8 GB RAM – 20GB spazio disco disponibile localmente + 3TB di spazio sul sistema di storage sottostante (inclusi nei requisiti dello storage system).	1	Server di registrazione in tempo reale e memorizzazione delle videoregistrazioni VMS.
Telecamera fissa da interno. Risoluzione 1080p30, Giorno / notte ottimizzata, obiettivo con focale variabile, Luminosità minima 0,25 lx (color) e 0.05 lx (B/W), WDR minimo 70 dB Correzione ad infrarossi, compressione H264, DNR, antinebbia, Motion detection, supporto criptatura SSL 128 bit, ONVIF conformant, supporto dei protocolli DNS e FTP su allarme, disponibilità di contatti di ingresso e uscita, ingresso ed uscita audio, slot per registrazione su memory card SDHC/SDXC o su NAS iSCSI/VRM, porta ethernet RJ45, uscita analogica in simultanea a segnale IP. Alimentazione 12 VDC o PoE.	18	Telecamera fissa da interno
Telecamera fissa dome da esterno con le stesse caratteristiche di quella da interno ma alloggiata all'interno di una custodia a cupola. Custodia in alluminio grigio ad apertura laterale con viti antimanomissione, vetrino ad alta risoluzione termostatato, binario interno rimovibile in grado di alloggiare una telecamera fino a 91 x 81 x 262 mm, custodia termostata e ventilata con range di temperatura fino a -40°C/+50°C, grado di protezione IP66, Illuminatore IR integrato, passaggio cavi attraverso connettori posteriori, staffa, alimentazione 24 VAC 2 A con convertitore AC/DC per telecamere IP.	3	Telecamera fissa da esterno

Software centrale con sistema di videoregistrazione, memorizzazione remota delle registrazioni, configurazione delle telecamere, esportazione delle registrazioni, configurazione dei flussi video. Supporto minimo di 60 telecamere per server. Illimitato numero di utenti, gestione allarmi, supporto di integrazione con applicazioni di terze parti, privacy masking, supporto mappe interattive, Licenze per gestire le telecamere installate.	1	Sistema centrale di gestione videosorveglianza.
Installazione delle telecamere, cablaggio locale, installazione e configurazione del server VMS e del client VMS.	1	Rilascio in produzione di tutto il sistema.
Control Room • n.1 Workstation con 1 Intel Core i5/i7 minimo 2,6Ghz - 4GB - 1 HD 7200 rpm ~500GB SAS almeno 3Gbit/s - 1 porta 1Gbit rame con Wake on LAN - 2 USB frontali e 2 posteriori – Scheda grafica con 2GB di RAM dedicati, Tastiera e mouse e monitor. Licenza Windows 8.1 Pro • n. 1 videowall con tecnologia a LED da almeno 50” - LED , Luminosità: 500 cd/m2; Contrasto: 3500:1, Angolo di Visuale (V/H): 178°/178°, Tempo di Risposta: 8ms, Video Input: D-Sub, HDMI1, HDMI2, DVI-D (Loop-out), CVBS, HDMI 1, HDMI 2, , Stereo mini Jack. Output: Stereo mini Jack, , Controllo Remoto; 1xRS232C (IN/OUT), 1x RJ45.Telecomando incluso, Anti-image retention, Controllo automatico della temperatura (Sensore), , Wall Mounting&Portrait (tipo VESA). Adatto per un utilizzo prolungato (tipo H24). • n.2 monitor con tecnologia a LED da almeno 23”, luminosità 250 cd/mq, contrasto std 1000:1, interfacce HDMI, VGA, altoparlanti integrati.	1	Control Room

Formattato: SpazioPrima: 1,2 linea, Dopo: 0,6 linea

4.5.3. SISTEMA DI RICONCILIAZIONE BAGAGLI

Formattato: Non Evidenziato

Qualora si desideri garantire il funzionamento del sistema di riconciliazione bagagli è necessario prescindere da connessioni dirette fra gli access point installati all’esterno dell’edificio aeroportuale e i dispositivi wireless a bordo pista, vista la problematica delle interferenze fisiche degli aeromobili.

Si suggerisce di realizzare dunque un sistema di conciliazione bagagli che prescinda dall’utilizzo della rete Wi-Fi (wireless standard IEEE 802.11x), ma che sfrutti nuovi tipi device di scansione basati sulle tecnologie “IoT” (Internet of Things), tipicamente poggianti su connessioni dati cellulari per la ricezione e la trasmissione dei dati, es.:

1. Utilizzo di scanner ottici bar-code portatili con memoria interna per l'identificazione dei bagagli, invio istantaneo delle informazioni di identificazione ai sistemi di riconciliazione via rete dati cellulare, ottenendo copertura rete quasi completa in aree aperte.
2. L'accesso al server di riconciliazione da parte dei barcode scanner portatili può venire effettuato posizionandolo in ascolto su un indirizzo IP pubblico sulla rete internet.
3. Dismissone degli Access-point obsoleti, con software ormai potenzialmente debole, ed attaccabile tramite i più modeni exploit informatici come il "furto" delle credenziali d'accesso o gli attacchi all'automazione Wi-fi PSK.

4.6. DOCUMENTAZIONE TECNICA – NOTA OPERATIVA (SUGGERIMENTO REQUISITI PER SVOLGERE L'ATTIVITÀ)

Prima dell'eventuale inizio lavori si rende necessaria la preparazione di un documento di progetto esecutivo nel quale saranno indicati dettagliatamente modalità, processi e tempi per la configurazione dell'intera soluzione di datacenter, conformemente alle regole generali indicate in tale studio tecnico. Il documento dovrebbe contenere almeno le seguenti indicazioni:

1. Indicazione delle fasi di progetto e tempi richiesti per ciascuna fase tramite cronoprogramma delle attività. Per ciascuna attività sarà indicato il tipo ed il numero di profili tecnici impiegati, in particolare sarà specificata la qualifica e la certificazione delle risorse impegnate.
2. Redazione di un GANTT di progetto con dettaglio almeno alle fasi del cronoprogramma.
3. Indicazione dei sistemi, sottosistemi e funzioni che saranno oggetto della configurazione.
4. Indicazione stimata della suddivisione dello spazio di storage e dei dischi logici dei sistemi operativi che si prevede di implementare per una configurazione ottimale dell'ambiente operativo.
5. Indicazione delle procedure e relative modalità di configurazione impiegate per la realizzazione del progetto.
6. Indicazione del supporto necessario che il personale dell'aeroporto dovrà fornire per ciascuna microattività, compresi i tempi di impegno del personale aeroportuale in giornate uomo.

Al termine delle attività di implementazione, le attività saranno soggette ad un collaudo esecutivo, che sarà elaborato dall'amministrazione al fine di verificare la corrispondenza delle opere effettuate alle richieste.

Una volta approvato con successo il collaudo esecutivo, dovrebbe essere prodotto un documento tecnico di rilascio, che dovrà contenere una descrizione dettagliata della configurazione di tutti i sistemi rilasciati in produzione.

4.7. STRUMENTI DI GESTIONE, CONTROLLO E MONITORAGGIO

Gli strumenti di gestione e controllo prevedono, come minimo la gestibilità dei seguenti sistemi, che dovrà essere garantita:

1. Server fisici; Attraverso interfaccia di management remote KVM dedicata.
2. Storage System; attraverso interfaccia di gestione dedicata oppure in condivisione di interfaccia con porte dati utilizzando il software previsto dal produttore dello storage system, le cui funzionalità sono integrate nel microcodice.
3. VMware VSphere Hypervisor web interface (VCenter), sulla rete di gestione di VSphere
4. Windows Server 2012R2 e Active directory via RDP
5. Server applicativi, via RDP con chiave a 512-1024bit per Microsoft Windows Server o via SSH/OpenSSL per LINUX + relative interfacce applicative una volta effettuato il log-on via rete.
6. Sistemi di rete e Firewall tramite interfacce di gestione con protocolli di cifratura della sessione/connessione attivi.
7. Tutte le connessioni verso i software di gestione che utilizzino come client un Browser internet, ovvero siano consultabili via "web interface", dovranno utilizzare il protocollo HTTPS/SSL.

A livello di monitoraggio dei sistemi, sarà necessario fornire un software di monitoring per ciascuna delle seguenti piattaforme:

1. Storage system (se non già incluso nella fornitura storage un sw di monitoring specifico)
2. Vmware VSphere (se non si intende configurare gli strumenti di monitoraggio già inclusi nella fornitura richiesta)
3. Server fisici (se non già incluso nell'offerta del produttore di server richiesta in fornitura un sw di monitoraggio specifico).
4. Rete – In tal caso il fornitore dovrebbe prevedere un sistema di monitoraggio della rete con le seguenti caratteristiche:
    a. Monitoraggio dello stato "alive" dei server Windows / Linux e dei client Windows
    b. Monitoraggio dei principali application server quali IIS, TOMCAT, Jboss.
    c. Monitoraggio dei principali database quali SQL Server, Oracle, PostGres, Mysql.
    d. Monitoraggio degli apparati di rete Cisco ed HP, produttori già presenti nella rete dell'aeroporto; in tal caso dovrà essere possibile monitorare passivamente tramite Syslog ed SNMP tutti gli eventi relativi a criticità hardware, di configurazione, software (come spanning tree events) e di sicurezza.
2. Firewall – il sistema di monitoraggio del firewall fornito dovrebbe corrispondere alle caratteristiche tecniche elencate nella rispettiva tabella del presente capitolato.

Tutti i sistemi di monitoraggio dovranno avere le seguenti carattistiche minime:

1. Registrazione di tutti gli eventi configurati, possibilità di esportare il database degli eventi per effettuarne il salvataggio.
2. Invio automatico di allarmi sotto forma di email a destinatari multipli configurabili, solo in caso di ricezione di eventi critici.

Il sistema di monitoraggio fornito per la gestione della rete dovrà avere le seguenti funzionalità di allarmistica:

1. Registrazione di tutti gli eventi in base alle categorie configurate, possibilità di esportare il database degli eventi per effettuarne il salvataggio.
2. Possibilità di categorizzare gli eventi e prioritizzare singoli eventi o gruppi di eventi.
3. Possibilità di scartare automaticamente tramite policy eventi irrilevanti, definiti tramite policy secondo espressioni regolari e/o algoritmi di intelligenza artificiale.
4. Invio automatico di allarmi sotto forma di email a destinatari multipli configurabili, in caso di ricezione di eventi critici, con soglie di criticità definibili.
5. Possibilità di effettuare analisi storiche secondo criteri flessibili, espressioni regolari o query, con dettaglio al singolo evento, ai gruppi o categorie.

4.8. ADDESTRAMENTO DEL PERSONALE

Al fine di ottenere una visione di dominio dell'architettura di datacenter realizzata, l'amministrazione dovrebbe richiedere la possibilità di detenere il controllo dell'infrastruttura informatica.

A tale scopo sarà necesario fornire ai soggetti indicati dall'amministrazione un adeguato addestramento sulla configurazione dei sistemi implementata.

Le sessioni di training saranno organizzate come segue:

1. **Briefing.** Sarà effettuata una sessione di formazione sull'architettura generale implementata, con particolare riferimento alla corrispondenza fra servizi e applicazioni erogati dall'aeroporto e la collocazione della rispettiva piattaforma e componenti hardware e software sottostanti.
2. **Training on the job**. Durante le fasi di installazione e configurazione dei sistemi, I soggetti nominati dall'amministrazione seguiranno il personale del fornitore nelle attività sul campo.
3. **Addestramento in aula**. Al termine della configurazione dell'infrastruttura saranno richieste alcune giornate di addestramento in aula sull'utilizzo dei sistemi rilasciati.
4. **Visibilità della documentazione di rilascio**.

4.8.1. ARGOMENTI DEL TRAINING

Tipicamente i seguenti argomenti devono essere affrontati:

1. **Hypervisor.** Configurazione dell'ambiente virtuale, HA, DRS, reti virtuali, guest OS in cluster e configurazione templates.
2. **Storage System.** Configurazione dello storage: Raid groups e storage pools, autotiering se previsto, LUN, volumi, masking e storage efficiency.
3. **Rete.** Configurazione architetturale, configurazione apparati, Topologia della rete, VLAN, routing e Firewalling.
4. **Backup System**. Configurazione dell'architettura server e backup device, host interessati e modalità, software di backup, Jobs e policies.

4.9. CRONOPROGRAMMA DELLE ATTIVITA' DI PROGETTO

Lo schema del cronopronogramma che il fornitore dovrebbe erogare deve rispettare almeno le seguenti fasi:

- ***ASSESMENT DETTAGLIATO (XX giorni di elapsed – XX Giorni lavoro)***
  - ✓ …
  - ✓ …..
- ***PROJECT DESIGN (XX giorni di elapsed – XX Giorni lavoro)***
  - ✓ …..
  - ✓ Scrittura progetto esecutivo
- ***IMPLEMENTAZIONE (XX giorni di elapsed – XX Giorni lavoro) –indicare giorni/uomo per ogni sotto-attività.***
  - ✓ Site preparation
  - ✓ Configurazione Storage
  - ✓ Configurazione Server
  - ✓ Configurazione Network, trunks, bilanciamento, VLAN, routing e sicurezza interna / internet.
  - ✓ HyperVisor - installazione e configurazione
  - ✓ Setup della virtual infrastructure & creazione dei template e virtual server.
  - ✓ Configurazione e Tuning del profilo a gestione utente in ambito NAS, Active directory GPOs.
  - ✓ Definizione delle access policies
  - ✓ Definizione del modello di Security in ambiente Server e rete
  - ✓ Importazione / migrazione nel nuovo ambiente virtuale di tutti i sistemi preesistenti previsti del server Oracle.
  - ~~✓ Installazione dei server Oracle (OS).~~
  - ✓ Proposta modello di verbale collaudo
- ***CONSEGNA DELLA DOCUMENTAZIONE FINALE (XX giorni di elapsed – XX Giorni lavoro)***
- ***TRAINING – preparazione e consegna documentazione di training (XX giorni di elapsed – XX Giorni lavoro)***

4.10. COMPONENTI E VALORI DELLA SOLUZIONE DI DATACENTER E RETE

(Specificato in modo approssimativo il valore dei costi per ogni blocco).

Lista dei componenti necessari con prezzo medio di mercato approssimativo:

4.10.1. DATACENTER E IMPIANTI SPECIALI

IMPIANTO	TIPO	PRODOTTO	BASE D'ASTA
ICT	HW/SW	Storage System	€ 44.800,00
	HW/SW	Elaboratori VSphere	€ 19.500,00
	HW/SW	Sistema di backup	€ 18.500,00
	HW/SW	Apparati di rete	€ 9.500,00
	HW/SW	Apparati di fabric	€ 6.800,00
	HW/SW	Firewall con Unified Threat Management	€ 2.550,00
	HW/SW	Licenze vmware VSphere	€ 4.300,00
	HW/SW	Licenze Windows Server (DataCenter ed Std)	€ 9.370,00
	~~HW/SW~~	~~Licenze Oracle~~	~~€ 900,00~~
		Porting server fisico Oracle su Infrastruttura Virtuale	€ 900,00
	HW/SW	Licenze Software di Backup Veeam	€ 1.390,00
	Servizi	Installazione e configurazione HW e SW Datacenter	€ 24.000,00
			€ 141.610,00
TVCC	HW/SW	Sistema di videosorveglianza	€ 24.950,00
	Servizi	Installazione e configurazione HW e SW sistema di videosorveglianza	€ 6.900,00
			€ 31.850,00
C.A.	HW/SW	Sistema controllo accessi	€ 12.400,00
	Servizi	Installazione e configurazione HW e SW sistema di controllo accessi	€ 2.400,00
			€ 14.800,00
A.I.	HW/SW	Sistema anti-intrusione	€ 3.700,00
	Servizi	Installazione e configurazione HW e SW sistema di anti-intrusione	€ 1.850,00
			€ 5.550,00
		TOTALE	**€ 193.810,00**

Tabella formattata

NOTE:

La presente proposta prevede:

- L'utilizzo di componenti di rete ad alte prestazioni (10Gigabit Ethernet) ed alta affidabilità (doppio switch di livello medium-business con ridondanza / tolleranza trasparente al guasto di uno switch).
- Una soluzione di backup che consenta il salvataggio locale dei dati ad elevate prestazioni più il salvataggio storico dei dati di lungo termine (con recupero di lungo termine) e protezione remota dei dati tramite possibilità di esportazione dei supporti di backup presso altro luogo. Connessioni di rete ad alta velocità bilanciate (10 Gigabit Ethernet).
- Una soluzione di Elaboratori ad alta capacità di memoria per consentire l'ospitalità di più risorse elaborative per i sistemi operativi virtuali e scorta per espansione. Connessioni di rete ad alta velocità bilanciate (10 Gigabit Ethernet).

4.10.2. PERSONAL COMPUTER UTENTI - SIMULAZIONE STANDARD

TIPO	PRODOTTO	BASE D'ASTA	
HW/SW	PC con sistema operativo e Office (escluso monitor)	€	670,00
Servizi	Installazione e configurazione HW e SW PC	€	100,00
	Prezzo Unitario	**€**	**770,00**
	Prezzo Totale per 18 PC	**€**	**13.860,00**

4.10.3. ESCLUSIONI

Di seguito sono riportate le attività e gli apparati esclusi dall'importo indicato nel precedente paragrafo:

- Opere di fabbro, falegname, muratore, verniciatore, elettricista.
- Disponibilità di alimentazione elettrica
- Impianto di illuminazione e suppellettili.
- Impianto videosorveglianza, controllo accessi e antintrusione:
  - Fornitura e stesura del cavo dati/bus e di alimentazione elettrica
  - Realizzazione di nuove canalizzazioni