

**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**



**Facultad de Ingeniería en Electricidad y Computación**

**Maestría en Seguridad Informática Aplicada**

**“ASEGURAMIENTO DE SISTEMA OPERATIVO RED  
HAT 6.6 ENTERPRISE PARA CUMPLIMIENTO DE  
NORMATIVA PCI DSS 3.0”**

**EXAMEN DE GRADO (COMPLEXIVO)**

**Previa a la obtención del Título de:**

**MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA**

**Presentado por**

**PEDRO JOSÉ ROBLES TOMALÁ**

**Guayaquil – Ecuador**

**2015**

## AGRADECIMIENTO

Mi agradecimiento a Dios por permitirme llegar hasta este momento tan importante de mi carrera, María por su guía de toda una vida, a mis padres, hermanos, mi sobrino, mi niña, familia y amigos que estuvieron pendientes en todo momento del resultado de este proyecto.

Al Ing. Lenin Freire por el apoyo y la invitación a formar parte de este grupo.

Y muy particularmente a aquellos que creyeron posible el que pueda llegar hasta aquí y me siguen apoyando en cada paso y decisión de mi vida, a todos ellos mi cariño y lo que con este proyecto pueda lograr. Va por cada uno de ellos. G.I, E.R, F.G. P.R, C.T y S.G.

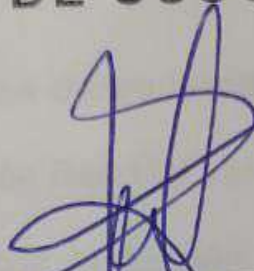
QCD? YDDD? YDDM?

## DEDICATORIA

A Dios en primer lugar y a María por su compañía incondicional.

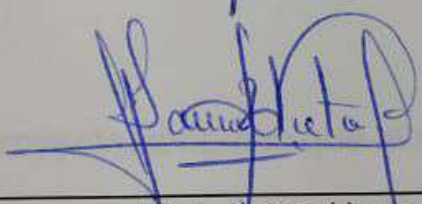
Dedico este regalo de Dios a tres personas muy importantes que siempre estuvieron conmigo y estarán sobre todo en mi corazón, Gustavo Robles, Raúl Tomalá y Carmen Ruiz, mi motivación para seguir adelante cada día buscando honrarlos con cada acción por todo lo que me han enseñado.

## TRIBUNAL DE SUSTENTACIÓN



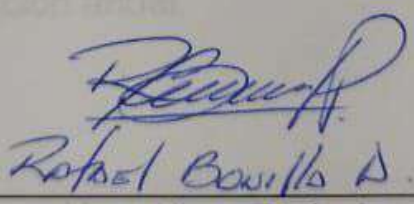
---

Ing. Lenín Freire  
DIRECTOR DEL MSIA



---

Mgs. Laura Ureta  
PROFESOR DELEGADO  
POR LA UNIDAD ACADÉMICA



---

Mgs. Albert Espinal  
PROFESOR DELEGADO  
POR LA UNIDAD ACADÉMICA

## RESUMEN

Como objetivo de este trabajo, se desea realizar el aseguramiento del sistema operativo LINUX en su distribución Red Hat versión 6.6 Enterprise a ser utilizado para un servidor que cumple con la función de switch transaccional en una empresa que presta servicios de interconexión de instituciones financieras.

Como antecedentes al proyecto, tenemos que la normativa PCI DSS dentro de su versión 3.0 incluyó el aseguramiento de la plataforma operativa como un requerimiento primario dentro de su auditoría tanto de certificación como de cumplimiento para la renovación anual.

Con este proyecto, la empresa podrá contar con una plataforma operativa aprobada por el ente certificador y sus QSA's (Asesores de calidad autorizados) responsables de realizar la validación.

Con ello lograremos que la empresa cuente con el nivel requerido de seguridad, que permitirá que su credibilidad tanto a nivel nacional como internacional crezca

y permanezca siendo considerada una de las más fuertes en el mercado de switches transaccionales.

## ÍNDICE GENERAL

AGRADECIMIENTO.....	ii
DEDICATORIA.....	iii
TRIBUNAL DE SUSTENTACIÓN.....	iv
RESUMEN.....	v
ÍNDICE GENERAL.....	vii
ABREVIATURAS.....	ix
ÍNDICE DE FIGURAS.....	xi
INTRODUCCIÓN.....	xiv
CAPÍTULO 1: GENERALIDADES.....	1
1.1 Antecedentes .....	1
1.2 Objetivo general.....	2
1.3 Objetivos específicos .....	2
1.4 Descripción del problema.....	3
1.5 Solución propuesta.....	4
1.6 Términos y acuerdos.....	5
CAPÍTULO 2: LEVANTAMIENTO DE INFORMACIÓN DEL EQUIPO.....	6

2.1 Auditoria de seguridad recomendada PCI/DSS 3.0. ....	7
2.2 Recopilación detalle de vulnerabilidades encontradas.....	9
2.3 Elaboración de plan de ejecución para el aseguramiento del Sistema Operativo.....	17
CAPÍTULO 3: EJECUCIÓN DEL ASEGURAMIENTO DEL EQUIPO.....	20
3.1 Remover servicios por defecto.....	21
3.2 Servicios de propósitos especiales.....	25
3.3 Configuración de red y firewall.....	28
3.4 Protocolos de red poco comunes.....	30
3.5 Logs del sistema.....	31
3.6 Configuración SSH.....	32
3.7 Configuraciones PAM.....	34
3.8 Cuentas de Usuario y ambientes.....	35
3.9 Banners de advertencia.....	37
CONCLUSIONES Y RECOMENDACIONES.....	38
GLOSARIO.....	41
BIBLIOGRAFIA.....	44



## ABREVIATURAS

<b>PCI DSS</b>	Estándar de Seguridad de Datos para Industria de Tarjetas de Crédito
<b>QSA</b>	Consultor de Calidad de Seguridad
<b>SSH</b>	Intérprete de Órdenes Seguro
<b>PAM</b>	Mecanismo de Autenticación Flexible
<b>NFS</b>	Sistema de Archivos de Red
<b>RPC</b>	Llamada a Procedimiento Remoto
<b>TELNET</b>	Red de Telecomunicaciones
<b>RSH</b>	Intérprete de Órdenes Remoto
<b>TFTP</b>	Protocolo de Transferencia de Archivos Trivial
<b>UDP</b>	Protocolo de Intercambio de Datagramas
<b>TCP</b>	Protocolo de Control de Transmisión
<b>NIS</b>	Servicio de Información de Red
<b>DHCP</b>	Protocolo de Configuración Dinámica de Host
<b>LDAP</b>	Protocolo Ligero de Acceso a Directorios

<b>NTP</b>	Protocolo de Tiempo de la Red
<b>DNS</b>	Sistema de Nombres de Dominio
<b>FTP</b>	Protocolo de Transferencia de Archivos
<b>HTTP</b>	Protocolo de Transferencia de Hipertexto
<b>SMNP</b>	Protocolo Simple de Administración de Red
<b>IP</b>	Protocolo de Internet
<b>ICMP</b>	Protocolo de Mensajes de Control de Internet
<b>SYN</b>	Bit de Control del Segmento TCP

## ÍNDICE DE FIGURAS

Figura 2.1: Verificación de configuraciones datagram por defecto.....	9
Figura 2.2: Verificación de configuración echo-stream .....	10
Figura 2.3: Verificación de configuraciones para máscara por defecto .....	10
Figura 2.4: Verificación de configuraciones NFS y RPC .....	11
Figura 2.5: Verificación de servicios de propósitos especiales .....	11
Figura 2.6: Verificación de configuraciones de red y firewall .....	12
Figura 2.7: Verificación de configuraciones redirección y enrutamiento de Paquetes .....	12
Figura 2.8: Verificación de protocolos de red poco comunes .....	13
Figura 2.9: Verificación de configuraciones Rsyslog .....	13
Figura 2.10: Verificación de parámetros en archivo rsyslog.conf .....	13
Figura 2.11: Verificación de parámetros por defecto en rsyslog.conf .....	14
Figura 2.12: Verificación de configuraciones SSH .....	14
Figura 2.13: Verificación de parámetros y configuraciones SSH .....	14
Figura 2.14: Verificación de configuraciones PAM .....	15
Figura 2.15: Verificación de configuraciones de usuarios. ....	15
Figura 2.16: Verificación de configuración de máscara por defecto .....	16
Figura 2.17: Verificación de configuraciones banners de advertencia .....	16

Figura 3.1: Remover servicio de servidor Telnet .....	21
Figura 3.2: Remover paquete de Telnet .....	21
Figura 3.3: Remover servicio de servidor RSH .....	21
Figura 3.4: Remover servicio de información de red.....	22
Figura 3.5: Remover paquete de servicio TFTP .....	22
Figura 3.6: Remover servicio de servidor TFTP .....	22
Figura 3.7: Remover controlador de servicios extendidos de internet .....	22
Figura 3.8: Remover servicio de generación de caracteres .....	22
Figura 3.9: Remover servicio de envío de fecha actual .....	23
Figura 3.10: Remover servicio de generación de mensajería de control Por protocolo UDP .....	23
Figura 3.11: Remover servicio de generación de mensajería de control por flujos .....	23
Figura 3.12: Remover servicio de multiplexado de protocolo TCP .....	23
Figura 3.13: Remover servicios de propósito especiales .....	25
Figura 3.14: Ajustar parámetros de servicios de propósito especiales.....	26
Figura 3.15: Desinstalar y Remover servicios de propósito especiales .....	27
Figura 3.16: Parámetros para servicios de red y firewalls .....	28
Figura 3.17: Remover configuraciones para redireccionamiento de paquetes.....	29

Figura 3.18: Parámetros para servicios de red poco comunes .....	30
Figura 3.19: Aseguramiento de Log's del sistema .....	31
Figura 3.20: Ajuste en parámetros SSH .....	32
Figura 3.21: Remover permisos de acceso a archivos de configuración en directorio /etc/ssh .....	33
Figura 3.22: Ajuste en configuración PAM .....	34
Figura 3.23: Confirmación de ejecución de aseguramiento para PAM .....	34
Figura 3.24: Ajuste en parámetros de usuarios .....	35
Figura 3.25: Ajuste en configuración de Banners de advertencia .....	37

## INTRODUCCIÓN

Se adquirió un servidor HP con una solución que requiere una plataforma operativa LINUX, por lo que se solicitó la evaluación de los sistemas operativos que aplican para soportar operativamente dicha aplicación, por lo que la recomendación fue de utilizar un sistema operativo REDHAT LINUX en su versión aprobada más actualizada para empresas que es la 6.6 [1].

Dentro del proceso de preparación del servidor, se procedió con la instalación de la aplicación previo al versionamiento con la finalidad de validar la correcta transaccionalidad del mismo, se verificó que se cumplió con el funcionamiento correcto según fue indicado por el proveedor externo responsable de la preparación de los ambientes.

Con los resultados obtenidos, se solicitó el aseguramiento del sistema operativo del servidor luego de la ejecución del demo de pruebas, motivo por el cual se inició este proyecto y del cual se espera obtener el mejor resultado con respecto al cumplimiento de la normativa.

# **CAPÍTULO 1**

## **GENERALIDADES**

### **1.1 Antecedentes**

En el campo financiero, la seguridad de la información se ha convertido en el punto más crítico para todas las instituciones que lo integran, tanto instituciones privadas como públicas en la actualidad se encuentran realizando arduos trabajos para garantizar la seguridad de sus clientes y por medio de esto atraer la atención del mercado.



Basándonos en las estadísticas, los índices de fraude se han visto incrementados, por lo que la mayoría de instituciones financieras están optando por implementar mecanismos que les permitan minimizar el riesgo sobre las transacciones que en ellas se realiza, de ahí la concepción de este proyecto.

## **1.2 Objetivo General.**

Realizar el aseguramiento del sistema operativo Red Hat 6.6 Enterprise de un servidor transaccional orientado al cumplir requerimientos propuestos dentro de la normativa PCI/DSS 3.0. [2].

## **1.3 Objetivo Específico**

Detallar los pasos para la efectiva implementación del aseguramiento del sistema operativo para que se cumpla con los requerimientos indicados en la normativa

PCI/DSS 3.0, confirmando que no se afecte la transaccionalidad soportada por sus aplicativos.

#### **1.4 Descripción del Problema**

Actualmente, en nuestro medio existen un sinnúmero de casos en los que hemos podido evidenciar fraudes realizados tanto por personal interno como externo a las instituciones financieras. Por ello la Superintendencia de Bancos y Seguros del Ecuador (SBS) se vio en la necesidad de incluir dentro de sus resoluciones una normativa que detalla que las instituciones financieras sujetas a ella, deben cumplir con un conjunto de consideraciones de seguridad básicas, las cuales están incluidas en la normativa PCI DSS, brindando mayor seguridad y confianza a todos los usuarios de la banca ecuatoriana. Esta normativa se extiende hasta el desarrollo de soluciones que cuenten con los estándares de seguridad implementados en muchas instituciones financieras de nivel mundial.

Los sistemas operativos que se encuentran en el mercado cuentan con un nivel de seguridad mediano, el cual se encuentra en riesgo de ser atacado si no se encuentra debidamente asegurado.

Las normativas internacionales, siendo en este caso particular la PCI/DSS en su versión 3.0, han presentado a sus acreditados un nivel mínimo recomendado de seguridad dentro de sus plataformas tecnológicas para mantener dicha certificación, por lo que la empresa se ve en la necesidad de realizar este aseguramiento ya que el equipo en mención se considera dentro del dominio de la norma dado que por el fluye información sensible.

## **1.5 Solución Propuesta**

Se recomienda el aseguramiento del sistema operativo indicado, siendo en este caso RED HAT LINUX en su versión 6.6 Enterprise [4].

Este aseguramiento permitirá que tanto archivos de configuración como la información contenida en el mismo, al igual que la comunicación con los equipos a los que por medio de este se accede, cuenten con la configuración de seguridad idónea que nos permita el bloqueo de comunicación, enmascaramiento de datos y control de acceso restringido sin que este afecte a la transaccionalidad que se soporta.

Dentro de las opciones a utilizarse tomamos en consideración los siguientes puntos:

- Análisis del sistema operativo previo a la implementación.
- Ubicación de los archivos de configuración.
- Reconfiguración de accesos de usuarios.
- Control de acceso y de sesiones.
- Configuración de redes y enlaces de comunicación.
- Configuración de puertos y red.
- Deshabilitación de servicios.

## **1.6 Términos y Acuerdos**

El proyecto se limita a la realización del aseguramiento del sistema operativo Red Hat en su versión 6.6 Enterprise instalado para el servidor transaccional, cubriendo con los requerimientos básicos solicitados por la entidad certificadora de la normativa PCI DSS v. 3.0 sobre los sistemas operativos Linux.

## **CAPÍTULO 2**

### **Levantamiento de información del equipo**

Este capítulo contiene el detalle de los procedimientos realizados mostrando sus respectivos resultados sobre la auditoría realizada al equipo sobre el que se está trabajando.

La información aquí obtenida es de suma importancia, ya que en base a ella se definirá el plan de acción al igual que el cronograma de trabajo que se presentará al cliente para completar con el requerimiento.

## 2.1. Auditoría de Seguridad Recomendada PCI/DSS 3.0

Dentro de la última actualización (versión 3.0), PCI DSS establece una serie de mejoras que deben ser consideradas para cada sistema operativo sobre el cual se recibirá transacciones que lleven números de tarjetas tanto de débito como de crédito.

Para poder determinar que configuraciones deben aplicarse en el sistema operativo, es conveniente en primer lugar, realizar una auditoría del mismo, la cual nos permita evaluar cada una de las vulnerabilidades y su mecanismo de remediación.

Las consideraciones que se deben tener en cuenta para el proceso de auditoría cubren los siguientes campos detallados a continuación:

- Actualizaciones y parches instalados
- Servicios del sistema operativo
- Servicios de propósitos especiales
- Configuración de red y firewall
- Logs y Auditoría
- Acceso a sistema, autenticación y autorización
- Cuentas de usuario y ambiente

- Banners de advertencia
- Mantenimiento del sistema

De las validaciones previas realizadas sobre el servidor, se pudo acordar, con el QSA asignado a la cuenta, los siguientes dominios, que contendrían todos los puntos requeridos para el cumplimiento de la norma según sus especificaciones, sin afectar el funcionamiento correcto de la herramienta:

1. Remover servicios por defecto
2. Servicios de propósitos especiales
3. Configuración de red y firewall
4. Protocolos de red poco comunes
5. Logs del sistema
6. Configuración SSH
7. Configuración PAM [3]
8. Cuentas de usuario y ambientes
9. Banners de advertencia

## 2.2. Recopilación detalle de vulnerabilidades encontradas

Se procedió con la revisión de los puntos indicados previamente, de los cuales obtuvimos los siguientes resultados:

```
[root@UPFSEVER ~]# chkconfig --list chargen-dgram
error al leer la información del servicio chargen-dgram: No existe el fichero o
el directorio
[root@UPFSEVER ~]# chkconfig --list chargen-stream
error al leer la información del servicio chargen-stream: No existe el fichero o
el directorio
[root@UPFSEVER ~]# chkconfig --list daytime-dgram
error al leer la información del servicio daytime-dgram: No existe el fichero o
el directorio
[root@UPFSEVER ~]# chkconfig --list daytime-stream
error al leer la información del servicio daytime-stream: No existe el fichero o
el directorio
[root@UPFSEVER ~]# chkconfig -- list echo-dgram
chkconfig versión 1.3.49.3 - Copyright (C) 1997-2000 Red Hat, Inc.
Este programa se distribuirá libremente distribuido con la
licencia pública de GNU.

uso:  chkconfig [--list] [--type <tipo>] [nombre]
      chkconfig --add <nombre>
      chkconfig --del <nombre>
      chkconfig --override <nombre>
      chkconfig [--level <niveles>] [--type <tipo>] <nombre> <on|off|reset|re
setpriorities>
[root@UPFSEVER ~]# _
```

Figura 2.1: Verificación de configuraciones datagram por defecto.



```
[root@UPFSERVER ~]# chkconfig -- list echo-stream
chkconfig versión 1.3.49.3 - Copyright (C) 1997-2000 Red Hat, Inc.
Este programa se distribuirá libremente distribuido con la
licencia pública de GNU.

Uso:  chkconfig [--list] [--type <tipo>] [nombre]
      chkconfig --add <nombre>
      chkconfig --del <nombre>
      chkconfig --override <nombre>
      chkconfig [--level <niveles>] [--type <tipo>] <nombre> <on|off|reset|re
setpriorities>
[root@UPFSERVER ~]# chkconfig --list tcpmux-server
error al leer la información del servicio tcpmux-server: No existe el fichero o
el directorio
[root@UPFSERVER ~]# _
```

Figura 2.2: Verificación de configuración echo-stream

```
[root@UPFSERVER ~]# grep umask/etc/sysconfig/init
^C
[root@UPFSERVER ~]# rpm -q xorg-x11-server-common
el paquete xorg-x11-server-common no está instalado
[root@UPFSERVER ~]# chkconfig --list avahi-daemon
error al leer la información del servicio avahi-daemon: No existe el fichero o e
l directorio
[root@UPFSERVER ~]# chkconfig --list cups
cups          0:desactivado  1:desactivado  2:activo      3:activo      4
:activo 5:activo  6:desactivado
[root@UPFSERVER ~]# rpm -q dhcp
el paquete dhcp no está instalado
[root@UPFSERVER ~]# grep "restrict default" /etc/ntp.conf
restrict default kod nomodify notrap nopeer noquery
[root@UPFSERVER ~]# grep "restrict-6 default" /etc/ntp.conf
[root@UPFSERVER ~]# grep "restrict-6 default" /etc/ntp.conf
[root@UPFSERVER ~]# grep "ntp:ntp" /etc/sysconfig/ntpd
# Drop root to id 'ntp:ntp' by default.
OPTIONS="-u ntp:ntp -p /var/run/ntpd.pid -g"
[root@UPFSERVER ~]# rpm -q openldap-servers
el paquete openldap-servers no está instalado
[root@UPFSERVER ~]# rpm -q openldap-clients
el paquete openldap-clients no está instalado
[root@UPFSERVER ~]# _
```

Figura 2.3: Verificación de configuraciones para máscara por defecto

```

[root@UPFSERVER ~]# chkconfig --list nfslock
nfslock      0:desactivado  1:desactivado  2:desactivado  3:activo      4
:activo 5:activo      6:desactivado
[root@UPFSERVER ~]# chkconfig --list rpcgssd
rpcgssd      0:desactivado  1:desactivado  2:desactivado  3:activo      4
:activo 5:activo      6:desactivado
[root@UPFSERVER ~]# chkconfig --list rpcbind
rpcbind      0:desactivado  1:desactivado  2:activo       3:activo      4
:activo 5:activo      6:desactivado
[root@UPFSERVER ~]# chkconfig --list rpcidmapd
rpcidmapd    0:desactivado  1:desactivado  2:desactivado  3:activo      4
:activo 5:activo      6:desactivado
[root@UPFSERVER ~]# chkconfig --list rpcsvcgssd
error al leer la información del servicio rpcsvcgssd: No existe el fichero o el
directorio
[root@UPFSERVER ~]# chkconfig --list rpcsvcgssd
rpcsvcgssd   0:desactivado  1:desactivado  2:desactivado  3:desactivado  4
:desactivado 5:desactivado 6:desactivado
[root@UPFSERVER ~]# rpm -qbind
-qbind: opción desconocida
[root@UPFSERVER ~]# rpm -q bind
el paquete bind no está instalado
[root@UPFSERVER ~]# _

```

Figura 2.4: Verificación de configuraciones NFS y RPC

```

[root@UPFSERVER ~]# rpm -q vsftpd
el paquete vsftpd no está instalado
[root@UPFSERVER ~]# rpm -q httpd
el paquete httpd no está instalado
[root@UPFSERVER ~]# rpm -q dovecot
el paquete dovecot no está instalado
[root@UPFSERVER ~]# rpm -q samba
el paquete samba no está instalado
[root@UPFSERVER ~]# rpm -q squid
el paquete squid no está instalado
[root@UPFSERVER ~]# rpm -q net-snmp
el paquete net-snmp no está instalado
[root@UPFSERVER ~]# netstat -an | grep LIST | grep ":25[[:space:]]"
tcp        0      0 127.0.0.1:25          0.0.0.0:*           LISTEN
tcp        0      0 :::1:25              :::*                 LISTEN
[root@UPFSERVER ~]# _

```

Figura 2.5: Verificación de servicios de propósitos especiales

```

[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.conf.all.send_redirects
net.ipv4.conf.all.send_redirects = 1
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.conf.all.accept_source_route
net.ipv4.conf.all.accept_source_route = 0
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.conf.default.accept_source_route
net.ipv4.conf.default.accept_source_route = 0
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.conf.default.accept_redirects
net.ipv4.conf.default.accept_redirects = 1
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.conf.all.accept_redirects
net.ipv4.conf.all.accept_redirects = 1
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.conf.all.secure_redirects
net.ipv4.conf.all.secure_redirects = 1
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.conf.default.secure_redirects
net.ipv4.conf.default.secure_redirects = 1
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.conf.all.log_martians
net.ipv4.conf.all.log_martians = 0
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.conf.default.log_martians
net.ipv4.conf.default.log_martians = 0
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.icmp_echo_ignore_broadcasts
net.ipv4.icmp_echo_ignore_broadcasts = 1
[root@UPFSERVER ~]# _

```

Figura 2.6: Verificación de configuraciones de red y firewall

```

[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.icmp_ignore_bogus_error_responses
net.ipv4.icmp_ignore_bogus_error_responses = 1
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.conf.all.rp_filter
net.ipv4.conf.all.rp_filter = 0
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.conf.default.rp_filter
net.ipv4.conf.default.rp_filter = 1
[root@UPFSERVER ~]# /sbin/sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 1
[root@UPFSERVER ~]# _

```

Figura 2.7: Verificación de configuraciones redirección y enrutamiento de paquetes

```

[root@UPFSERVER ~]# grep "install dccp/bin/true"
^C
[root@UPFSERVER ~]# grep "install sctp/bin/true"
^C
[root@UPFSERVER ~]# grep "install rds/bin/true"
^C
[root@UPFSERVER ~]# grep "install tipc/bin/true"
^C
[root@UPFSERVER ~]# chkconfig --list iptables
iptables          0:desactivado  1:desactivado  2:activo        3:activo        4
:activo 5:activo  6:desactivado
[root@UPFSERVER ~]# _

```

Figura 2.8: Verificación de protocolos de red poco comunes

```

[root@UPFSERVER ~]# rpm -q rsyslog
rsyslog-5.8.10-6.el6.x86_64
[root@UPFSERVER ~]# chkconfig --list syslog
error al leer la información del servicio syslog: No existe el fichero o el directorio
[root@UPFSERVER ~]# chkconfig --list rsyslog
rsyslog           0:desactivado  1:desactivado  2:activo        3:activo        4
:activo 5:activo  6:desactivado
[root@UPFSERVER ~]# _

```

Figura 2.9: Verificación de configuraciones Rsyslog

```

-rw-----, 1 root root 57040 jul 28 18:11 anaconda.xlog
-rw-----, 1 root root 64821 jul 28 18:11 anaconda.yum.log
drwxr-x---, 2 root root 4096 jul 31 23:12 audit
-rw-r--r--, 2 root root 2861 jul 31 23:12 boot.log
-rw-----, 1 root utmp 1536 jul 31 23:13 btmp
drwxr-xr-x, 2 root root 4096 jul 31 23:13 ConsoleKit
-rw-----, 1 root root 1981 ago 1 01:20 cron
drwxr-xr-x, 2 lp sys 4096 nov 6 2012 cups
-rw-r--r--, 1 root root 21569 jul 31 23:12 dmesg
-rw-r--r--, 1 root root 161260 jul 28 18:11 dracut.log
-rw-r--r--, 1 root root 146000 jul 31 23:13 lastlog
-rw-----, 1 root root 197 jul 31 23:12 maillog
-rw-r--r--, 1 root root 0 jul 31 23:12 mcelog
-rw-----, 1 root root 30998 jul 31 23:13 messages
drwxr-xr-x, 2 ntp ntp 4096 ene 10 2013 ntpstats
drwxr-xr-x, 2 root root 4096 oct 20 2011 prelink
drwxr-xr-x, 2 root root 4096 jul 31 23:14 rhsm
drwxr-xr-x, 2 root root 4096 ago 1 00:00 sa
drwx-----, 3 root root 4096 jul 28 18:08 samba
-rw-----, 1 root root 1360 jul 31 23:13 secure
-rw-----, 1 root root 0 jul 28 18:08 spooler
drwxr-x---, 2 root root 4096 ene 23 2013 sssd
-rw-----, 1 root root 0 jul 28 18:06 tallylog
-rw-rw-r--, 1 root utmp 4224 jul 31 23:13 wtmp
[root@UPFSERVER ~]# _

```

Figura 2.10: Verificación de parámetros en archivo rsyslog.conf

```
[root@UPFSERVER ~]# grep '$ModLOAD imtcp.so' /etc/rsyslog.conf
[root@UPFSERVER ~]# grep '$InputTCPServerRun' /etc/rsyslog.conf
#$InputTCPServerRun 514
[root@UPFSERVER ~]# _
```

Figura 2.11: Verificación de parámetros por defecto en rsyslog.conf

```
[root@UPFSERVER ~]# grep "Protocol" /etc/ssh/sshd_config
Protocol 2
[root@UPFSERVER ~]# grep "LogLevel" /etc/ssh/sshd_config
#LogLevel INFO
[root@UPFSERVER ~]# grep "X11Forwarding"
^C
[root@UPFSERVER ~]# grep "MaxAuthTries"
^C
[root@UPFSERVER ~]# grep "IgnoreRhosts"
^C
[root@UPFSERVER ~]# grep "HostbasedAuthentication"
^C
[root@UPFSERVER ~]# grep "PermitRootLogin"
^C
[root@UPFSERVER ~]# grep "PermitEmptyPasswords"
^C
[root@UPFSERVER ~]# grep "PermitUserEnviroments"
^C
[root@UPFSERVER ~]# grep PermitUserEnviroments
^C
[root@UPFSERVER ~]# grep "Ciphers" /etc/ssh/sshd_config
[root@UPFSERVER ~]# grep "ClentAliveCountMax" /etc/ssh/sshd_config
[root@UPFSERVER ~]# _
```

Figura 2.12: Verificación de configuraciones SSH

```
[root@UPFSERVER ~]# grep "AllowUsers" /etc/ssh/sshd_config
[root@UPFSERVER ~]# grep "AllowGroups" /etc/ssh/sshd_config
[root@UPFSERVER ~]# grep "DenyUsers" /etc/ssh/sshd_config
[root@UPFSERVER ~]# grep "DenyGroups" /etc/ssh/sshd_config
[root@UPFSERVER ~]# grep "Banner" /etc/ssh/sshd_config
#Banner none
[root@UPFSERVER ~]# _
```

Figura 2.13: Verificación de parámetros y configuraciones SSH

```

[root@UPFSERVER ~]# authconfig --test | grep hashing | grep sha512
password hashing algorithm is sha512
[root@UPFSERVER ~]# grep pam_cracklib.so /etc/pam.d/system-auth
password requisite pam_cracklib.so try_first_pass retry=3 type=
[root@UPFSERVER ~]# grep "pam_faillock" /etc/pam.d/password-auth |grep success_1
[root@UPFSERVER ~]# grep "pam_faillock" /etc/pam.d/password-auth |grep success=1

[root@UPFSERVER ~]# grep "pam_faillock" /etc/pam.d/password-auth |grep success=1
[root@UPFSERVER ~]# grep "pam_faillock" /etc/pam.d/system-auth
[root@UPFSERVER ~]# grep "pam_unix.so" /etc/pam.d/system-auth |grep success=1
[root@UPFSERVER ~]# grep "remember" /etc/pam.d/system-auth
[root@UPFSERVER ~]# cat/etc/securetty
-bash: cat/etc/securetty: No existe el fichero o el directorio
[root@UPFSERVER ~]# grep pam_wheel.so /etc/pam.d/su
#auth sufficient pam_wheel.so trust use_uid
#auth required pam_wheel.so use_uid
[root@UPFSERVER ~]# grep wheel /etc/group
wheel:x:10:
[root@UPFSERVER ~]# _

```

Figura 2.14: Verificación de configuraciones PAM

```

[root@UPFSERVER ~]# grep PASS_MAX_DAYS /etc/login.defs
# PASS_MAX_DAYS Maximum number of days a password may be used.
PASS_MAX_DAYS 99999
[root@UPFSERVER ~]# chage --list root
Last password change : Jul 28, 2015
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
[root@UPFSERVER ~]# chage --list qauser
Last password change : Aug 01, 2015
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
[root@UPFSERVER ~]# grep "root" /etc/passwd | cut -f4 -d:
0
0
[root@UPFSERVER ~]# _

```

Figura 2.15: Verificación de configuraciones de usuarios.

```

[root@UPFSERVER ~]# grep "umask 077" /etc/bashrc
[root@UPFSERVER ~]# grep "umask 077" /etc/profile.d/*
[root@UPFSERVER ~]# useradd -D | grep INACTIVE
INACTIVE=-1
[root@UPFSERVER ~]# _

```

Figura 2.16: Verificación de configuración de máscara por defecto.

```

[root@UPFSERVER ~]# ls /etc/issue
/etc/issue
[root@UPFSERVER ~]# egrep '(\\v|\\r|\\m|\\s)' /etc/issue
Kernel \\r on an \\m
[root@UPFSERVER ~]# egrep '(\\v|\\r|\\m|\\s)' /etc/motd
[root@UPFSERVER ~]# egrep '(\\v|\\r|\\m|\\s)' /etc/issue.net
Kernel \\r on an \\m
[root@UPFSERVER ~]# _

```

Figura 2.17: Verificación de configuraciones banners de advertencia

De la revisión realizada sobre los resultados obtenidos como parte de la auditoría llevada a cabo sobre la configuración del sistema operativo encontramos las siguientes novedades:

- Existen paquetes que no están instalados debido a que no se incluyen dentro de la instalación original del sistema operativo.
- Existen directorios que no fueron encontrados, por lo que se procede al registro de dichas novedades.
- El usuario root se encuentra habilitado y con el se realizará el proceso de aseguramiento, luego de ello se procederá con su inhabilitación.

- Se procedió a crear un usuario de prueba, el mismo que demostró contener permisos de administración, excluyendo la caducidad de la clave, posibilidad de inhabilitación e inhabilitación posterior de cuenta por expiración.
- El syslog se encuentra deshabilitado, sin embargo el rsyslog permanece activo y está registrando actividad que podría realizarse en el syslog.

### **2.3. Elaboración del plan de ejecución para el aseguramiento del sistema operativo.**

Para poder ejecutar el aseguramiento del servidor indicado, se estableció un plan de acción por medio del cual se remediarán las inconformidades registradas durante la auditoría preliminar, mismo que se ejecutará tomando en consideración lo siguiente:

- Se validará la funcionalidad del equipo antes de iniciar con el proceso de aseguramiento.
- Se verificará en conjunto con el QSA los resultados obtenidos con la ejecución de cada uno de los comandos indicados.
- Aunque el usuario root sea el que realice las configuraciones, este quedará deshabilitado, por lo que las validaciones de acceso se realizarán con el usuario administrador creado.



- Se deberá documentar los pasos a realizar con la finalidad de evidenciar cualquier novedad que pudiera presentarse.
- Previo a la ejecución de cada configuración se debe contar con su respectiva opción de reverso para que en caso de reportarse una novedad, la misma pueda ser solucionada inmediatamente.
- Se realizará una validación final de los resultados, con la que se dará por cerrado el proceso de aseguramiento, y el mismo deberá ser aprobado por el cliente.

Con las consideraciones mencionadas, los dominios que se procederá a verificar cubren los siguientes puntos:

- Servicios propios del sistema operativo que se encuentran en ejecución
- Servicios especiales requeridos por el aplicativo
- Configuraciones de entrada y salida de red
- Firewall interno del servidor
- Protocolos de red
- Logs del sistema
- Configuración SSH para acceso al sistema de forma remota
- Mecanismos de autenticación

- Cuentas de usuario
- Configuración de ambientes separados por etapa del ciclo de vida de los sistemas
- Alertas

## **CAPÍTULO 3**

### **Ejecución del aseguramiento del equipo.**

Finalmente, en este capítulo se detalla paso a paso como realizar el aseguramiento del servidor siguiendo tanto las recomendaciones de la norma PCI DSS como lo indicado por el asesor del ente certificador.

En base a lo indicado, dentro de esta etapa del proyecto, se presentará el resultado obtenido, mismo que nos brindará las evidencias suficientes para determinar el beneficio logrado para la institución.

### 3.1. Remover servicios por defecto



```
devuser@BRGUPP:~  
[devuser@BRGUPP ~]$ rpm -q telnet-server  
package telnet-server is not installed  
[devuser@BRGUPP ~]$
```

Figura 3.1: Remover servicio de servidor Telnet




```
devuser@BRGUPP:~  
[devuser@BRGUPP ~]$  
[devuser@BRGUPP ~]$ rpm -q telnet package  
telnet-0.17-48.el6.x86_64  
package package is not installed  
[devuser@BRGUPP ~]$
```

Figura 3.2: Remover paquete de Telnet



```
devuser@BRGUPP:~  
[devuser@BRGUPP ~]$ rpm -q rsh-server package  
package rsh-server is not installed  
package package is not installed  
[devuser@BRGUPP ~]$ rpm -q rsh  
package rsh is not installed  
[devuser@BRGUPP ~]$
```

Figura 3.3: Remover servicio de servidor RSH



```
devuser@BRGUPP:~  
[devuser@BRGUPP ~]$ rpm -q ypbind  
package ypbind is not installed  
[devuser@BRGUPP ~]$ rpm -q ypserv  
package ypserv is not installed  
[devuser@BRGUPP ~]$
```

Figura 3.4: Remover servicio de información de red.

```

devuser@BRGUPP:~
[devuser@BRGUPP ~]$ rpm -q tftp
package tftp is not installed
[devuser@BRGUPP ~]$

```

Figura 3.5: Remover paquete de servicio TFTP

```

devuser@BRGUPP:~
[devuser@BRGUPP ~]$ rpm -q tftp-server package
package tftp-server is not installed
package package is not installed
[devuser@BRGUPP ~]$

```

Figura 3.6: Remover servicio de servidor TFTP

```

devuser@BRGUPP:~
[devuser@BRGUPP ~]$ rpm -q xinetd
package xinetd is not installed
[devuser@BRGUPP ~]$

```

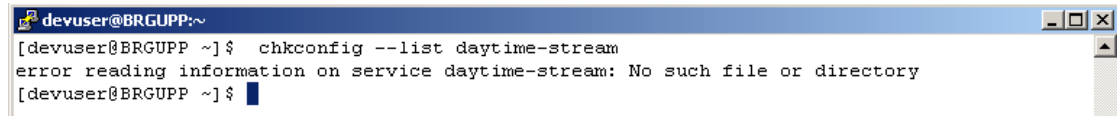
Figura 3.7: Remover controlador de servicios extendidos de internet.

```

devuser@BRGUPP:~
[devuser@BRGUPP ~]$ chkconfig --list chargin-dgram
error reading information on service chargin-dgram: No such file or directory
[devuser@BRGUPP ~]$ chkconfig --list chargin-stream
error reading information on service chargin-stream: No such file or directory
[devuser@BRGUPP ~]$ chkconfig --list daytime-dgram
error reading information on service daytime-dgram: No such file or directory
[devuser@BRGUPP ~]$

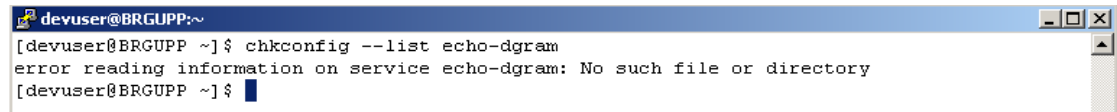
```

Figura 3.8: Remover servicio de generación de caracteres



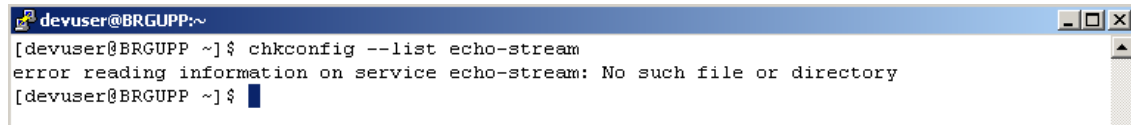
```
devuser@BRGUPP:~$ chkconfig --list daytime-stream
error reading information on service daytime-stream: No such file or directory
[devuser@BRGUPP ~]$
```

Figura 3.9: Remover servicio de envío de fecha actual



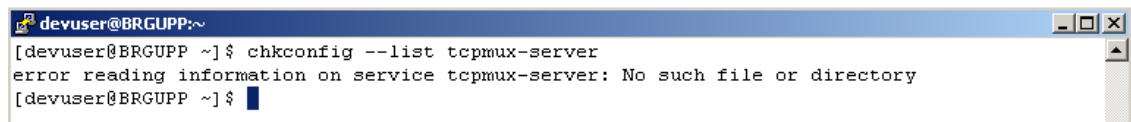
```
devuser@BRGUPP:~$ chkconfig --list echo-dgram
error reading information on service echo-dgram: No such file or directory
[devuser@BRGUPP ~]$
```

Figura 3.10: Remover servicio de generación de mensajería de control por protocolo UDP



```
devuser@BRGUPP:~$ chkconfig --list echo-stream
error reading information on service echo-stream: No such file or directory
[devuser@BRGUPP ~]$
```

Figura 3.11: Remover servicio de generación de mensajería de control por flujos



```
devuser@BRGUPP:~$ chkconfig --list tcpmux-server
error reading information on service tcpmux-server: No such file or directory
[devuser@BRGUPP ~]$
```

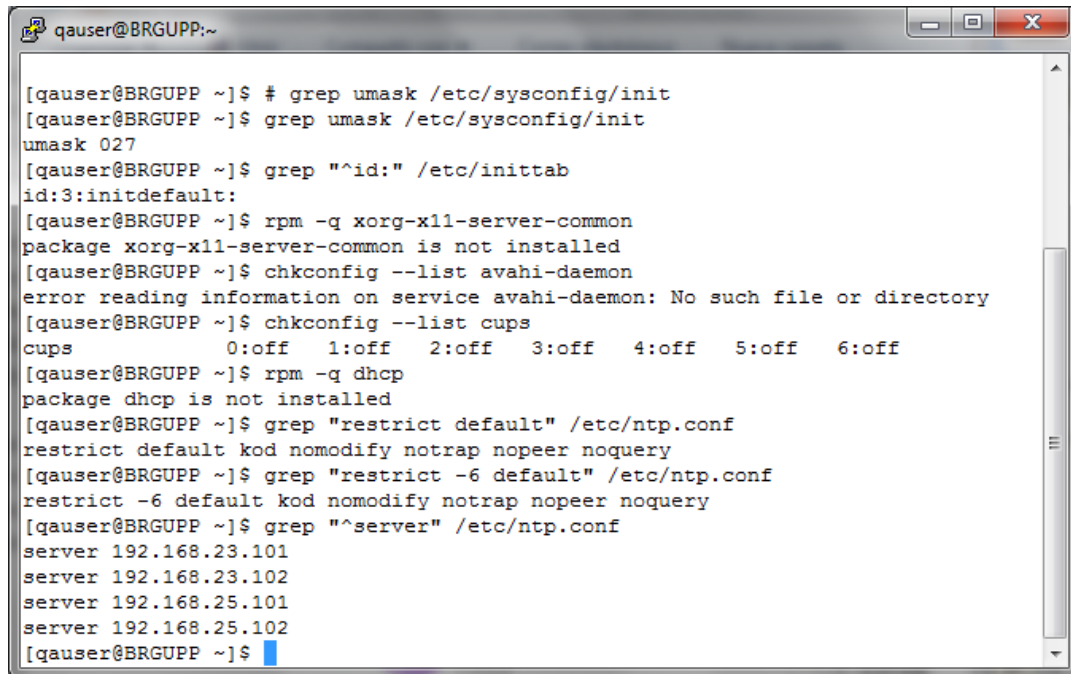
Figura 3.12: Remover servicio de multiplexado de protocolo TCP.

Como parte del proceso de aseguramiento se procedió a realizar las siguientes actividades:

- Remover servidor y cliente Telnet
- Remover servidor y cliente RSH

- Remover cliente y servidor NIS
- Remover tftp
- Remover tftp-server
- Remover xinetd
- Deshabilitar chargen-dgram
- Deshabilitar chargen-stream
- Deshabilitar daytime-dgram
- Deshabilitar daytime-stream
- Deshabilitar echo-dgram
- Deshabilitar echo-stream
- Deshabilitar tcpmux-server

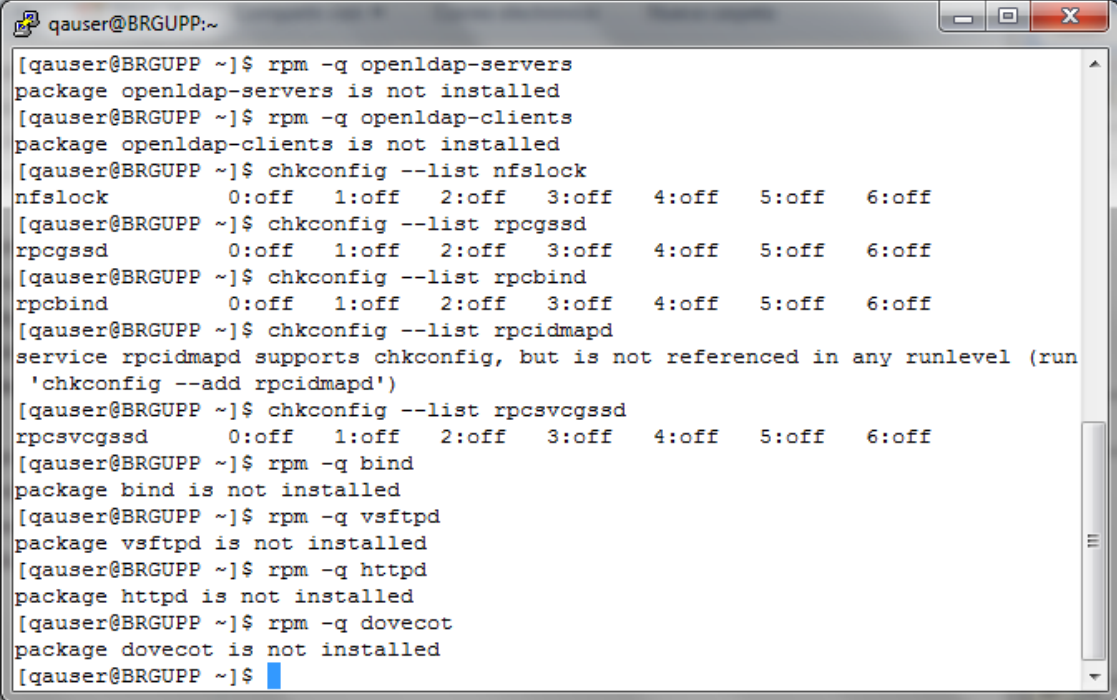
## 3.2. Servicios de propósitos especiales

A terminal window titled 'qauser@BRGUPP:~' showing a series of commands and their outputs. The commands include: 1. 'grep umask /etc/sysconfig/init' which outputs 'umask 027'. 2. 'grep "^id:" /etc/inittab' which outputs 'id:3:initdefault:'. 3. 'rpm -q xorg-x11-server-common' which outputs 'package xorg-x11-server-common is not installed'. 4. 'chkconfig --list avahi-daemon' which outputs an error: 'error reading information on service avahi-daemon: No such file or directory'. 5. 'chkconfig --list cups' which outputs 'cups 0:off 1:off 2:off 3:off 4:off 5:off 6:off'. 6. 'rpm -q dhcp' which outputs 'package dhcp is not installed'. 7. 'grep "restrict default" /etc/ntp.conf' which outputs 'restrict default kod nomodify notrap nopeer noquery'. 8. 'grep "restrict -6 default" /etc/ntp.conf' which outputs 'restrict -6 default kod nomodify notrap nopeer noquery'. 9. 'grep "^server" /etc/ntp.conf' which outputs four lines: 'server 192.168.23.101', 'server 192.168.23.102', 'server 192.168.25.101', and 'server 192.168.25.102'. The prompt '[qauser@BRGUPP ~]\$' is visible at the end of the terminal output.

```
[qauser@BRGUPP ~]$ # grep umask /etc/sysconfig/init
[qauser@BRGUPP ~]$ grep umask /etc/sysconfig/init
umask 027
[qauser@BRGUPP ~]$ grep "^id:" /etc/inittab
id:3:initdefault:
[qauser@BRGUPP ~]$ rpm -q xorg-x11-server-common
package xorg-x11-server-common is not installed
[qauser@BRGUPP ~]$ chkconfig --list avahi-daemon
error reading information on service avahi-daemon: No such file or directory
[qauser@BRGUPP ~]$ chkconfig --list cups
cups          0:off  1:off  2:off  3:off  4:off  5:off  6:off
[qauser@BRGUPP ~]$ rpm -q dhcp
package dhcp is not installed
[qauser@BRGUPP ~]$ grep "restrict default" /etc/ntp.conf
restrict default kod nomodify notrap nopeer noquery
[qauser@BRGUPP ~]$ grep "restrict -6 default" /etc/ntp.conf
restrict -6 default kod nomodify notrap nopeer noquery
[qauser@BRGUPP ~]$ grep "^server" /etc/ntp.conf
server 192.168.23.101
server 192.168.23.102
server 192.168.25.101
server 192.168.25.102
[qauser@BRGUPP ~]$
```

Figura 3.13: Remover servicios de propósito especiales.





```
qauser@BRGUPP:~  
[qauser@BRGUPP ~]$ rpm -q openldap-servers  
package openldap-servers is not installed  
[qauser@BRGUPP ~]$ rpm -q openldap-clients  
package openldap-clients is not installed  
[qauser@BRGUPP ~]$ chkconfig --list nfslock  
nfslock    0:off  1:off  2:off  3:off  4:off  5:off  6:off  
[qauser@BRGUPP ~]$ chkconfig --list rpcgssd  
rpcgssd    0:off  1:off  2:off  3:off  4:off  5:off  6:off  
[qauser@BRGUPP ~]$ chkconfig --list rpcbind  
rpcbind    0:off  1:off  2:off  3:off  4:off  5:off  6:off  
[qauser@BRGUPP ~]$ chkconfig --list rpcidmapd  
service rpcidmapd supports chkconfig, but is not referenced in any runlevel (run  
'chkconfig --add rpcidmapd')  
[qauser@BRGUPP ~]$ chkconfig --list rpcsvcgssd  
rpcsvcgssd 0:off  1:off  2:off  3:off  4:off  5:off  6:off  
[qauser@BRGUPP ~]$ rpm -q bind  
package bind is not installed  
[qauser@BRGUPP ~]$ rpm -q vsftpd  
package vsftpd is not installed  
[qauser@BRGUPP ~]$ rpm -q httpd  
package httpd is not installed  
[qauser@BRGUPP ~]$ rpm -q dovecot  
package dovecot is not installed  
[qauser@BRGUPP ~]$
```

Figura 3.14: Ajustar parámetros de servicios de propósito especiales.

```

qauser@BRGUPP:~
[qauser@BRGUPP ~]$ chkconfig --list rpcsvcgssd
rpcsvcgssd    0:off  1:off  2:off  3:off  4:off  5:off  6:off
[qauser@BRGUPP ~]$ rpm -q bind
package bind is not installed
[qauser@BRGUPP ~]$ rpm -q vsftpd
package vsftpd is not installed
[qauser@BRGUPP ~]$ rpm -q httpd
package httpd is not installed
[qauser@BRGUPP ~]$ rpm -q dovecot
package dovecot is not installed
[qauser@BRGUPP ~]$ clear
[qauser@BRGUPP ~]$ rpm -q samba
package samba is not installed
[qauser@BRGUPP ~]$ rpm -q squid
package squid is not installed
[qauser@BRGUPP ~]$ rpm -q net-snmp
package net-snmp is not installed
[qauser@BRGUPP ~]$ netstat -an | grep LIST | grep ":25[[:space:]]"
tcp        0      0 127.0.0.1:25          0.0.0.0:*             LISTEN
EN
tcp        0      0 :::1:25               :::*                   LISTEN
EN
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0

```

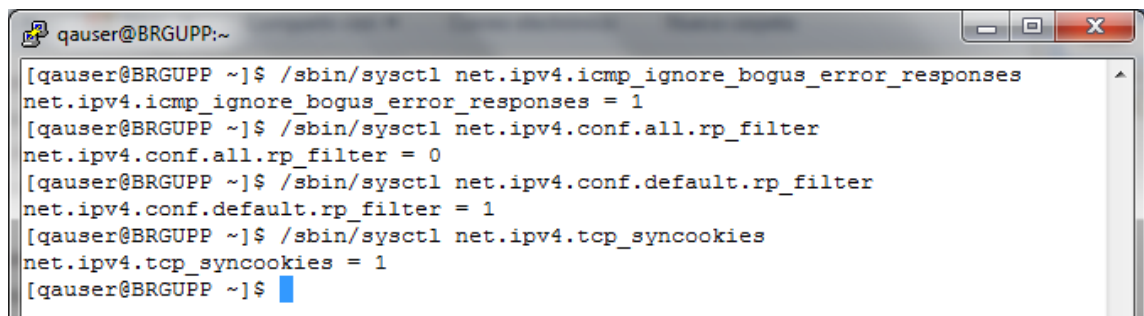
Figura 3.15: Desinstalar y Remover servicios de propósito especiales.

Para solventar las novedades evidenciadas en este punto, se procedió a:

- Configurar Daemon umask
- Remover X Window System
- Deshabilitar Avahi Server
- Deshabilitar Print Server - CUPS
- Remover DHCP Server
- Configurar NTP
- Remover LDAP
- Deshabilitar NFS Y RPC

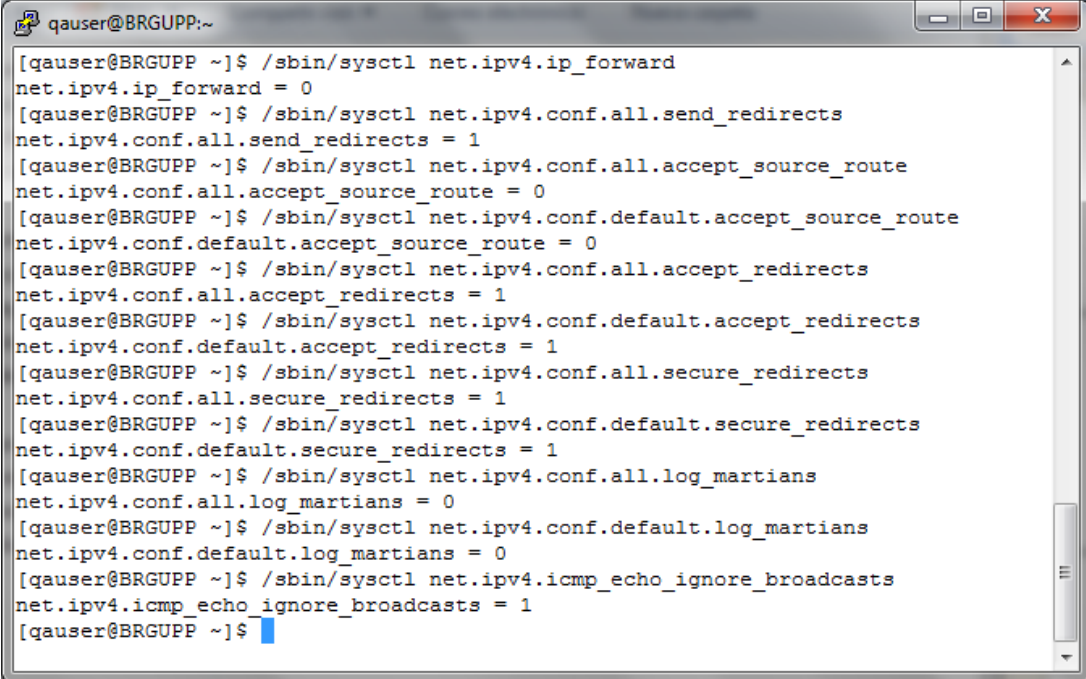
- Remover DNS Server
- Remover FTP Server
- Remvoer HTTP Server
- Remover Dovecot (IMAP Y POP3 Services)
- Remover Samba
- Remover HTTP Server
- Remover SNMP Server
- Configurar Mail Transfer Agent para Modo Local - Only

### 3.3. Configuración de red y firewall

A terminal window titled 'qauser@BRGUPP:~' showing a series of sysctl commands and their outputs. The commands are: 1. '/sbin/sysctl net.ipv4.icmp\_ignore\_bogus\_error\_responses' resulting in 'net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1'. 2. '/sbin/sysctl net.ipv4.conf.all.rp\_filter' resulting in 'net.ipv4.conf.all.rp\_filter = 0'. 3. '/sbin/sysctl net.ipv4.conf.default.rp\_filter' resulting in 'net.ipv4.conf.default.rp\_filter = 1'. 4. '/sbin/sysctl net.ipv4.tcp\_syncookies' resulting in 'net.ipv4.tcp\_syncookies = 1'. The prompt returns to '[qauser@BRGUPP ~]\$' with a blue cursor.

```
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.icmp_ignore_bogus_error_responses
net.ipv4.icmp_ignore_bogus_error_responses = 1
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.conf.all.rp_filter
net.ipv4.conf.all.rp_filter = 0
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.conf.default.rp_filter
net.ipv4.conf.default.rp_filter = 1
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 1
[qauser@BRGUPP ~]$
```

Figura 3.16: Parámetros para servicios de red y firewalls.



```

qauser@BRGUPP:~$ /sbin/sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.conf.all.send_redirects
net.ipv4.conf.all.send_redirects = 1
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.conf.all.accept_source_route
net.ipv4.conf.all.accept_source_route = 0
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.conf.default.accept_source_route
net.ipv4.conf.default.accept_source_route = 0
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.conf.all.accept_redirects
net.ipv4.conf.all.accept_redirects = 1
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.conf.default.accept_redirects
net.ipv4.conf.default.accept_redirects = 1
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.conf.all.secure_redirects
net.ipv4.conf.all.secure_redirects = 1
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.conf.default.secure_redirects
net.ipv4.conf.default.secure_redirects = 1
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.conf.all.log_martians
net.ipv4.conf.all.log_martians = 0
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.conf.default.log_martians
net.ipv4.conf.default.log_martians = 0
[qauser@BRGUPP ~]$ /sbin/sysctl net.ipv4.icmp_echo_ignore_broadcasts
net.ipv4.icmp_echo_ignore_broadcasts = 1
[qauser@BRGUPP ~]$

```

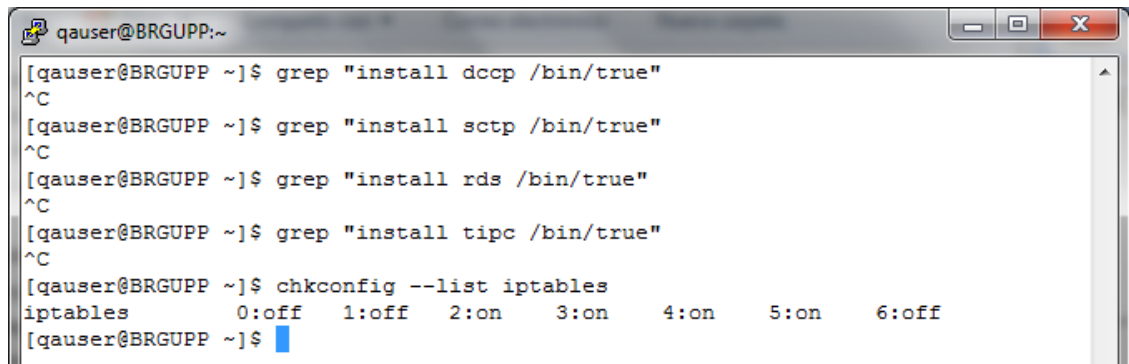
Figura 3.17: Remover configuraciones para redireccionamiento de paquetes.

Para solventar las novedades en este punto, se realizaron las siguientes actividades:

- Deshabilitar IP Forwarding
- Deshabilitar Redirección de envío de paquetes
- Deshabilitar aceptación de paquetes de enrutación de fuentes
- Deshabilitar aceptación de paquetes ICMP redirigidos
- Deshabilitar aceptación de paquetes ICMP seguros
- Logs de Paquetes Sospechosos

- Habilitar "Ignorar peticiones de broadcast"
- Habilitar Protección contra "Bad Error Message"
- Habilitar "RFC-recommende Source Route Validation"
- Habilitar TCP SYN Cookies

### 3.4. Protocolos de redes poco comunes



```
qauser@BRGUPP:~  
[qauser@BRGUPP ~]$ grep "install dccp /bin/true"  
^C  
[qauser@BRGUPP ~]$ grep "install sctp /bin/true"  
^C  
[qauser@BRGUPP ~]$ grep "install rds /bin/true"  
^C  
[qauser@BRGUPP ~]$ grep "install tipc /bin/true"  
^C  
[qauser@BRGUPP ~]$ chkconfig --list iptables  
iptables      0:off  1:off  2:on   3:on   4:on   5:on   6:off  
[qauser@BRGUPP ~]$
```

Figura 3.18: Parámetros para servicios de red poco comunes.

Como solución a las novedades reportadas, se ejecutaron las siguientes tareas:

- Con la configuración de iptables para la denegación de acceso a direcciones IP no permitidas por el administrador del servicio.

- al cierre de puertos y monitoreo de los mismos por medio del uso de iptables.
- al levantamiento de firewall local.

### 3.5. Logs del sistema



```

qauser@BRGUPP:~
[qauser@BRGUPP ~]$ /etc/rsyslog.conf
-bash: /etc/rsyslog.conf: Permission denied
[qauser@BRGUPP ~]$ grep "^*.*[^\I][^\I]*@" /etc/rsyslog.conf
*.* @@192.168.44.94:514
[qauser@BRGUPP ~]$ grep '$ModLoad imtcp.so' /etc/rsyslog.conf
[qauser@BRGUPP ~]$ grep '$InputTCPServerRun' /etc/rsyslog.conf
#$InputTCPServerRun 514
[qauser@BRGUPP ~]$

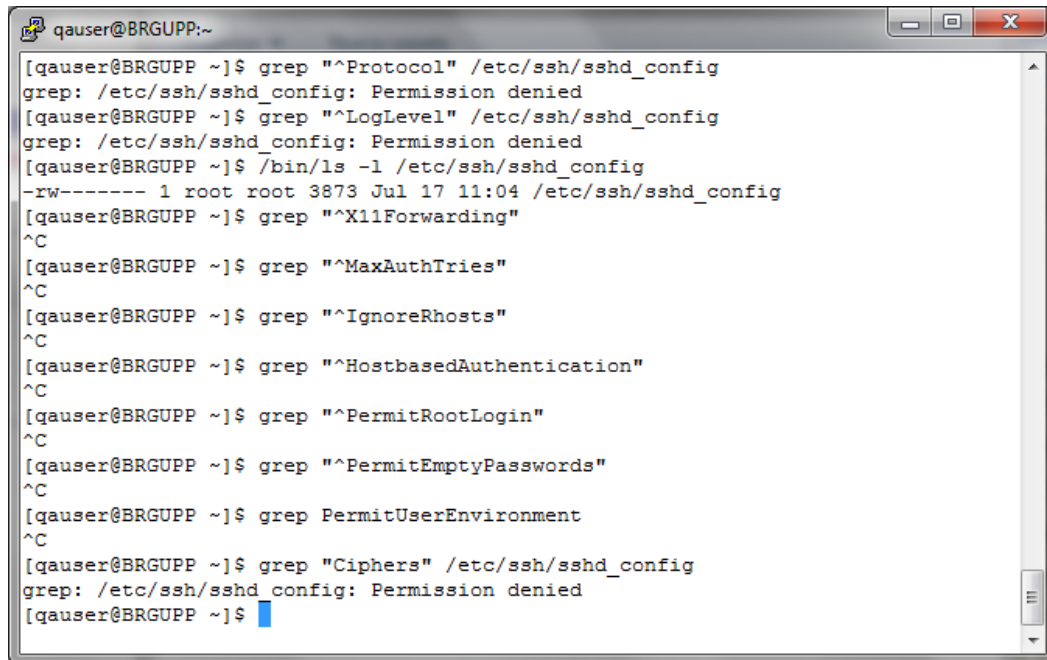
```

Figura 3.19: Aseguramiento de Log's del sistema.

El caso fue cubierto con las siguientes consideraciones:

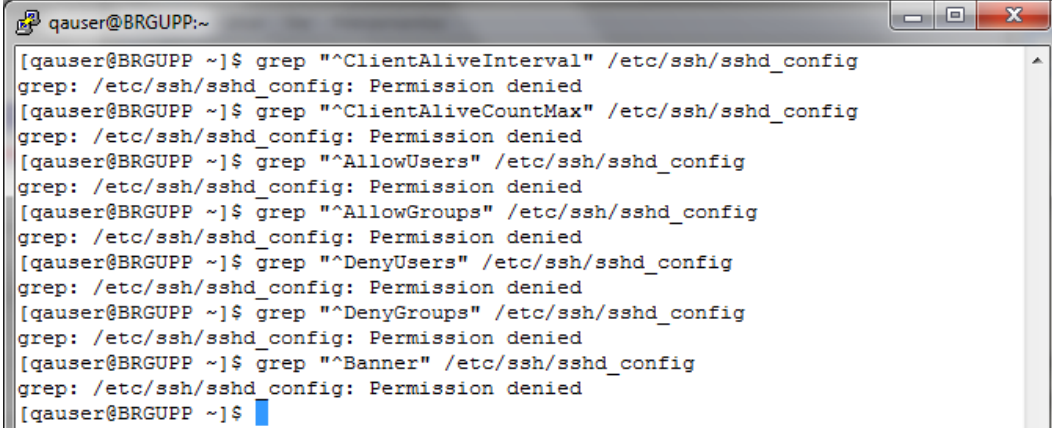
- Instalar el paquete rsyslog
- Activar el servicio rsyslog
- Configurar /etc/rsyslog.conf
- Crear y configurar permisos sobre archivos de rsyslog
- Configurar rsyslog para enviar logs a servidor remoto
- No aceptar mensajes remotos de rsyslog

### 3.6. Configuración SSH

A terminal window titled 'qauser@BRGUPP:~' showing a series of commands and their outputs. The user is checking various SSH configuration parameters using 'grep' and 'ls'. The outputs indicate that several parameters are not present in the configuration file, resulting in 'Permission denied' messages. The user also lists the contents of the configuration file, showing it is a regular file with permissions '-rw-----' owned by 'root' and 'root', with a size of 3873 bytes, last modified on Jul 17 11:04. The user then checks for 'X11Forwarding', 'MaxAuthTries', 'IgnoreRhosts', 'HostbasedAuthentication', 'PermitRootLogin', 'PermitEmptyPasswords', and 'PermitUserEnvironment', all of which are not found. Finally, the user checks for 'Ciphers' and also receives a 'Permission denied' message.

```
qauser@BRGUPP:~$ grep "^Protocol" /etc/ssh/sshd_config
grep: /etc/ssh/sshd_config: Permission denied
qauser@BRGUPP:~$ grep "^LogLevel" /etc/ssh/sshd_config
grep: /etc/ssh/sshd_config: Permission denied
qauser@BRGUPP:~$ /bin/ls -l /etc/ssh/sshd_config
-rw----- 1 root root 3873 Jul 17 11:04 /etc/ssh/sshd_config
qauser@BRGUPP:~$ grep "^X11Forwarding"
^C
qauser@BRGUPP:~$ grep "^MaxAuthTries"
^C
qauser@BRGUPP:~$ grep "^IgnoreRhosts"
^C
qauser@BRGUPP:~$ grep "^HostbasedAuthentication"
^C
qauser@BRGUPP:~$ grep "^PermitRootLogin"
^C
qauser@BRGUPP:~$ grep "^PermitEmptyPasswords"
^C
qauser@BRGUPP:~$ grep PermitUserEnvironment
^C
qauser@BRGUPP:~$ grep "Ciphers" /etc/ssh/sshd_config
grep: /etc/ssh/sshd_config: Permission denied
qauser@BRGUPP:~$
```

Figura 3.20: Ajuste en parámetros SSH.



```
qauser@BRGUPP:~  
[qauser@BRGUPP ~]$ grep "^ClientAliveInterval" /etc/ssh/sshd_config  
grep: /etc/ssh/sshd_config: Permission denied  
[qauser@BRGUPP ~]$ grep "^ClientAliveCountMax" /etc/ssh/sshd_config  
grep: /etc/ssh/sshd_config: Permission denied  
[qauser@BRGUPP ~]$ grep "^AllowUsers" /etc/ssh/sshd_config  
grep: /etc/ssh/sshd_config: Permission denied  
[qauser@BRGUPP ~]$ grep "^AllowGroups" /etc/ssh/sshd_config  
grep: /etc/ssh/sshd_config: Permission denied  
[qauser@BRGUPP ~]$ grep "^DenyUsers" /etc/ssh/sshd_config  
grep: /etc/ssh/sshd_config: Permission denied  
[qauser@BRGUPP ~]$ grep "^DenyGroups" /etc/ssh/sshd_config  
grep: /etc/ssh/sshd_config: Permission denied  
[qauser@BRGUPP ~]$ grep "^Banner" /etc/ssh/sshd_config  
grep: /etc/ssh/sshd_config: Permission denied  
[qauser@BRGUPP ~]$
```

Figura 3.21: Remover permisos de acceso a archivos de configuración en directorio/etc/ssh.

Para este punto, se consideró lo siguiente:

- Se procede con la configuración del algoritmo de cifrado de datos para contraseñas sha512
- Se procede a configurar el borrado automático del archivo `cat/etc/pam.d/password-auth` `##%PAM-1.0` para cada oportunidad en que el `authconfig` se encuentre en ejecución.



### 3.7. Configuración PAM

```

qauser@BRGUPP:~
[qauser@BRGUPP ~]$ grep "remember" /etc/pam.d/system-auth
password sufficient pam_unix.so remember=4
[qauser@BRGUPP ~]$ cat /etc/securetty
cat: /etc/securetty: Permission denied
[qauser@BRGUPP ~]$ grep pam_wheel.so /etc/pam.d/su
#auth      sufficient      pam_wheel.so trust use_uid
#auth      required        pam_wheel.so use_uid
[qauser@BRGUPP ~]$ grep wheel /etc/group
wheel:x:10:
[qauser@BRGUPP ~]$

```

Figura 3.22: Ajuste en configuración PAM.

```

qauser@BRGUPP:~
[qauser@BRGUPP ~]$ authconfig --test | grep hashing | grep sha512
password hashing algorithm is sha512
[qauser@BRGUPP ~]$ grep pam_cracklib.so /etc/pam.d/system-auth
password requisite pam_cracklib.so try_first_pass retry=3 type=
password required pam_cracklib.so try_first_pass retry=3 minlen=14 dcredit
it=-1 ucredit=-1 ocredit=-1 lcredit=-1
[qauser@BRGUPP ~]$ grep "pam_faillock" /etc/pam.d/password-auth
auth      required        pam_faillock.so preauth audit silent deny=5 unlock_time=900
auth      [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900
auth      sufficient     pam_faillock.so authsucc audit deny=5 unlock_time=900
[qauser@BRGUPP ~]$ grep "pam_unix.so" /etc/pam.d/password-auth | grep success=1
auth      [success=1 default=bad] pam_unix.so
[qauser@BRGUPP ~]$ grep "pam_faillock" /etc/pam.d/system-auth
auth      required        pam_faillock.so preauth audit silent deny=5 unlock_time=900
auth      [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900
auth      sufficient     pam_faillock.so authsucc audit deny=5 unlock_time=900
[qauser@BRGUPP ~]$ grep "pam_unix.so" /etc/pam.d/system-auth | grep success=1
auth      [success=1 default=bad] pam_unix.so
[qauser@BRGUPP ~]$

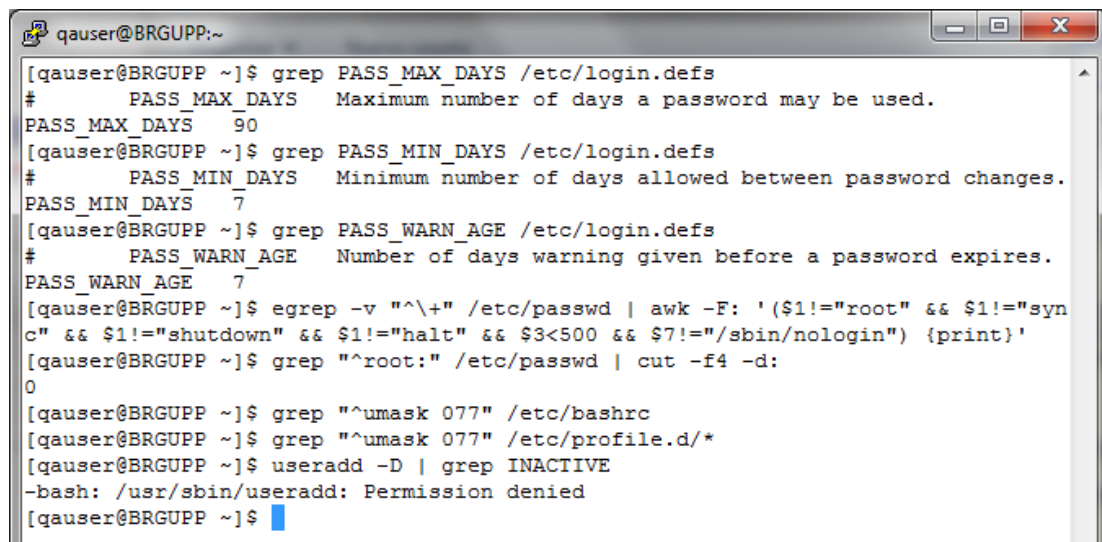
```

Figura 3.23: Confirmación de ejecución de aseguramiento para PAM.

Para este caso, se efectuaron las siguientes tareas:

- Se procede con la restricción el acceso a los archivos de sistema y de configuración de permisos de usuario.
- Se procede a configurar en `/etc/pam.d/su` el parámetro `authrequiredpam_wheel_souse_uid`.
- Se incluye la lista de los usuarios que pueden ejecutar el comando `su` en el archivo `Wheel` en el directorio `/etc/groups`.

### 3.8. Cuentas de Usuario y ambientes.



```

[qauser@BRGUPP ~]$ grep PASS_MAX_DAYS /etc/login.defs
#      PASS_MAX_DAYS  Maximum number of days a password may be used.
PASS_MAX_DAYS  90
[qauser@BRGUPP ~]$ grep PASS_MIN_DAYS /etc/login.defs
#      PASS_MIN_DAYS  Minimum number of days allowed between password changes.
PASS_MIN_DAYS  7
[qauser@BRGUPP ~]$ grep PASS_WARN_AGE /etc/login.defs
#      PASS_WARN_AGE  Number of days warning given before a password expires.
PASS_WARN_AGE  7
[qauser@BRGUPP ~]$ egrep -v "^\+" /etc/passwd | awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $3<500 && $7!="/sbin/nologin") {print}'
[qauser@BRGUPP ~]$ grep "^root:" /etc/passwd | cut -f4 -d:
0
[qauser@BRGUPP ~]$ grep "^umask 077" /etc/bashrc
[qauser@BRGUPP ~]$ grep "^umask 077" /etc/profile.d/*
[qauser@BRGUPP ~]$ useradd -D | grep INACTIVE
-bash: /usr/sbin/useradd: Permission denied
[qauser@BRGUPP ~]$

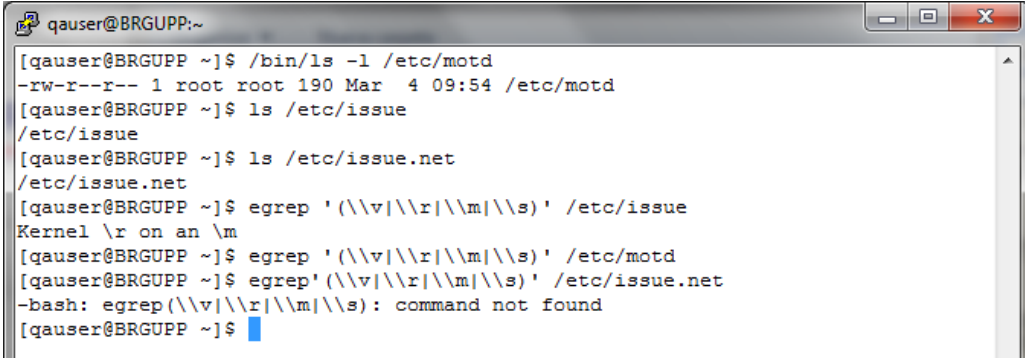
```

Figura 3.24: Ajuste en parámetros de usuarios.

Para el control de usuarios, las consideraciones fueron las siguientes:

- Se procede con el ajuste dentro del sistema para que la caducidad de las contraseñas sea de 90 días.
- Se procede con la inhabilitación del usuario root para hacer login en el sistema operativo directamente.
- Se procede con la reducción de privilegios para los usuarios no administradores aprobados por la empresa.
- Se procede con la configuración del mínimo de días para cambiar la contraseña, incluyendo el mensaje de advertencia de expiración del password.
- Se procede a deshabilitar las cuentas del sistema por medio del uso del siguiente comando:
  - o `egrep -v "^+" /etc/passwd | awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $3<500 && $7!="/sbin/nologin") {print}'`
- Se procede a configurar la máscara por defecto para los usuarios en las rutas:
  - o `/etc/bashrc`
  - o `/etc/peodilw.s/cis.sh`

### 3.9. Banners de advertencia.



```

[qauser@BRGUPP ~]$ /bin/ls -l /etc/motd
-rw-r--r-- 1 root root 190 Mar  4 09:54 /etc/motd
[qauser@BRGUPP ~]$ ls /etc/issue
/etc/issue
[qauser@BRGUPP ~]$ ls /etc/issue.net
/etc/issue.net
[qauser@BRGUPP ~]$ egrep '(\\v|\\r|\\m|\\s)' /etc/issue
Kernel \\r on an \\m
[qauser@BRGUPP ~]$ egrep '(\\v|\\r|\\m|\\s)' /etc/motd
[qauser@BRGUPP ~]$ egrep '(\\v|\\r|\\m|\\s)' /etc/issue.net
-bash: egrep(\\v|\\r|\\m|\\s): command not found
[qauser@BRGUPP ~]$

```

Figura 3.25: Ajuste en configuración de Banners de advertencia.

Finalmente, para solventar estas novedades, se realizó lo siguiente:

- Configurar Banner de Advertencia para servicios standard de login.
- Remover Información de Sistema Operativo para logeo de Banners de Advertencia.

## CONCLUSIONES Y RECOMENDACIONES

### Conclusiones:

1. Con el desarrollo del proyecto se pudo completar exitosamente lo solicitado, lo cual consistía en el aseguramiento de la plataforma operativa del nuevo switch transaccional para producción, el cual fue ejecutado en conjunto entre el personal responsable por parte del proveedor del aplicativo, de Red Hat Inc., la entidad certificadora y los ingenieros de la empresa.
2. Dentro de la ejecución de las pruebas pudimos observar que existen mejoras que podrían realizarse a nivel de cada una de las instancias participantes por lo que

fue el inicio de un proyecto de mejoras en los que se participará de igual manera, generando así una gran ayuda para futuros proyectos con otros clientes.

### **Recomendaciones:**

1. Se pudo evidenciar dentro del proceso del aseguramiento que existen opciones las cuales son consideradas por la entidad certificadora y ya fueron solventadas en las últimas actualizaciones del sistema operativo, por lo que se levantó la alerta para el ajuste de la documentación hacia nuestros auditores.
2. Una vez implementada la solución, se recomienda igualmente que como alcance al proyecto, se haga una evaluación sobre los permisos requeridos por el sistema para incrementar el nivel de seguridad, ya que la implementación realizada actualmente cubre con las necesidades básicas de PCI 3.0, sin embargo para inicios del año 2016 se espera que las auditorias de cumplimiento se realicen sobre su última actualización en la versión 3.1

3. Con la implementación se contempla un crecimiento transaccional del 50%, lo cual está proyectado para cubrir los próximos 3 años, sin embargo el tiempo puede verse reducido por lo que luego de su salida a producción se recomienda se haga un análisis de las transacciones por segundo que el mismo podrá soportar y así tener una proyección más real
  
4. Dentro del proceso de aseguramiento, el personal administrador de la infraestructura tecnológica nos indicó que cuentan con un servidor con sistema operativo Oracle LINUX 6 sobre el que se desea realizar el mismo trabajo; se procedió con la evaluación de la plantilla de aseguramiento y según pudimos evidenciar se mantienen las mismas consideraciones que en la plantilla utilizada para Red Hat 6, por lo que se recomienda aplicar las mismas configuraciones indicadas en el documento. [5]

## **GLOSARIO**

### **Aseguramiento (hardening)**

Consiste en el endurecimiento de la plataforma operativa, de manera que se puedan solventar las vulnerabilidades que han sido estudiadas y publicadas previamente por los organismos de seguridad competentes tanto a nivel nacional como internacional.

### **PCI DSS**

P.C.I. D.S.S. son las siglas por las cuales reconocemos al PaymentCardIndustry Data security Standard, o en su traducción a nuestra lengua como el estándar de seguridad en los datos de la industria de pagos por tarjetas. Este estándar nos permite mantener un nivel de seguridad adecuado para el correcto uso de tarjetas de crédito y débito, reduciendo en gran porcentaje el número de fraudes y el impacto de estos tanto para los clientes como para las instituciones financieras.

### **QSA:**

Siglas utilizadas para describir al Quality Security Advisor, o su traducción Consultor de Calidad de Seguridad. Es el oficial encargado de realizar la auditoría PCI DSS por parte



de la entidad certificadora. Se asigna regularmente un QSA por cada ejercicio, es decir por cada proceso de auditoría que se realice, ya sea de certificación inicial o de renovación.

**Vulnerabilidad:**

Es un punto débil que se descubre tanto a nivel de software como de hardware, el cual compromete la disponibilidad, confidencialidad o integridad de la información. Estas vulnerabilidades son catalogadas dependiendo el impacto que puede producir su explotación, siendo el caso de las más severas pueden permitir al atacante tener control absoluto del equipo y por ende de la información a la que este puede tener acceso.

**Booteo:**

Denominado se esta manera al proceso de arranque del sistema desde su estado de apagado.

**PAM:**

PluggableAuthentication Modules, es un mecanismo de acceso o autenticación que trabaja de manera flexible, este permite aislar a las aplicaciones y otro software existente del proceso de identificación. La identificación del usuario, implementa niveles de

seguridad mayores, tal sea el caso del uso de Biométricos, autenticaciones con claves temporales, entre otras, reemplazando a los mecanismos tradicionales o simplemente fortaleciendo dichos métodos de autenticación.

## BIBLIOGRAFÍA

[1] Red Hat Inc., Red Hat Enterprise Linux 6 Guía de Seguridad, [https://access.redhat.com/documentation/es-ES/Red\\_Hat\\_Enterprise\\_Linux/6/pdf/Security\\_Guide/Red\\_Hat\\_Enterprise\\_Linux-6-Security\\_Guide-es-ES.pdf](https://access.redhat.com/documentation/es-ES/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-es-ES.pdf)

[2] PCI Security Standards Council, Requirements and Security Assessment Procedures Version 3.0, [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf), fecha de consulta julio 2015.

[3] Gonzalez, Padrón, PluggableAuthentication Modules, [http://sopa.dis.ulpgc.es/ii-aso/portal\\_aso/lelinux/seguridad/pam/pam\\_doc.pdf](http://sopa.dis.ulpgc.es/ii-aso/portal_aso/lelinux/seguridad/pam/pam_doc.pdf), fecha de consulta julio 2015.

[4] Capek, T., Petrová, A., Navrátil, M., Ballard, E., Red Hat Enterprise Linux 6 Identity Management Guide, [https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/6/pdf/Identity\\_Management\\_Guide/Red\\_Hat\\_Enterprise\\_Linux-6-Identity\\_Management\\_Guide-en-US.pdf](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Identity_Management_Guide/Red_Hat_Enterprise_Linux-6-Identity_Management_Guide-en-US.pdf), fecha de consulta julio 2015.

[5] ORACLE, Oracle Linux

Security GuideforRelease 6, [http://docs.oracle.com/cd/E37670\\_01/E36387/E36387.pdf](http://docs.oracle.com/cd/E37670_01/E36387/E36387.pdf), fecha de consulta julio 2015.