BRESCIA MOBILITA'

Allegato B

"UPGRADE SBE"

(SISTEMA DI BIGLIETTAZIONE ELETTRONICA)

PER I SERVIZI DI TPL DI AREA URBANA

DEL BACINO DI BRESCIA

Prescrizioni IT

all'integrazione con l'infrastruttura di gruppo

		Rev:	A	Data emissione:	10/03/2016

	Nome	Ente	Responsabile	Firma	Data

Controllato	S. Pace	TR	Responsabile tecnico		11/03/2016
Approvato	G. Marinoni	TR	Responsabile di Progetto		11/3/2016

REVISIONI

Rev.	Data	Autore/i	Firma	Descrizione
A	10/03/2016	E. Scarpazza		Prima Stesura

INDICE

1. Premessa

Il presente documento intende fornire gli elementi tecnici e normativi affinché sia possibile integrare il sistema di bigliettazione elettronica (S.B.E.) all'interno della infrastruttura "private cloud" del Gruppo Brescia Mobilità (BSM).
Il fornitore dovrà pertanto, in intesa con i dipartimenti tecnologici del Gruppo e a recepimento delle disposizioni di legge italiane, predisporre un progetto di fornitura del sistema di bigliettazione elettronica in grado di armonizzarsi alle policy adottate dal Gruppo che sia dotato di modalità di funzionamento e gestione che permettano il conseguimento della certificazione ISO 27001.

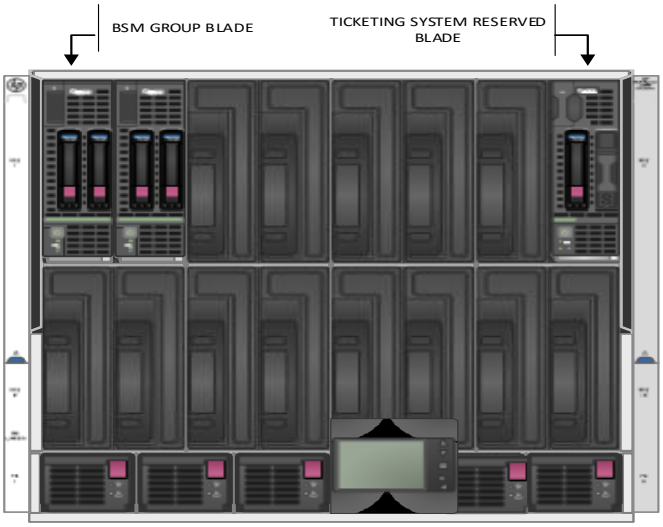
2. Hardware

2.1 Infrastruttura Attuale del Gruppo

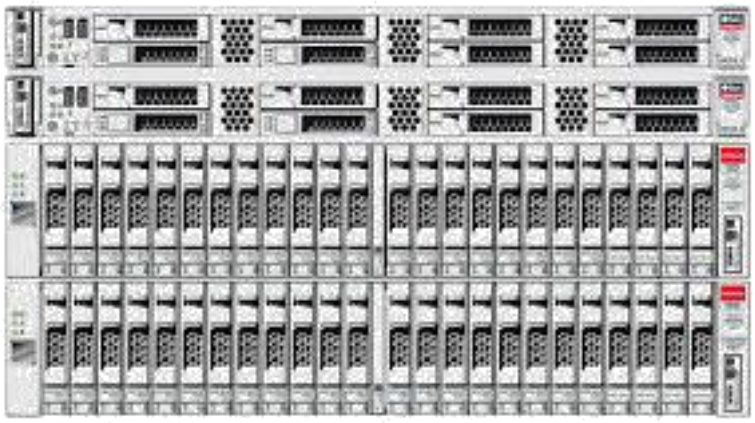
L'attuale infrastruttura costituisce un sistema "private cloud" composto da due nodi geografici+1 collegati in anello ridondato a 10GB, dove il terzo nodo è specializzato nella gestione del controllo del failover dei due nodi di sistema.
I due nodi geografici, realizzati secondo specifiche di Business Continuity e di Disaster Recovery, sono dotati di gruppo di continuità statico (UPS) e da motogeneratore che ne garantiscono la continuità di funzionamento in caso di blackout. La loro operatività, attiva-attiva, è garantita dall'aggregazione di due ulteriori link a 10Gb realizzati su percorsi diversi. L'impiego della tecnologia blade associata a quella virtuale (vmware®) ne garantisce la scalabilità per eventuali sviluppi ed evoluzioni.
Ogni singolo nodo prevede l'impiego di un Blade System Enclosure che mette in collegamento le singole blade con le SAN tramite interfacce virtul connect a 10GB. La ridondanza delle interfacce del System Blade e delle SAN garantisce la funzione di High availability

2.2 Modifica Infrastruttura – Integrazione SBE

Allo SBE, e relativi servizi, si prevede di assegnare un server blade dedicato implementandolo nell'enclosure di ogni nodo dell'infrastruttura del Gruppo. Il server individuato, perfettamente compatibile con l'infrastruttura esistente, è un HP BL 460c G9 256KB(min) RAM, 2 socket,20 core min.

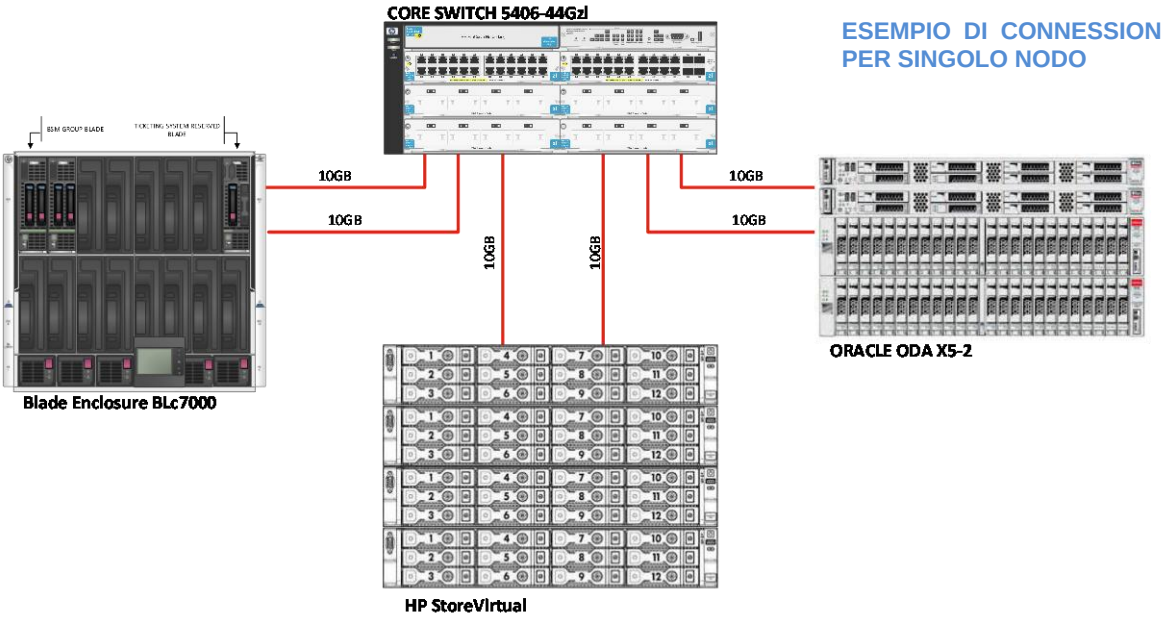


Per garantire le funzioni di High availability dei processi di produzione, il servizio di database ORACLE necessario al sistema di bigliettazione sarà ospitato in un cluster proprietario ORACLE composto da due nodi ODA X5-2 dotati ognuno di doppio server.



La soluzione ORACLE individuata garantisce la scalabilità sia come capacità elaborativa tramite la licenziazione su necessità di ulteriori core/CPU e/o l'espansione di memoria, che di archiviazione tramite l'eventuale aggiunta di ulteriori cassetti disco. (per maggiori informazioni: http://www.oracle.com/technetwork/database/database-appliance/documentation/oracle-database-appliance-ds-1867697.pdf)

ESEMPIO DI CONNESSIONE PER SINGOLO NODO



3. Piattaforma SoftWare

3.1 Microsoft – Sistema Operativo

Ogni blade sarà dotata di licenza di sistema operativo Microsoft DataCenter Server 2012 R2. Le necessità di installazione di Sistemi Operativi di versioni precedenti sono supportate dalla tipologia di licenza adottata. In ogni caso la versione di sistema operativo che potrà essere impiegato dai diversi software applicativi dovrà essere compreso nella tabella dei sistemi supportati da Microsoft e tempestivamente aggiornati.

3.2 VMware – Piattaforma di Virtualizzazione

Per la gestione dei servizi informatici del Gruppo è attiva la piattaforma virtuale VMware versione 5.5[1].
Suddetta piattaforma viene costantemente manutenuta provvedendo all'attivazione delle patch o delle versioni più recenti rilasciate dal produttore.
Il SBE, integrandosi con l'infrastruttura del Gruppo, erediterà le medesime configurazioni e funzionalità .

3.3 Dbase

Il Gruppo rende disponibili due piattaforme di data base:
MS SQL 2008 R2[1]
Oracle 12 su Appliance Oracle X5-2
I relativi server sono costantemente aggiornati secondo i specifici rilasci forniti dai rispettivi produttori.

[1] *versione* valida al momento della redazione del presente documento

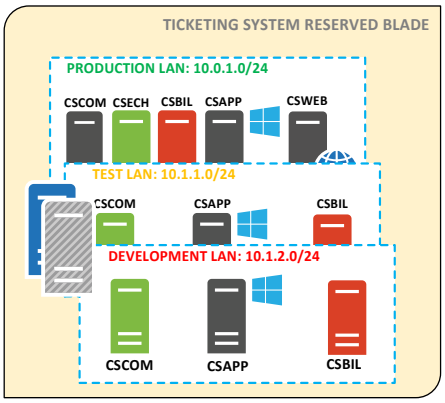
4. Network

Viene riservato alla nuova versione di SBE un piano di indirizzi dedicato che ne permetterà l'installazione e le procedure di setup.
Suddetta predisposizione, che fa capo al cluster firewall/router del Gruppo, si armonizzerà con l'intera struttura esistente permettendo al SBE di poter usufruire in modo più agevole dei diversi servizi.

4.1 Ticketing LAN

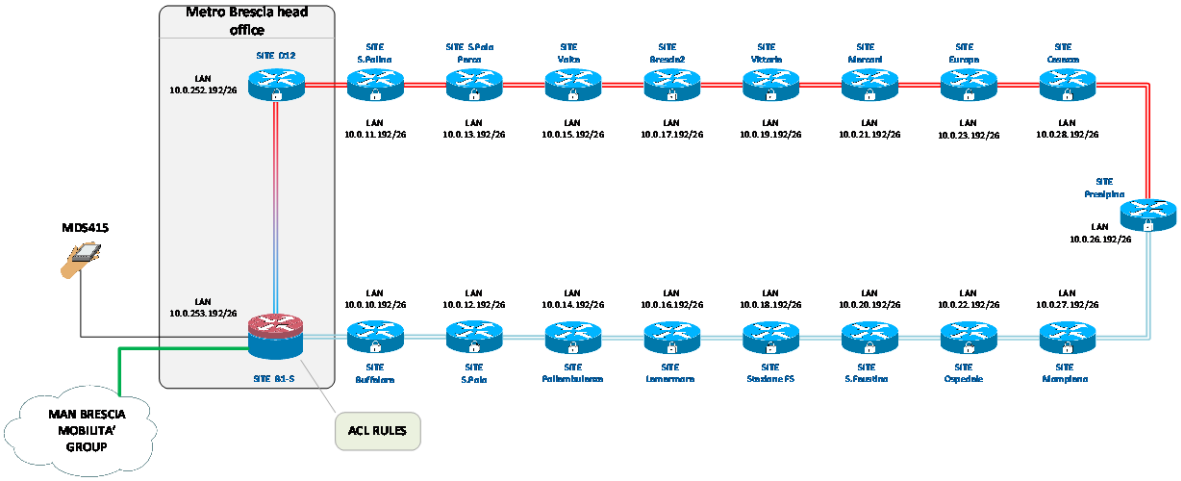
Alla ticketing LAN sono riservati tre pool di indirizzi ognuno dei quali riservato ad uno specifico servizio:

Production LAN: 10.0.1.0/24; riservata alla produzione e gestione dei titoli di viaggio distribuiti all'utenza.
Test LAN: 10.1.1.0/24; a disposizione del cliente per il test delle funzionalità del sistema e dei titoli di viaggio.
Development LAN: 10.1.2.0/24; a disposizione del fornitore per l'elaborazione di aggiornamenti e/o nuove versioni dei diversi applicativi che compongono il SBE.



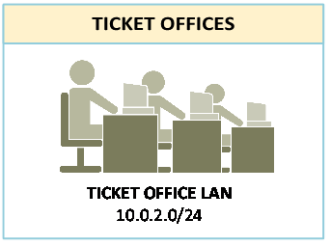
4.2 Metro Station LAN

Address:10.0.x.192/26 dove "x" rappresenta l'identificativo di rete della singola stazione.
Originariamente implementata come rete di Livello 2, questa struttura è stata modificata in una rete di livello 3. Questo permette una razionalizzazione dell'hardware, ed un incremento dell'efficienza della gestione del traffico tramite l'impiego di ACL (access control list).



4.3 Ticketing Offices

Address:10.0.2.0/24 – BST Office
Address:10.0.9.0/26 – Info Stazione
Address:10.0.4.0/24 –> 10.0.9.64/26 InfoPoint Office
Pool di indirizzi riservati agli uffici presidiati da personale del Gruppo che provvede all'emissione e al rinnovo di titoli di viaggio. Brescia Mobilità assicura il raggiungimento dei siti tramite la gestione del routing della MAN del Gruppo.

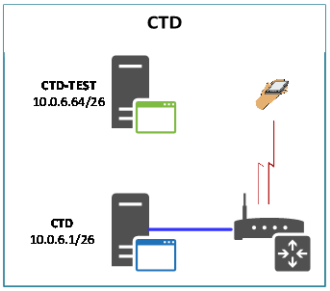


4.4 Ticketing machine

Address:10.0.3.0/24
Pool di indirizzi riservato alle macchine di distribuzione di titolo di viaggio (TVM) predisposte in corrispondenza delle fermate bus. Il sistema di connettività proprietario del Gruppo permette il trasporto della MAN e con essa la gestione del routing necessario alla gestione delle TVM.

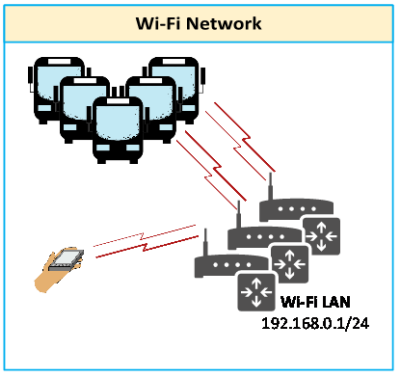
4.5 CTD network

Address CTD:10.0.6.0/24 - *>10.0.6.0/26*
Address CTD:10.0.8.0/24 - *>10.0.6.64/26*
Queste network sono definite all'interno dell'area della sede di Brescia Trasporti e sono attestate a macchine aventi funzione di concentratori di dati provenienti da dispositivi mobili quali le obliteratici e bordo bus e i terminali degli agenti .controllori. La riorganizzazione del sistema prevede l'ottimizzazione delle reti



4.6 Wi-Fi network

Address Wi-Fi: 192.168.0.1/24
Network presente nell'area di deposito della sede di Brescia Trasporti attualmente terminata sul CDT di produzione permette il recupero delle informazioni presenti a bordo dei singoli autobus ogni volta questi rientrano in deposito. Si prevede la modifica di tale network attestandola in modo logico al firewall del Gruppo. Tale intervento offrirà la possibilità, oltre a garantire la sicurezza degli accessi, di trasportare suddetta rete anche presso sedi remote del Gruppo.



4.7 APN

Address APN: 172.17.6.0/24 from 101 to 254
Pool di indirizzi veicolati tramite APN assegnati ai dispositivi di ricarica abbonamento e vendita titoli di viaggio dislocati presso gli esercizi commerciali convenzionati. Suddetti indirizzi sono autenticati e governati dall'insieme dei servizi di firewall e radius del Gruppo.

5. Servizi e Protocolli

I servizi e i protocolli IP delle diverse reti del ticketing system saranno coordinate dal cluster di Firewall del Gruppo. Sarà quindi possibile specializzare ogni singola rete e/o apparato in rapporto alle proprie necessità funzionali nel rispetto delle garanzie di sicurezza di cui ognuna di essa deve essere dotata.
Il fornitore dovrà definire, in contraddittorio con il dipartimento IT del Gruppo, un piano dettagliato di servizi e protocolli da assegnare da ogni singola rete.

5.1 Servizio di End Point Protection (EPP)

Al momento dell'edizione del presente documento, il servizio EPP distribuito dal Gruppo è il Symantec ver. 12.1.6. I componenti di protezione attiva del suddetto servizio dovranno essere installabili e aggiornabili in modalità continuativa sia sui dispositivi client (es:TVM) che sui diversi server che compongono l'universo dei sistema di bigliettazione. La supervisione dei diversi dispositivi sarà assicurata dalla console centralizzata, tramite TCP port 8014, che provvederà anche alla distribuzione automatica degli aggiornamenti dei file contenti le definizioni di protezione.
Il fornitore dovrà comunque fornire una tabella di compatibilità con altri sistemi di protezione quali ad esempio Kaspersky Endpoit Sucurity e/o McAffy EPP.

5.2 Servizio di DNS (Port UDP 53)

E' attivo, nell'infrastruttura del Gruppo, il servizio di risoluzione dei nomi costituito da un cluster di server di dominio in configurazione HA. Suddetto cluster assicurerà la risoluzione dei nomi anche per i dispositivi di rete del SBE.

5.3 Servizio di DHCP (Port UDP 67-68)

Il servizio di attribuzione dell'indirizzo IP destinato al funzionamento in rete dei diversi client del sistema di bigliettazione è fornito da apposito server del Gruppo. Al fine di poter facilitare le operazioni di troubleshooting, per ogni singolo dispositivo client sarà attivata la funzione di reservation dell'indirizzo IP basato sul MAC address del dispositivo stesso.

5.4 Servizio RADIUS (Port TCP/UDP 1812)

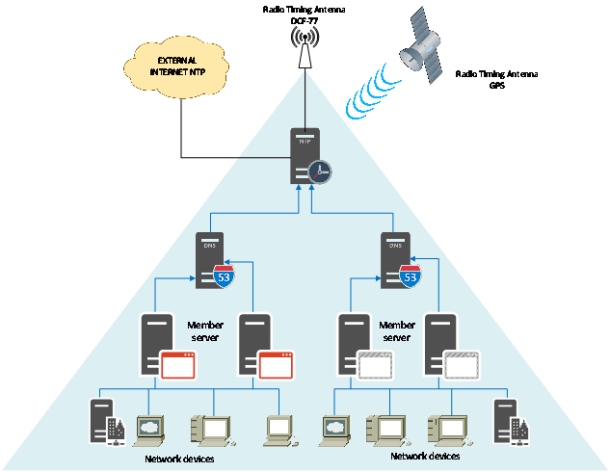
Il Gruppo dispone di un cluster di server in configurazione HA tramite il quale si provvede all'autenticazione dei dispositivi configurati su reti esterne al Dominio BSM o reti esposte al possibile accesso pubblico come ad esempio le reti Wi-Fi e APN.

5.5 Servizio FireWall

Il Gruppo dispone cluster di firewall in configurazione HA tramite il quale vengono sorvegliate tutte le reti informatiche che insistono sull'infrastruttura del Gruppo stesso. Il firewall ha attiva la DMZ per la pubblicazione dei servizi web based.

5.6 Servizio NTP (Port TCP/UDP 123)

Il Gruppo dispone di un server NTP con combinazioni multiple di riferimento temporale.
Al fine di regolamentare il numero di richieste indirizzate al server NTP di dominio, nel sistema di bigliettazione deve essere eletto un server che provveda a re-distribuire il sincronismo orario dell'NTP di dominio verso tutti gli altri dispositivi dell'universo SBE.



5.7 Servizio IT Infrastructure Monitoring

Il Gruppo dispone del sistema di monitoraggio dell'infrastruttura IT NAGIOS. Su ogni server e client del S.B.E. il fornitore dovrà garantire la possibilità di attivare l'agent necessario al monitoraggio.

6. Policy del Gruppo

La necessità di regolamentare l'accesso e l'uso delle risorse informatiche deriva da un più generale contesto che, partendo dalle circolari del CNIPA e dalle linee guida emanate dagli organismi internazionali, ha prodotto una serie di leggi e decreti in tema di trasmissione delle informazioni e di sicurezza informatica.
La vigente normativa riconosce, infatti, un ruolo centrale e strategico alle nuove tecnologie informatiche nello sviluppo e nel potenziamento dei servizi offerti e, nel contempo, sottolinea il problema della gestione dei potenziali fattori di rischio connessi con tali tecnologie: l'affidabilità del mezzo e la disponibilità, integrità e riservatezza delle informazioni, non lasciando alcuna discrezionalità nell'adozione di efficaci misure atte a prevenire o minimizzare i rischi di incidente informatico o di atti di pirateria informatica.
Aderendo a quanto prescritto dalla vigente normativa e con particolare attenzione al **Provvedimento "Amministratori di sistema" del 27 novembre 2008 emesso dal Garante della Privacy, il Gruppo ha provveduto alla nomina di un proprio Amministratore di Sistema al quale sono stati demandati gli incarichi relativi alla definizione delle policy per la gestione della rete Informatica, sollecitando particolare attenzione per tutti gli aspetti che riguardano la sicurezza dei sistemi e dei dati.**
Pertanto, si richiede al fornitore di attenersi a quanto di seguito indicato:

6.1 Coordinamento Informatico

Al Dipartimento IT del Gruppo Brescia Mobilità è demandato il compito di provvedere alla attivazione e gestione di tutte le infrastrutture fisiche, virtuali e di network del Gruppo ivi comprese quelle necessarie al corretto funzionamento del SBE. Per coordinare efficacemente qualsiasi intervento di modifica o implementazione si rende quindi indispensabile fare riferimento allo stesso dipartimento.

6.2 Accesso Amministrativo

Applicando quanto disposto dal Garante della Privacy nel capoverso 4.5 del provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 e pubblicato su G.U. n. 300 del 24 dicembre 2008, Brescia Mobilità adotterà anche per il SBE la registrazione dei log amministrativi.
Pertanto si ritiene necessario normalizzare anche per il S.B.E. l'accesso alle risorse informatiche discriminando l'accesso con ruolo Amministrativo, dedicato esclusivamente all'amministratore del sistema responsabile IT e in subordine al fornitore/manutentore, dai semplici user, assegnato a tutti gli operatori del servizio. E' quindi fondamentale che i dispositivi collegati in rete debbano erogare servizi tramite login (manuale o automatico) con accesso NON amministrativo al fine di poter controllare il corretto utilizzo delle risorse informatiche e per garantire la protezione e l'integrità dei dati in essi contenuti.
Si rende quindi necessario che i diversi client e server che compongono l'universo SBE eseguano il processo di autenticazione tramite procedure di iscrizione a dominio. Sarà valutato in fase esecutiva l'opportunità di attivare un dominio ad hoc per il SBE.

6.3 Servizi Client-Server

Facendo riferimento al paragrafo 6.2, per i processi che richiedo accesso a protocolli di comunicazione o a servizi client-server in modalità amministrativa verrà istituito un utente di dominio con diritti amministrativi locali dei singoli dispositivi.

6.4 Back-Up

Recependo quanto prescritto nell'allegato B del "Disciplinare tecnico in materia di misure minime di sicurezza del Codice in materia di protezione dei dati personali", Brescia Mobilità attiverà una procedura di back-up volta al salvataggio delle macchine server e alla conservazione dei dati.
Al momento dell'edizione del presente documento, lo strumento di back-up in dotazione a Brescia Mobilità e il VERITAS(Symantec) NetBackUp 7.x.
Il fornitore deve assicurare la possibilità di installazione di agent di Veritas e/o di terze parti volti a migliorare i processi di backup.

6.5 System upgrade

Recependo quanto prescritto nell'allegato B del "Disciplinare tecnico in materia di misure minime di sicurezza del Codice in materia di protezione dei dati personali" il fornitore deve corredare il S.B.E. di un piano di Manutenzione Adattativa comprendente tutti gli interventi necessari per mantenere operativo il sistema con versioni e/o aggiornamenti successivi a quelli previsti dal contratto di fornitura.
Il piano di manutenzione adattiva deve prevedere l'aggiornamento (se necessario) dei diversi software con cadenza minima semestrale con la possibilità da parte del committente di richiedere interventi anticipati e più frequenti a fronte di rilascio di patch per sistemi operativi relative alla sicurezza.

7. Certificazione

Ai prestatori di servizi rivolti al pubblico è fatto obbligo generale di assicurare per tutti gli strumenti offerti alla clientela adeguati presidi tecnico-organizzativi di sicurezza al fine di garantire in ogni momento il regolare funzionamento degli stessi, nonché la fiducia del pubblico nel loro utilizzo. E' inoltre interesse del Gruppo mantenere un rapporto di trasparenza verso l'Amministrazione Pubblica e la clientela circa il corretto operato del Sistema di Bigliettazione.
Le prescrizioni definite nei capitoli precedenti, oltre ad armonizzare il SBE con l'infrastruttura esistente, daranno la possibilità a Brescia Mobilità di affrontare una procedura volta al conseguimento della certificazione ISO 27001 che attesti la corretta operatività del Gruppo.