



SMS

**Systems
Management
Specialists**

Cloud Computing

Grupo SMS – www.grupo-sms.com – 949.223.9240 option 3 for sales





Cloud Computing

The SMS Model:

- Cloud computing is a model for enabling ubiquitous, convenient, on-demand access to a dedicated or shared pool of computing resources (e.g., servers, storage, networks, and services) that can be rapidly provisioned with minimal management or effort by the customer.
- SMS is providing a customizable Dedicated as well as a more cost effective Shared Cloud model that allows you to pay for use based on the smallest commitment that is practical. As a business customer your resource requirements can be predictable and schedulable. We work with you to create standard models that reflect your application environment, so that when you need to activate an environment the only issues that need to be dealt with are resource sizing and utilization.
- The Cloud environment is built around a dedicated OS that can be configured to meet your needs. The environment can be either Microsoft or Linux based, with a wide variety of development and system utilities. Customers select the CPUs, Storage Tiers, Network Services that are dedicated to the environment and can be in production within hours.



Vision and Value Proposition

‘Responsibility for your business results’

came from many years of experience that taught us that when the customer is experiencing a problem we are all responsible until resolution.

Information Technology is a business of solving problems.



SMS History

- Founded in 1982
- Global Offices: Irvine, CA, Madrid, Malaga, Buenos Aires, Caracas
- Over 600 Employees Globally
- Privately Held – Net Income Positive
- Over 20+ years of proven Infrastructure Hosting and Outsourcing
- Pioneer of Fixed Monthly Cost Model
- Awarded Inc. 500 Fastest Growing Companies Award
- Won the Federal Government Outsourcer of the Year for the NASA Space Shuttle Program



Cloud Definitions + SMS Value

Cloud Definitions (as related to Virtualization of Servers)

- Public Cloud – the market generally thinks of this as a virtual server provided on shared multi-tenant infrastructure. Amazon EC2 and Azure are examples.
- Dedicated Cloud Hosting – Marketed by companies like Rackspace and Design Data as virtualized dedicated single tenant servers. Service provider typically pays for the hardware.
- **Private Managed Cloud** – The SMS Enterprise offering. Our infrastructure is private, and secure however, the service is Completely Managed from a dedicated or shared perspective.

Grupo SMS Customer Value

- Customers can eliminate the cost, complexity, and security issues associated with physical servers
- SMS reduces complexity by transforming virtual server computing into a cloud based outsourced renting service
- Local meaning low latency hosted in an SMS owned purpose built Tier III datacenter
- Ability to Scale
- Enterprise Level Infrastructure
- Zero cost and risk, associated with selecting, owning or managing the physical on-site resources
- Instant time to value – rapid provisioning of servers
- Simplified management



Differentiators vs AWS and others

- Customizable
 - Dedicated or Shared Private Managed Cloud and Hybrid with Colocation
 - Completely Managed or Shared Responsibilities
 - Build your own size VMs with cores in .50 increments
 - No new GUIs or Web Portals to learn
- More than just Infrastructure
 - Business Partner Consulting Approach
 - Onsite and Offsite Network Management – Design, Circuit procurement, Monitoring
 - Voice Services – Hosted PBX and SIP
 - Business Continuity and Disaster Recovery Design
 - Application Development
 - Virtual Desktops
 - Professional Services
- Proven Enterprise Architecture from elite Manufacturers
 - Separate Redundant Networks for Internet, Storage, and Back-up
 - Adaptive Flash, Fiber Channel and iSCSI Storage
 - Layer 2 Connectivity from over 9 carriers
 - Onsite and Offsite Designs for Redundancy and DR



Security and Compliance

SOC 2 Audited Datacenter

- **Physical Security**

- Data center access controlled and limited to only Authorized Personnel listed on each customers form and controlled by an Administrator
- Mantrap, Key-card and Scramble pad for controlled data center access
- Security camera monitoring and recording throughout the entire data center
- 24x7 onsite staff provides additional protection against unauthorized entry as well as patrolled after hours perimeter security

- **Operational Security**

- Best practices used in the random generation of initial passwords
- All passwords encrypted during transmission and while in storage
- Secure media handling and destruction procedures for all customer data
- Support-ticket history available for review via customer portal

- **System Security**

- System installation using hardened, patched OS
- System patching configured by Grupo-SMS and coordinated with customers to provide ongoing protection from exploits
- Dedicated firewall and VPN services to help block unauthorized system access
- Data protection with managed backup solutions
- Anti-virus protection
- Web Application firewalls
- IDS/IPS solutions



Certifications

- **The SMS Group maintains the following regulatory and compliance standards:**

- ✓ SOC 2 Audit formally known as a SAS70 Audit
- ✓ ISO 27001
- ✓ ISO 9001
- ✓ ISO 14001

- **Sensitivity to:**

- ✓ PCI – as a **Service Provider**
- ✓ HIPAA – as a **Service Provider**
- ✓ ISO – as a Service Provider
- ✓ SOX



SMS Supports all three areas of data security, ensuring the security of customer data



PCI Compliance

The 3 elements of comprehensive compliance

Technologies

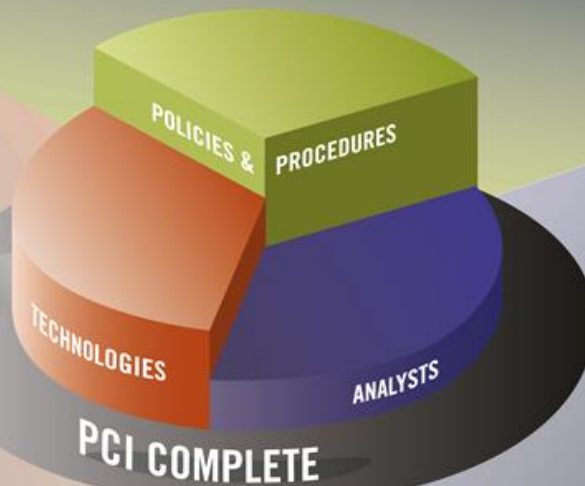
- ✓ Firewall
- ✓ Intrusion Detection & Prevention
- ✓ SSL and IPsec VPN
- ✓ Multi-Factor Authentication
- ✓ Security Event Log Management and Monitoring
- ✓ Internal Vulnerability Scanning
- ✓ External Vulnerability Scanning
- ✓ Web Application Firewall
- ✓ File Integrity Monitoring

Policies & procedures

- ✓ 24x7 QSA-approved and SSAE 16 Type II audited SOCs
- ✓ Change control management for services provided
- ✓ Daily event review of all security event log files
- ✓ 6 month firewall and Web application firewall rule configuration reviews
- ✓ Alert escalation procedures
- ✓ Incident response procedures

Analysts

- ✓ 24 x 7 coverage from expert analysts
- ✓ Expertise on PCI management
- ✓ Rapid response to security events
- ✓ Rapid response to incoming customer inquiries—"third ring" service pledge
- ✓ World-wide threat monitoring





HIPAA Compliance Framework

The **Privacy Rule** defines and limits the circumstances in which individual identifiable health information may be used or disclosed by covered entities. This information includes demographic data such as name, address, birth date, Social Security Number and information that relates to:

- The individual's past, present, or future physical or mental health or condition
- The provision of healthcare to the individual
- The past, present, or future payment for the provision of healthcare to the individual

The Privacy Rule calls this information Protected Health Information (PHI)

The **Security Rule** covers the protection of the confidentiality, integrity, and availability of electronic protected health information (ePHI). It prescribes a number of required policies, procedures, and reporting mechanisms that must be in place for all information systems that process, store, and transmit ePHI within and between covered entities and contains multiple proposed requirements (or standards) and implementation specifications designed to protect the confidentiality, integrity and availability of ePHI within each enterprise. These specifications fall into five categories:

1. Administrative Safeguards (§
2. Physical Safeguards (§164.310)
3. Technical Safeguards (§164.312)
4. Organizational Requirements (§164.314)
5. Policies and Procedures (§164.316)



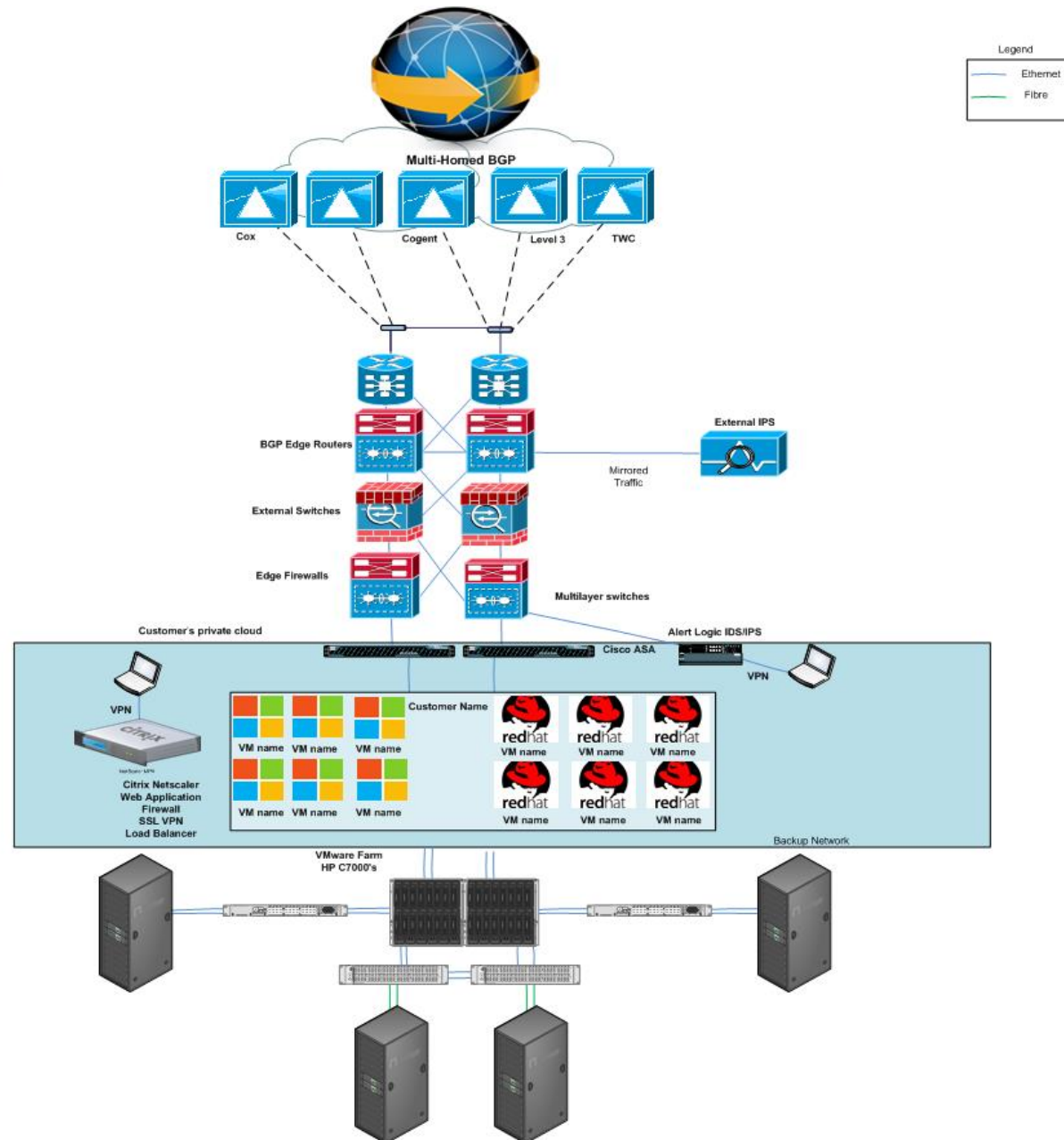
HIPAA Compliance

HIPAA Compliance Roles and Responsibilities Checklist

SMS Shared Customer

Physical Security	(Datacenter, Infrastructure)	<input checked="" type="checkbox"/>		
Perimeter Security	(IP reputation filtering, DDoS mitigation)	<input checked="" type="checkbox"/>		
Application Security	(WAF, OS, webserver, database patching)	<input checked="" type="checkbox"/>		
Network Security	(IDS/IPS, hypervisor firewall, vulnerability mgmt, SSL certs)	<input checked="" type="checkbox"/>		
Server Security	(Hardened OS, patching, anti-virus, log mgmt)	<input checked="" type="checkbox"/>		
Administrative Security	(Secure access, two-factor authentication)	<input checked="" type="checkbox"/>		
Data Backup	(Nightly volume based, client based, custom retention)	<input checked="" type="checkbox"/>		
Secure Data Deletion	(Secure deletion upon service termination)	<input checked="" type="checkbox"/>		
Security Audits	(PCI, HITECH, SOC2/SAS70, ISO 27001, Vulnerability Scans)	<input checked="" type="checkbox"/>		
Access Control	(Logical access control to server)		<input checked="" type="checkbox"/>	
Maintain Policies	(Security policies and procedures)		<input checked="" type="checkbox"/>	
Change Control	(Firewall changes, OS Patching)		<input checked="" type="checkbox"/>	
Incident Response	(For customer servers)		<input checked="" type="checkbox"/>	
Risk Assessment	(Annual risk assessment)		<input checked="" type="checkbox"/>	
Data Management	(DBA duties, encryption)		<input checked="" type="checkbox"/>	
Application Management	(Customer specific applications)			<input checked="" type="checkbox"/>

Reference Architecture





Partners and Service Providers



Why Grupo SMS?

Benefits for Enterprises

- ❖ Local specialist in cloud computing, managed services, and professional services
- ❖ Support via onsite meetings, phone, or email
- ❖ We offer customizable solutions and think outside of the box
- ❖ The scale to meet our customers needs
- ❖ Avoid “Cloud Lock”. Unlike others our service is local, accessible, portable, and a client is always able to access their data onsite.
- ❖ Provide BGP Multi-homed bandwidth and inexpensive Layer 2 connectivity
- ❖ Monitoring and onsite access 24/7/365
- ❖ Tier 3+ Data Center

