PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1 2	Install and maintain a firewall configuration to protect cardholder data. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3 4	Protect stored cardholder data Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5 6	Protect all systems against malware and regularly update anti-virus software or programs Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7 8 9	Restrict access to cardholder data by business need to know Identify and authenticate access to system components. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10 11	Track and monitor all access to network resources and cardholder data Regularly test security systems and processes
Maintain an Information Security Policy	12	Maintain a policy that addresses information security for all personnel

Normas de seguridad de datos de la PCI: descripción general de alto nivel

Desarrollar y mantener una red segura	**1.** Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta **2.** No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores
Proteger los datos del titular de la tarjeta	**3.** Proteja los datos del titular de la tarjeta que fueron almacenados **4.** Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas
Mantener un programa de administración de vulnerabilidad	**5.** Utilice y actualice con regularidad los programas o software antivirus **6.** Desarrolle y mantenga sistemas y aplicaciones seguras
Implementar medidas sólidas de control de acceso	**7.** Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa **8.** Asignar una ID exclusiva a cada persona que tenga acceso por computador **9.** Restringir el acceso físico a los datos del titular de la tarjeta
Supervisar y evaluar las redes con regularidad	**10.** Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas **11.** Pruebe con regularidad los sistemas y procesos de seguridad
Mantener una política de seguridad de información	**12.** Mantenga una política que aborde la seguridad de la información para todo el personal

Build and Maintain a Secure Network and Systems	1 2	Linux, IPTABLES Control Never
Protect Cardholder Data	3 4	Encrypted Without access to public network
Maintain a Vulnerability Management Program	5 6	Minimum quarterly updates Linux + PMS 23 years old
Implement Strong Access Control Measures	7 8 9	Without access Accessibility total control personnel identification only Without access
Regularly Monitor and Test Networks	10 11	Each access is mandatory individual identification generating logs for verification Minimum quarterly updates
Maintain an Information Security Policy	12	Regulatory Compliance (LOPD)