



Soluzione tecnica

Sommario

Sommario	i
Versione.....	ii
Note	iii
1. Introduzione	1
2. Descrizione del Data Center Aruba	2
Impianto di distribuzione elettrica	3
Impianto di condizionamento/raffreddamento	5
Sicurezza fisica	7
3. Servizio di backup remoto	11
3.1 Dimensionamento della banda in funzione del backup	13
4. Servizio di Disaster Recovery	15

Versione

Vers. documento	Autore	Data Rilascio	Note
0.1	Enrico Gloria	10/10/2013	
0.2	Enrico Gloria	11/10/2013	

Note

Il presente documento è da considerarsi una bozza in fase di lavorazione

1. Introduzione

Il presente documento descrive come Aruba intende fornire i servizi di disaster recovery e backup per i comuni della Regione Basilicata, nell'ambito del progetto di rilascio e gestione della Firma Digitale ai cittadini.

I servizi offerti da Aruba sono di due tipi

- Servizio di Backup Remoto
- Servizio di Disaster Recovery Remoto

Il comune di Garaguso, utilizzerà per la messa in sicurezza del proprio patrimonio informativo entrambe le soluzioni ed ha indicato i seguenti servizi come facenti parte del piano di continuità operativa indicandone la criticità:

Servizio/ Classe di Servizi	Indice complessivo di criticità	Classe di criticità	Soluzione tecnologica (Tier)
Albo Pretorio	2	Bassa	2
Gestione del personale	2	Bassa	2
Gestione Sito Web	3	Media	2
Protocollo	3	Media	3
Servizi Demografici	4	Media	3

La soluzione tecnologica offerta da Aruba permetterà di realizzare un sistema di DR per tutti i servizi elencati ed attualmente forniti da un singolo server fisico.

Il volume dei dati stimato, da salvaguardare quotidianamente, è dell'ordine di 1,2 GB utilizzando le procedure di backup incrementale previste dalla soluzione.

2. Descrizione del Data Center Aruba

Di recentissima apertura, il nuovo data center di Aruba è uno dei pochi in Italia a rispondere ai requisiti tecnici necessari a garantire i **livelli di uptime propri del Tier IV**: tutta l'infrastruttura è ridondata in modo da poter funzionare anche in caso di guasto nei sistemi elettrici e di condizionamento. Inoltre l'impianto elettrico è stato realizzato in modo che qualsiasi componente dello stesso possa essere rimossa per guasti o manutenzione senza che nessun sistema subisca disservizio. L'azienda e il data center sono certificati ISO27001 per la sicurezza delle informazioni.

Il data center, che ha una superficie pari a 4.000 mq dedicata alle sole sale dati e locali di presidio, è progettato per contenere a pieno regime circa 40.000 server in 1.100 armadi rack, per una potenza elettrica assorbita dai soli server ed apparecchiature informatiche di circa 4,5 MW, in ridondanza 2*n.

Adiacenti all'edificio principale, ma separati da esso per motivi di sicurezza, si trovano:

- un ulteriore edificio che ospita i **Power Center** che alimentano i server ed il sistema di condizionamento
- una costruzione per ciascuno dei due rami dell'impianto (distanti 6 metri dai **Power Center**) - dedicate ad ospitare le batterie di alimentazione del sistema **UPS**

Tutti gli edifici rispondono alle normative sismiche. La scelta di separare i Power Center e i locali batterie dal resto del data center è stata adottata per annullare il rischio che eventi accidentali a queste componenti possano influire sul regolare funzionamento del data center o danneggiare i server.

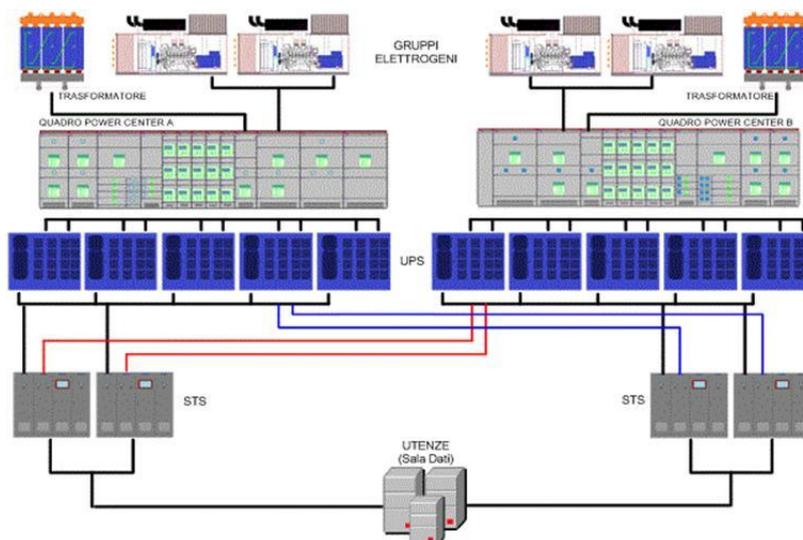
La progettazione e realizzazione del data center è avvenuta seguendo le direttive emanate da "Uptime Institute" <http://www.uptimeinstitute.org/> secondo il livello più alto previsto per lo standard di classificazione: tipo "Tier IV" – a garanzia della disponibilità e continuità di funzionamento.

UptimeInstitute professional services	TIER I	TIER II	TIER III	TIER IV
Ridondanza	N	N+1	N+1	Minimo N+1
Distribuzione	1	1	1 normale & 1 alternativa	2 Simultanee
Manutenzione	Spento	Spento	A caldo	A Caldo
Resilienza (capacità di resistenza ad una rottura)	no	no	no	si
Massimo Downtime/anno	28h36'	22h	1h36'	48'

Le sale dati sono dotate di sistemi di condizionamento e la connettività è ridondata in modo da garantire la massima affidabilità e il massimo uptime dell'infrastruttura. Il data center è monitorato e presidiato 24h su 24h, 365 giorni all'anno e l'accesso alla struttura è permesso solo a seguito di riconoscimento e registrazione.

2.1 Impianto di distribuzione elettrica

L'impianto di distribuzione elettrica è stato realizzato in modo che qualsiasi componente dell'impianto stesso possa essere rimossa per guasti o manutenzione senza che nessun sistema subisca disservizio.



Tutti i cavi utilizzati sono del tipo resistente al fuoco secondo le norme **IEC 331 / CEI 20-36 EN 50200**.

Il data center dispone di alimentazione elettrica fornita da Enel Distribuzione in Media Tensione (15.000 Volt). L'anello in M.T. è costituito da 4 gruppi di trasformazione M.T./B.T. collegati ad un **Power Center** completamente indipendente dagli altri - in completa ridondanza 2*n:

- 2 gruppi M.T/B.T (3150 kVA ciascuno) per alimentazione Power Centers **Sale Dati**;
- 2 gruppi M.T/B.T (3150 kVA ciascuno) per alimentazione Power Centers **Condizionamento**.

In parallelo ai gruppi di trasformazione, ogni **Power Center** è connesso a gruppi elettrogeni Diesel – con potenza di 1650 kVA - in grado di erogare una potenza continua pari a quella dei trasformatori M.T/B.T.

Il funzionamento del datacenter a pieno regime - in assenza di energia elettrica Enel ed in assenza di rifornimento **per oltre 48 ore** - è garantito dalla presenza di uno stoccaggio di carburante costituito da 4 cisterne interrate da 25.000 litri ciascuna, per un totale di 100.000 litri di gasolio.

L'alimentazione della Sala Dati è costituita da due **Power Center** simili, collegati tra di loro da gruppi di apparati **STS (Static Transfer Switch)** e fisicamente separati tra di loro e dal resto del **datacenter** da pareti e porte con resistenza al fuoco **REI 120**.

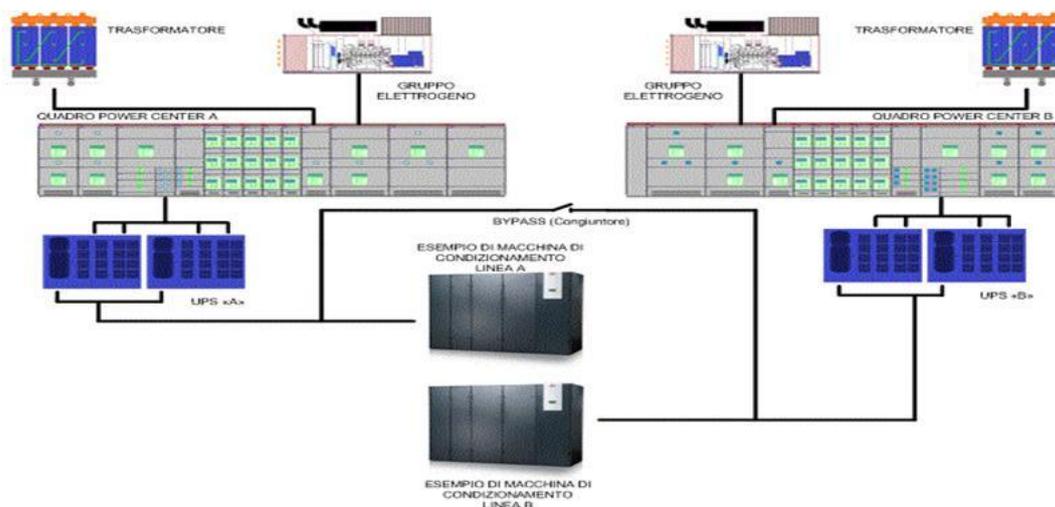
Tutti gli armadi rack presenti dispongono di 2 **PDU (Power Distribution Unit)**, alimentate singolarmente da entrambi i **Power Center**.

Qualora venga a mancare l'alimentazione elettrica proveniente da uno dei due **Power Center** - in caso di guasto o intervento di manutenzione - il sistema **STS (Static Transfer Switch)** è in grado di alimentare istantaneamente e senza interruzioni verso i server entrambe le **PDU** presenti in ciascun armadio del **Power Center** superstite, realizzando pertanto una ridondanza completa di tipo 2*n.

La scelta di utilizzare UPS del tipo a doppia conversione garantisce la stabilità totale dell'alimentazione elettrica erogata, non essendo mai i server alimentati direttamente dall'energia proveniente da Enel o dai gruppi elettrogeni. Tutti i server o gli apparati forniti dispongono di doppia alimentazione, oppure sono apparati ridondati a singola alimentazione connessi ognuno alla **PDU** opposta rispetto all'altro. Si configura pertanto un'architettura di distribuzione ridondata su tutti i livelli del sistema di alimentazione elettrica.

L'utilizzo della UPS per l'impianto di raffreddamento rappresenta una soluzione onerosa e poco frequente, ma utile a garantire il funzionamento ottimale dei server anche in condizioni di emergenza. Una **sala dati** ad

alta densità – infatti - richiede un condizionamento continuo per mantenere le caratteristiche di uptime e funzionamento richieste dallo standard di classificazione “Tier IV”, come si può leggere nel documento:



Tutti i quadri e le linee elettriche sono fisicamente separate, in modo che un guasto o un intervento di manutenzione non influiscano sul funzionamento degli apparati in essi contenuti.

2.2 Impianto di condizionamento/raffreddamento

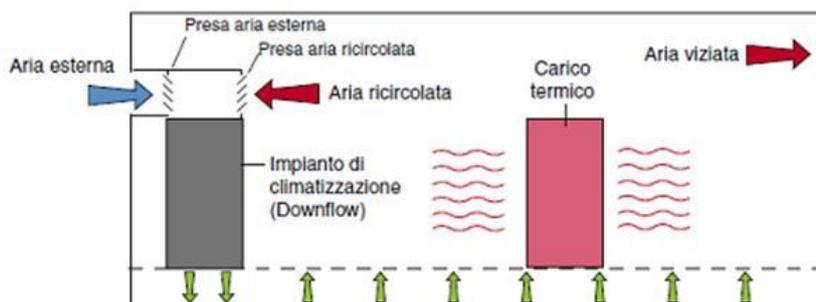
L’impianto di condizionamento dell’aria (o di climatizzazione) è stato progettato a partire dall’individuazione delle più adeguate tecnologie atte a garantire affidabilità (in una situazione di alti carichi termici e funzionamento continuativo) e facilità di gestione, di controllo e risparmio energetico.

La distribuzione dell’aria in modalità “UNDER” è supportata dall’elevata altezza del pavimento flottante (50 cm, aumentato a 60 cm nei punti di passaggio cavi principali) che consente di ridurre al minimo le perdite di carico anche in presenza di passerelle e cavi.

Il controllo e gestione della temperatura e dell’umidità dell’ambiente sono realizzati mediante l’impiego di climatizzatori di precisione costituiti da unità autonome di condizionamento ad espansione diretta condensate ad aria - ad alta efficienza - tramite **gas refrigerante R407C**.

Le condizioni ambientali della sala dati vengono garantite tenendo conto del carico termico, del mutamento delle temperature e del tasso di umidità nell'ambiente mediante apposite sonde.

Il **sistema free cooling** permette un **elevato risparmio energetico**, in quanto è in grado di funzionare a temperature esterne moderate (fino a 16-18°C) e permette di effettuare un ricambio d'aria costante negli ambienti (fino a 100 volumi/ora), che può comunque essere forzato o ridotto al minimo necessario anche durante i mesi estivi, in modo da garantire comunque il ricambio d'aria anche in questo periodo. Allo stesso tempo, esso può essere escluso in casi particolari, come ad esempio presenza di fumo o polvere nell'ambiente esterno all'edificio.



Con l'obiettivo di elevare al massimo l'efficienza energetica in ottica Green, la realizzazione del **data center** ha seguito una soluzione utile a garantire la compartimentazione dell'aria fredda, mantenendo nel contempo tutti i corridoi alla stessa temperatura.

Ciò ha richiesto l'utilizzo di armadi rack di profondità superiore all'usuale (1200 mm anziché 1000 mm), ricavando così davanti ai server uno spazio di circa 200 mm. Ciascun rack è costituito da uno sportello anteriore di tipo vetrato a tenuta d'aria ed uno sportello posteriore di tipo metallico grigliato. Lo spazio ricavato tra la parte frontale dei server e lo sportello anteriore di ciascun rack rappresenta quindi un "canale" di aria fredda.



Naturalmente gli armadi rack - a parte tale modifica - sono del tipo standard e consentono il montaggio di tutte le apparecchiature predisposte per il montaggio su **rack 19" (IEC 60297-3-100)**.

2.3 Sicurezza fisica

Il data center è certificato ISO 27001 e in esso sono attuate le principali misure volte a garantire la sicurezza fisica della struttura.

L'edificio è stato progettato ponendo la massima attenzione alla **sicurezza fisica degli accessi**:

- le porte esterne sono di tipo blindato;
- le finestre e le superfici vetrate esterne a piano terra sono dotate di vetro antiproiettile dello spessore di 21 mm;
- le griglie per il passaggio dell'aria necessaria al raffreddamento della sala dati sono protette da sbarre trasversali in acciaio del diametro di 20 mm.

L'accesso dei visitatori avviene attraverso una "bussola" a due ante rotanti e interbloccate, analoga a quelle normalmente utilizzate negli istituti bancari - anch'essa dotata di vetri anti-proiettile da 21 mm di spessore. Una volta avuto accesso all'interno, è presente una seconda barriera, costituita da varchi motorizzati. Per attraversare tali varchi è necessario essere accreditati alla antistante Reception, con lo scopo di ottenere un badge abilitato. Per la registrazione dei visitatori, è istituito un apposito registro conservato in conformità con quanto previsto dalla normativa ISO 27001.

Superata la barriera dei varchi motorizzati, si trova davanti la sala dati principale, delimitata da una parete in vetro antiproiettile da 21 mm. L'accesso, consentito solo al personale abilitato, avviene tramite porte scorrevoli di sicurezza assoggettate al controllo accessi. L'intero stabile è circondato da una recede che lo separa su tutti i lati dalle altre proprietà, e protetto da una recinzione rigida in metallo dell'altezza di 260 cm. La struttura è presidiata e sorvegliata 24x7x365.

Accesso controllato tramite autenticazione

Il **data center** è dotato di un **sistema di controllo accessi** esteso a tutti i varchi, sia esterni (ingresso principale, uscite di sicurezza, magazzini, locali tecnici) che interni (sale dati, locali tecnici, uffici). Il riconoscimento è basato su un doppio criterio di autenticazione, mediante l'utilizzo di una tessera di prossimità e la digitazione di un pin. Il sistema di gestione degli accessi prevede la possibilità di abilitare e disabilitare le singole tessere in base alle aree, agli orari ed ad altri parametri, in modo da garantire sia la massima sicurezza degli ambienti che la necessaria fluidità degli accessi.

Impianto anti-intrusione

L'edificio è dotato di un sistema anti-intrusione che utilizza sensori volumetrici a doppia tecnologia, assieme a sensori a contatti su infissi e sensori di vibrazione sui vetri delle sale dati.

L'impianto è integrato da sistemi evoluti di analisi delle immagini rese disponibili dall'impianto di video-sorveglianza (trattato di seguito). La sede esterna è protetta tramite barriere a raggi infrarossi applicate lungo tutto il perimetro della recinzione esterna. L'impianto anti-intrusione è integrato con il sistema di controllo accessi.

Impianto di video-sorveglianza

L'**impianto di video-sorveglianza** è costituito da un cospicuo numero di telecamere (oltre 120) posizionate sia all'interno dell'edificio (lungo tutti i punti di passaggio e all'interno dei locali sensibili) che all'esterno (lungo la recinzione, sulla copertura dell'edificio e nella zona dove sono ubicati i gruppi elettrogeni). Le telecamere utilizzate sono di tipologie diverse in base alle diverse esigenze derivanti dai singoli posizionamenti (angolo e distanza di visuale, tipologia di illuminazione, ecc). Le immagini vengono rese disponibili in real-time al personale di presidio mediante appositi monitor presenti all'interno del NOC. Tutte le immagini acquisite vengono immagazzinate tramite videoregistratori digitali, situati in ambienti protetti e conservate per 24H, come previsto dalle vigenti normative in ambito Privacy.

Impianto rilevamento fumi e spegnimento incendio

Tutto l'edificio è dotato di un **sistema di rilevamento dei fumi** costituito da sensori ottici posizionati in ambiente, sotto al pavimento flottante e sopra il controsoffitto. I sensori sono collegati tra loro in loop e mediante cavo antifiamma, in modo da garantire il loro funzionamento anche in caso di interruzione di un collegamento. Sono stati previsti opportuni sensori in grado di verificare la presenza di fumo all'interno delle condotte per il ricambio dell'aria degli ambienti.

La gestione dell'impianto è demandata ad una centrale a 6 loop, con il compito di rilevare i segnali provenienti dai sensori, attivando gli allarmi ottici e acustici, nonché provvedendo all'attivazione dell'impianto di spegnimento mediante apposite unità di spegnimento. Le aree sensibili e/o a maggiore rischio (2 sale dati, 2 sale tlc, 6 power center, 6 sale trasformatori MT e 2 sale quadri MT) sono dotate di sistema di spegnimento a gas inerte (Azoto).

Il **metodo di spegnimento** è quello della diluizione d'ossigeno, ottenuto mediante una scarica di un'adeguata quantità di azoto in grado di ridurre la percentuale di ossigeno dal 23% presente normalmente in atmosfera al 12% circa, valore che non consente la combustione. Tale scarica non rappresenta un pericolo per la salute delle persone eventualmente ancora presenti nell'ambiente al momento della scarica (comunque annunciata con un anticipo di 60 secondi da allarmi acustici e ottici) e preserva gli apparati consentendo la continuità nell'erogazione dei servizi.

I gruppi elettrogeni di emergenza presenti, posizionati all'esterno, sono dotati di impianti di rilevazione e di spegnimento incendi (ad anidride carbonica) dedicati e autonomi. Tali gruppi sono dotati inoltre di sistema di intercettazione del carburante, in grado di interrompere l'afflusso in caso di incendio. E' inoltre presente la normale dotazione di estintori portatili e carrellati.

Impianto di rilevamento liquidi e sistema anti-allagamento

I vari locali dell'edificio sono dotati di sensori per il **rilevamento della presenza di liquidi**, posizionati sotto il pavimento flottante. Per quanto riguarda la possibilità di allagamento derivante da rottura delle tubazioni per l'acqua dei servizi igienici (o dalla dimenticanza di rubinetti aperti), è stato previsto un sistema costituito da sensori (flussostati e rilevatori di presenza) e da una logica che, nel caso in cui venga rilevato il flusso di acqua in assenza di persone all'interno dei singoli servizi igienici, provvede all'interruzione dell'erogazione dell'acqua nel medesimo ambiente tramite l'attivazione di una elettrovalvola, eliminando la possibilità di riversamento di acqua a terra.

Le eventuali problematiche derivanti da alluvioni sono scongiurate, in quanto la struttura è ubicata in zona pianeggiante ed in posizione rilevata di circa un metro rispetto al piano di campagna. In fase progettuale si è provveduto inoltre a evitare il posizionamento di impianti strategici o di parte di essi a quota inferiore a tale valore: ciò esclude la necessità di sistemi anti-allagamento dotati di pompe idrauliche.

Sicurezza degli apparati

I server dislocati presso il Centro Servizi saranno dotati di meccanismi di sicurezza fisica utili ad impedire il furto locale dei dati. Gli armadi rack sono tutti dotati di sportelli metallici con serratura a chiave e i supporti di memorizzazione contenenti dati sono conservati in luogo sicuro. Gli apparati attivi di rete saranno posizionati in armadi di cablaggio con chiusura a chiave che inibisce l'accesso fisico ai dischi locali e ne impedisce la rimozione.

BMS

Tutti gli impianti sopradescritti, assieme agli impianti e sistemi strategici (gruppi elettrogeni, ups, quadri elettrici, condizionamento di potenza) e agli impianti standard (illuminazione, condizionamento uffici) sono supervisionati da un sistema BMS (Building Management System) a mappe, in grado di gestire tutti gli eventi e gli allarmi, di interpretarli e di assegnare loro le opportune priorità, generando le conseguenti notifiche in modo da ridurre al massimo i tempi di interpretazione e individuazione degli eventi. Il **BMS** - controllato dal personale di presidio del **NOC (Network Operation Center)** - è accessibile anche da remoto ed in grado di provvedere alla notifica degli allarmi tramite i consueti canali (e-mail, SMS, ecc).

2.4 Connettività

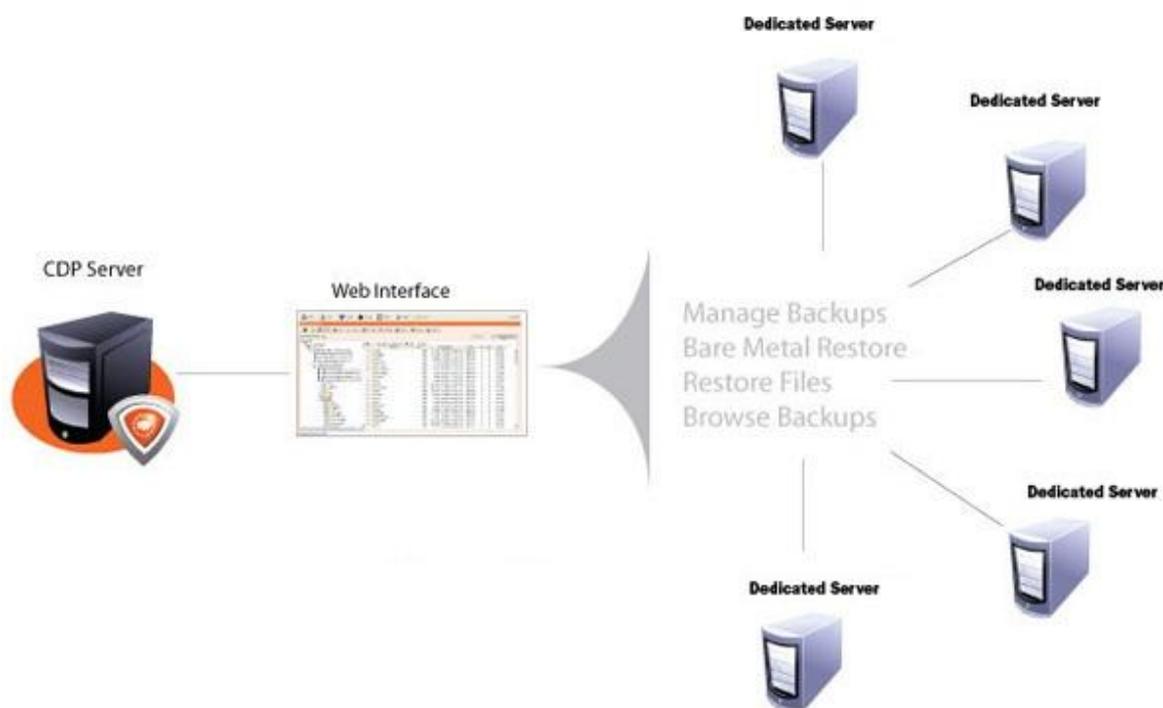
La connettività presso il datacenter, designato per ospitare l'infrastruttura, rappresenta lo stato dell'arte per sicurezza, prestazioni e ridondanza, in quanto è servito da 6 carrier diversi in ridondanza (Telecom, Cogent, Wind, Mix, Namex, Interoute) per un aggregato totale pari a 80Gbit/sec.

Gli apparati di bordo e gli interior gateway del data center sono di marca Cisco, brand che garantisce lo stato dell'arte negli apparati di routing.

Il firewall che fornisce l'accesso all'infrastruttura dedicata a Regione Basilicata è un Fortinet Fortigate ed è certificato EAL4+ dallo standard internazionale per la sicurezza Common Criteria (ISO/IEC 15408), che costituisce l'organismo internazionale per la sicurezza informatica e FIPS140-2 per la sicurezza del motore di cifratura.

3. Servizio di backup remoto

Il servizio di backup remoto con Disaster Recovery prevede l'utilizzo di un server di backup dedicato al progetto posto nella webfarm di Aruba. Il software utilizzato è Idera CDP e funziona ad agenti, ovvero ogni server da sottoporre a backup deve necessariamente installare un software di piccole dimensioni che una volta installato crea un canale cifrato con il server centrale.



La comunicazione diretta tra i server target posti presso Garaguso ed il server centrale di backup posto in Arezzo deve essere garantita da una comunicazione diretta qualora il server sia direttamente esposto su internet, oppure mediante l'instaurazione di un canale VPN IPSEC di tipo Lan-to-Lan. Per ottenere questo è stato previsto un firewall dedicato al progetto in grado di instaurare tunnel cifrati verso Internet, e dunque raggiungibili dal sito del Comune di Garaguso.

Una volta instaurata la connessione client-server verrà configurato il backup giornaliero incrementale, compatibilmente con la banda in uscita dal Comune.

Basandosi sul numero di server da porre sotto backup e sullo spazio complessivo da utilizzare, il Comune di Garaguso dovrà selezionare uno dei pacchetti proposti:

Pacchetto	Numero di agenti forniti	Spazio disco remoto fornito
BR1	2	200 GB
BR2	5	500 GB
BR3	10	1000 GB

BR4	20	2000 GB
BR5	50	5000 GB

Valutando lo spazio utilizzato dal Comune di Garaguso in 45 GB **il pacchetto BR1 risulta essere sufficiente per la soluzione da implementare.**

Il funzionamento del software di backup può essere diviso in due fasi:

- **Allineamento Iniziale:** Il software a bordo del server deve inviare tutti i dati al server centrale di backup, è probabile che impieghi giorni o settimane, dipende dalla banda disponibile. E' anche possibile portare direttamente in datacenter una copia su nastro o DVD per accelerare questa fase.
- **Allineamento a regime:** La maggior parte dei dati di un server non cambia di giorno in giorno ma solo una piccola parte di essi nell'ordine del 3% giornaliero. Questo vuol dire che se ho un server Windows che occupa spazio pari a 100MB, dopo un giorno solo 3MB sono realmente cambiati rispetto al giorno precedente. Il software Idera effettua il backup incrementale, il che vuol dire che riesce in automatico ad individuare quei 3MB al giorno che sono realmente cambiati e li invia al server centrale.

Superata la fase di allineamento iniziale del backup è indispensabile dimensionare la banda a disposizione del Comune in funzione del backup incrementale, come descritto nel paragrafo successivo.

Il server centrale nel Datacenter Aruba memorizza ogni giorno le variazioni dei dati del server di Garaguso, e li consolida con il backup completo effettuato nella fase di backup iniziale, riuscendo in questo modo ad avere sempre una copia coerente che al più differisce di 24 ore rispetto a quella in produzione presso Garaguso. Tale copia sarà disponibile al Comune per ripristinare il server principale.

La retention, ovvero il tempo in cui i vecchi dati di backup rimangono sul server prima di essere sovrascritti dai dati più recenti, viene deciso in base allo spazio libero rimasto sul server centrale, un buon valore di retention proposto al Comune di Garaguso è 15 giorni, compatibilmente con lo spazio residuo del pacchetto scelto.

Grazie alla retention si potrà scegliere di far ripartire il server di Garaguso dalla copia di diversi giorni prima di un eventuale crash oppure dalla copia del giorno precedente.

3.1 Dimensionamento della banda in funzione del backup

E' fondamentale per il corretto funzionamento del backup, e di conseguenza del Disaster Recovery, capire la dimensione massima dei file gestibile dal backup.

Parlando di connettività Internet spesso si intende una banda full-duplex simmetrica, ovvero un tipo di connessione in grado di trasmettere e ricevere i dati alla stessa velocità, ad esempio una connessione HDSL Aruba ad 1Mbps sta a significare che posso utilizzare contemporaneamente 1Mbps per i dati in uscita e 1Mbps per i dati in entrata.

Purtroppo non per tutte le connessioni d'accesso vale lo stesso principio, ad esempio la ADSL è caratterizzata da una forte asimmetria tra upload (banda dal cliente verso Internet) e download (banda da Internet al cliente), e non è sempre facile capire nel contratto quanto valga effettivamente il valore di upload che è comunque sempre inferiore al download; una connessione ADSL tipicamente utilizzata è quella a 640Kbps, il valore indicato e pubblicizzato è in realtà il solo valore di download, un valore tipico per l'upload in questo caso potrebbe essere 64kpbs.

La banda che maggiormente ci interessa per il backup è quella in Upload, ed è la banda utilizzabile dal Comune di Garaguso a Internet, e dunque necessaria per raggiungere il server di backup nel Datacenter di Arezzo.

Di seguito alcuni esempi di quanto deve essere grande il file da porre in backup in funzione della banda in UPLOAD:

DIMENSIONAMENTO INDICATIVO PER BACKUP CON BANDA DEDICATA

Banda Upload	Dimensione Massima	Tempo Impiegato
64kbps	600MB	21 ore 20 minuti
128kbps	1,2GB	21 ore 20 minuti
256kbps	2,4GB	21 ore 20 minuti
500kbps	4,8GB	21 ore 20 minuti
1Mbps	9,4GB	21 ore 20 minuti
2Mbps	19GB	21 ore 20 minuti
4Mbps	38GB	21 ore 20 minuti
10Mbps	100GB	23 ore
20Mbps	200GB	23 ore

Se ad esempio il comune di Garaguso deve mettere in backup ogni giorno circa 5GB, dovrà essere provvisto di una banda dedicata in upload di almeno 500kbps.

I valori descritti in tabella fanno riferimento ad una banda di upload effettivamente garantita (non sempre il provider di accesso ad Internet non sempre garantisce il valore massimale) e prevede che quella banda sia esclusivamente dedicata al backup.

Se si prevede che durante il giorno sia necessario dedicare la banda in upload al web-server e considerando quindi opportuno fare il backup solo nelle 12 ore notturne, allora il valore massimo del backup giornaliero si dimezza e per un uplink a 500kbps si possono spostare solamente 2,4GB ogni notte.

DIMENSIONAMENTO INDICATIVO PER BACKUP CON BANDA CONDIVISA

Banda Upload	Dimensione Massima
850kpbs	3GB
1.7Mbbs	6GB
4Mbps	15GB
8,5Mbps	30GB
42Mbps	150GB
84Mbps	300GB

Le dimensioni del backup discusse fanno riferimento alla variazione giornaliera dei dati, come descritto nel paragrafo precedente.

4. Servizio di Disaster Recovery

4.1 Definizioni

È fondamentale per il corretto funzionamento del backup, e di conseguenza del Disaster Recovery, capire la dimensione massima.

Il processo di disaster recovery si basa sulla valutazione del Business Impact analysis che valuta i servizi e gli aspetti considerati “vitali per il business dell’azienda” da cui si deducono i valori di RTO (recovery time objective) e RPO (recovery point objective) richiesti.

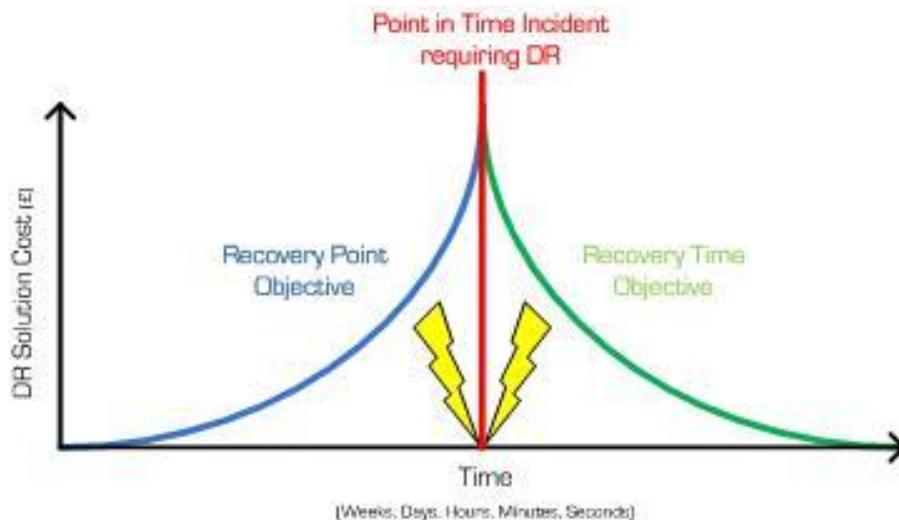
Il Recovery Time Objective (RTO) è il tempo necessario per il pieno recupero dell'operatività di un sistema o di un processo organizzativo. È in pratica la massima durata, prevista o tollerata, del disservizio (downtime) occorso.

Il Recovery Point Objective (RPO) rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un “disastro”.

Al diminuire dell'RPO richiesto si rendono necessarie politiche di sicurezza sempre più stringenti e dispendiose, che possono andare dal salvataggio dei dati su supporti ridondanti tolleranti ai guasti fino alla loro pressoché immediata replicazione su un sistema informatico secondario d'emergenza (soluzione in grado di garantire, in linea teorica, valori di RPO prossimi allo zero).

Per regolare al meglio questi due parametri, è necessario calcolare a priori il “costo del disservizio”, in altre parole il costo subito dall’azienda in caso di mancanza del supporto informatico.

La figura qui di seguito riportata consente di comprendere esattamente come questi due parametri influiscono sul costo e la complessità del processo di Disaster Recovery.



Il grafico implica il crescere del costo dell'infrastruttura al diminuire dei parametri RTO e RPO e come questi si abbassino aumentando il tempo a disposizione.

4.2 Survey iniziale

E' stata richiesta una survey iniziale per conoscere nel dettaglio l'architettura di produzione del Comune

Dimensionamento e verifica canale di trasferimento dati

Banda su rete pubblica disponibile per funzionalità di replica - DOWNLINK	3 Mbps
Banda su rete pubblica disponibile per funzionalità di replica - UPLINK	2 Mbps
Necessità di VPN IPSEC tra Aruba ed il Comune?	No
Attualmente sono necessarie VPN per l'erogazione dei servizi?	No

Identificazione dei server da mantenere sotto servizio Backup Remoto

Server 1:

Identificativo	SERVER HALLEY
Spazio disco complessivo	278 GB
Spazio disco attualmente utilizzato	45 GB
Sistema Operativo e relativa versione	Windows Server 2008 R2

Identificazione dei server da mantenere sotto servizio Disaster Recovery

Server 1:

Identificativo	SERVER HALLEY
Spazio disco complessivo	278 GB
Spazio disco attualmente utilizzato	45 GB
Numero Core e modello CPU	Intel(R) Xeon(R) CPU X 3430 - 2,40 GHZ
RAM	4 GB
Sistema Operativo e relativa versione	Windows Server 2008 R2
Lista Applicativi e relative versioni	Protocollo Servizi Demografici Gestione del Personale Gestione Sito Web Albo Pretorio
Indirizzi IP del server	
DNS	
Configurazione Firewall	

Gateway (firewall/router):

Identificativo	
Indirizzi IP del gateway	IP INTERNI (IP, NETMASK, GATEWAY) (IP, NETMASK, GATEWAY) (IP, NETMASK, GATEWAY) IP ESTERNI (IP, NETMASK, GATEWAY) (IP, NETMASK, GATEWAY) (IP, NETMASK, GATEWAY) (IP, NETMASK, GATEWAY)
Configurazione Firewall	(Elenco Porte da aprire per il funzionamento dei servizi)

Schema logico delle comunicazioni tra i servers

(allegare schema logico/fisico delle comunicazioni tra i servers coinvolti dal progetto. Devono essere indicati i server utilizzando lo stesso identificativo usato nella precedente scheda)

Scheda di ripartenza dei server e dei servizi

Questa sezione deve contenere i normali step necessari alla ripartenza dei servizi in caso di ripartenza da disastro (equivalente ad un blackout. Dovrà quindi contenere tutti i server coinvolti e i servizi da riavviare in sequenza temporale indicando l'esatto identificativo indicato nelle schede precedenti.

Ogni step da effettuare può avere delle dipendenze da step precedenti (ad esempio il lancio di un comando su di un server deve avere come dipendenza lo step di accensione del server).

Nel caso in cui ci siano dei dubbi nel compilare la scheda è possibile compilare queste informazioni insieme al personale aruba.

Step Temporale (es. 1a, 1b, 2a)	Step Requisiti	Nome Server	Servizio Coinvolto	Operazione da effettuare (es. avvio o l'effettivo comando da lanciare)
1a				
2a				

Esempio di compilazione della scheda:

Step (es. 1a, 1b, 2a)	Step Requisiti	Nome Server	Servizio Coinvolto	Operazione da effettuare (es. avvio o l'effettivo comando da lanciare)
1a	-	db01	protocollo	Accensione server
1b	1a	db01	protocollo	Avvio servizio mysql con /etc/init.d/mysqld start
2a	1b	web01	protocollo	Accensione
2b	2a	web01	protocollo	Avvio servizio HTTPD con /etc/init.d/httpd start

4.3 Modalità di DR scelta

Il servizio di Disaster Recovery offerto da Aruba è quello scelto dal Comune di Garaguso.

Questo servizio è da considerarsi una estensione di quello appena descritto, consiste infatti nel ricevere i dati di backup e nel mettere a disposizione le risorse per accendere la copia di backup in un server virtuale in grado di erogare i servizi del Comune di Garaguso nel caso si attivi la procedura di Disaster Recovery.

I pacchetti proposti sono i seguenti:

Pacchetto	vCPU	RAM	Spazio Disco
DR1	4	8 GB	120 GB
DR2	6	12 GB	180 GB
DR3	5	20 GB	300 GB
DR4	14	28 GB	420 GB

Basandoci sui dati forniti dal Comune di Garaguso, poiché è su un solo server che risiedono gli applicativi **si ritiene che il pacchetto DR1 sia correttamente dimensionato alle specifiche esigenze.**

Il servizio di DR si basa su uno o più hypervisor di virtualizzazione che in caso di disastro interagiscono con il server di backup andando a raccogliere i dati del Comune opportunamente trasformati con la procedura “physical-to-virtual” e li accolgono nella piattaforma di virtualizzazione accendendo la macchina.

Per il corretto funzionamento è indispensabile replicare le subnet e le vlan in uso presso il Comune, oltre a modificare il DNS in modo che l’eventuale dominio associato all’indirizzo ip venga ruotato sul nuovo ip assegnato da Aruba.

Lo schema logico dell’interazione tra server di virtualizzazione, server del Comune e server di backup è rappresentato nel seguente schema

