



**Bienestar**  
al aprendiz

## **CENTRO DE TECNOLOGÍAS AGROINDUSTRIALES SENA REGIONAL VALLE**

**Red de Conocimiento en Informática, Diseño y Desarrollo de  
Software**

**SERVICIO NACIONAL DE APRENDIZAJE SENA  
Marzo de 2017**

## TABLA DE CONTENIDO

1. INTRODUCCIÓN .....	3
2. JUSTIFICACIÓN.....	3
3. OBJETIVOS.....	3
4. DIRIGIDO A .....	3
5. REQUISITOS .....	4
6. FICHA TÉCNICA .....	6
REDES DE DATOS Y SISTEMAS OPERATIVOS DE RED.....	6
7.1 JORNADA DÍA 1.....	6
7.2 JORNADA DÍA 2 .....	9
7.3 JORNADA DÍA 3 .....	13
7. COMPETENCIAS RELACIONADAS.....	15
8. CRITERIOS DE EVALUACIÓN.....	15
9.1 JORNADA DÍA 1.....	16
9.2 JORNADA DÍA 2 .....	17
9.3 JORNADA DÍA 3.....	22
9. MATERIALES, EQUIPOS Y HERRAMIENTAS.....	24
CONTROL DE DOCUMENTO .....	27

## 1. INTRODUCCIÓN

La ficha técnica establecida en este documento, permite a instructores, aprendices competidores, jurados y diseñadores de las pruebas, conocer los parámetros que rigen la competencia SENASoft Valle 2017 en la categoría Redes de datos y Sistemas operativos de red. Estos lineamientos guían a todos los interesados para la preparación y el desarrollo de la competencia.

## 2. JUSTIFICACIÓN

Con la rápida globalización de los sistemas de TI, los Administradores de Redes de Datos afrontan rápidamente oportunidades de expandir sus conocimientos así como también nuevos retos. Para el talentoso Administrador de Redes de Datos, hay muchas oportunidades internacionales en el sector público y comercial; sin embargo, esto requiere que el Administrador de Redes necesite entender y trabajar con diversas plataformas para poder mantenerse al tanto con los rápidos avances tecnológicos de la industria. Por lo tanto la cantidad de las habilidades asociadas con el Administrador de Redes de Datos es muy susceptible al cambio.

## 3. OBJETIVO

Definir los requisitos de carácter técnico que regirán la ejecución de las pruebas de la categoría Redes de Datos y Sistemas Operativos de Red según los criterios y contenidos propios del programa de formación Tecnología en Gestión de redes de datos, los cuales deben ser interpretados e identificados por todos los actores involucrados en la competencia.

## 4. DIRIGIDO A

Instructores líderes SENASoft en cada centro de formación, aprendices participantes y evaluadores.

## 5. REQUISITOS

- a. La participación es en parejas.
- b. Un centro sólo podrá inscribir una pareja.
- c. No podrán participar:
  - Egresados del SENA.
  - Aprendices de programas de formación titulada o complementaria de formación virtual.
  - Aprendices que hayan participado en eventos anteriores de SENASoft.
  - Aprendices que hayan participado o que actualmente hagan parte del evento Worldskills.
  - Aprendices que sean o hayan sido Instructores SENA.
  - Aprendices de formación titulada de nivel especialización tecnológica.
  - Aprendices que tengan título universitario a nivel de tecnología o superior en cualquier área de formación.
- d. Los aprendices participantes deberán portar el carné que lo identifica como aprendiz SENA, la escarapela que lo acredita como participante, el carné de beneficiario del servicio de salud y su respectivo uniforme o la camiseta del evento.
- e. Los equipos o elementos necesarios que se requieran para la prueba (incluyendo librerías externas) deberán ser asignados al inicio de la competencia por el líder técnico de la categoría. No se permitirán ingresos posteriores.
- f. Antes de iniciar la prueba, el jurado verificará que la pareja participante no ingrese:
  - Material que constituya ventaja para la realización de la prueba sobre los demás competidores
  - Material dañino para el hardware, software o personas.
- g. El jurado revisará el contenido del computador, y podrá solicitar la desinstalación o borrado de material en cumplimiento de lo dispuesto en el inciso f.
- h. Si se encuentra algún material considerado en el punto f se procederá a formatear el o los equipos donde se encuentre, la pareja de participantes será sancionada restándole el 30% del puntaje que logre en la prueba del día. El líder nacional SENASoft presentará al subdirector del centro organizador el informe respectivo aportando las evidencias del caso, a su vez el subdirector del centro organizador deberá notificar al subdirector del centro origen de aprendices sancionados.
- i. A la competencia no se permite el ingreso de personas en estado de embriaguez o bajo el efecto de sustancias que impidan un normal desempeño.
- j. Terminada la prueba, no se admitirán correcciones ni modificaciones. Los resultados serán evaluados en el computador objeto del desarrollo de la prueba. En caso de requerirlo, el jurado de la prueba podrá exigir la presencia de la pareja participante, al momento de hacer la evaluación.
- k. Al terminar cada prueba, el computador quedará en custodia del jurado, para su posterior evaluación.
- l. El ingreso de los participantes se habilitará 15 minutos previos al inicio de la prueba. Una vez

iniciada la prueba según los horarios establecidos en el cronograma del evento se permitirá el acceso a los participantes so pena de recibir una sanción equivalente a la pérdida del 30% del puntaje de la prueba del día respectivo.

- m. Los equipos de cómputo, y/o materiales magnéticos y digitales, serán custodiados por la Regional Valle y solo podrán ser retirados una vez culminada la prueba en el espacio dispuesto para tal fin según el cronograma del evento.
- n. Cada equipo participante deberá traer los equipos, materiales y herramientas del centro de formación origen, descritos en el ítem materiales. Estos elementos deben ser revisados por el comité dispuesto para tal fin.
- o. Todos los equipos, herramientas y materiales que se usen en la competencia deben pertenecer al inventario SENA y deben estar debidamente marcados con el nombre del centro y la categoría.
- p. Todos los equipos que se utilicen en la competencia deben estar con privilegios de administrador y sin contraseñas. Para el caso de los equipos linux, el superusuario **root** debe tener contraseña **redhat**.
- q. Los editores de código definidos no deben tener instalados ningún tipo de plugin o snippets (el equipo técnico de la categoría realizará la respectiva revisión).
- r. Si se comprueba que hay fraude en unas de las diferentes competencias se sanciona el equipo de participantes con la pérdida de todos los puntos de ese día de la competencia.

## 6. FICHA TÉCNICA

### REDES DE DATOS Y SISTEMAS OPERATIVOS DE RED

#### TEMAS A CONSIDERAR:

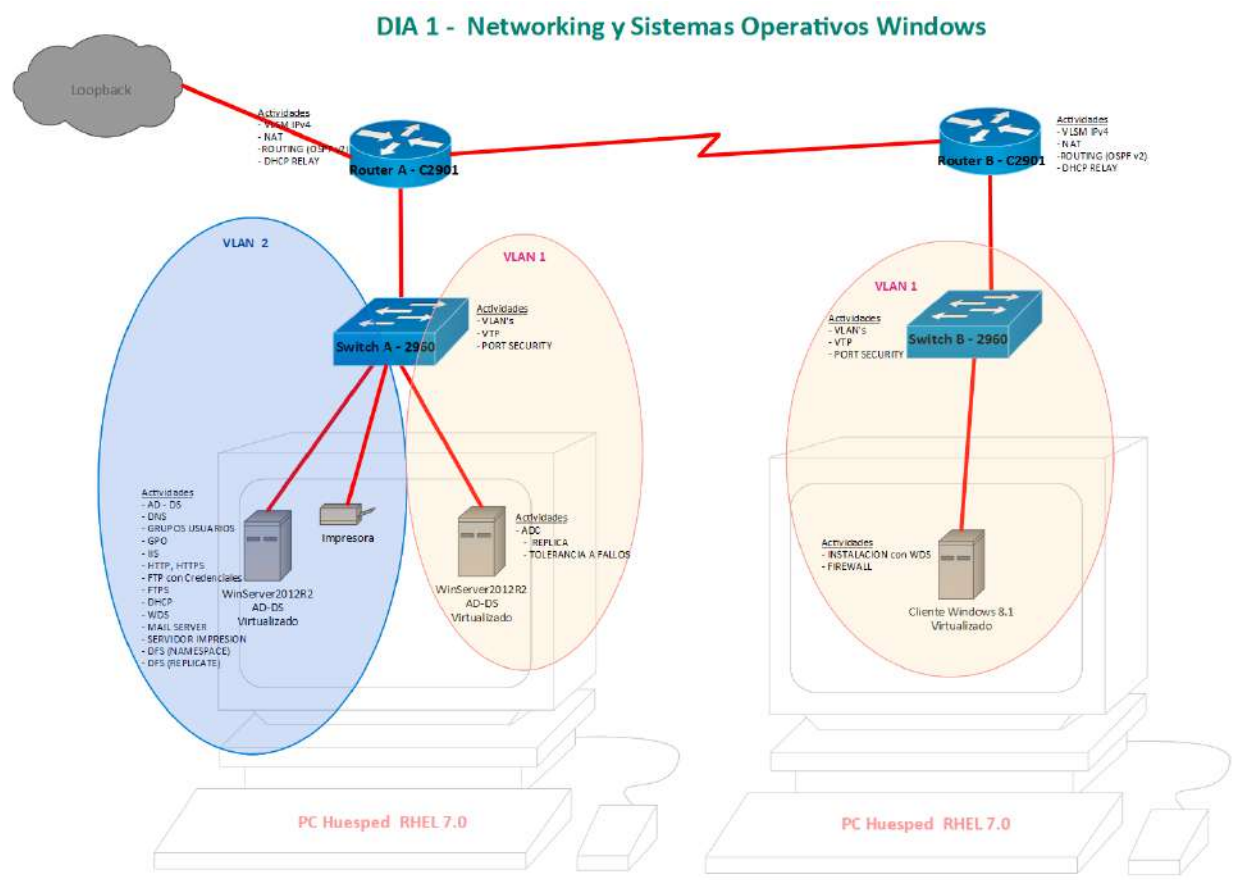
La competencia se llevará a cabo en tres jornadas de 5 horas cada una, en las cuales los equipos desarrollarán una prueba dispuesta para cada jornada.

Al finalizar cada jornada de trabajo o sesión de prueba los equipos de cómputo quedarán dispuestos para el resguardo por parte del comité dispuesto para tal fin. Los aprendices no podrán ingresar trabajos prefabricados, elementos prediseñados y/o scripts, librerías, códigos, software y/o hardware adicional al permitido en este documento. La inclusión de algún elemento adicional no permitido será causal de sanción según reglamento.

#### 7.1 JORNADA DÍA 1

(35% del total posible en el conjunto de las 3 pruebas)

#### Proceso: NETWORKING Y SISTEMAS OPERATIVOS WINDOWS



Durante esta primera Jornada, se trabajará con sistema operativo **WINDOWS SERVER 2012R2** en los servidores **SERVER A** y **SERVER B** y sistema operativo **Windows 8.1** en el equipo **CLIENTE A**. En esta topología se realizara la implementación y prueba de servicios de red para la solución tecnológica de infraestructura de la prueba.

## TEMAS A CONSIDERAR

Creación del Ambiente virtualizado sobre maquinas PC huésped que tengan instalado el sistema operativo **RHEL7.0 (RedHat Enterprise Linux 7.0)**, utilizando el gestor de virtualización nativo **VMM (Virtual Machine Manager)** que permite la conectividad con los dispositivos de interconexión según el requerimiento.

A los equipos de aprendices, se les entregara información de los requerimientos de una red, con base a ello, los aprendices deben diseñar e implementar una solución, se tendrán en cuenta los siguientes criterios:

## NETWORKING

- Diseño de
- la red:
  - Diseño de direccionamiento con ipv4
  - VLSM
  - VLANs
- Router:
  - OSPF V2
  - NAT
  - DHCP Relay
- SWITCH:
  - VTP
  - Port Security
  - DHCP Snooping

## SISTEMAS OPERATIVOS WINDOWS

SERVIDOR A - WINDOWS SERVER 2012 R2

- Instalación Sistema Operativo
- Configuración Controladores
- Configuración Firewall Windows
- Configuración IPV4

#### SERVICIOS DE RED:

- AD – DS
- DNS
- GRUPOS Y USUARIOS
- GPO
- IIS
  - WEB SERVER (HTTP)
  - WEB SERVER (HTTPS)
  - FTP SERVER (USUARIOS)
  - FTP SERVER(FTPS)
- DHCP
- WDS
- MAIL SERVER (EXCHANGE 2012)
- SERVIDOR DE IMPRESIÓN
- DFS (NAMESPACE)
- DFS (REPLICATION)

#### SERVIDOR B - WINDOWS SERVER 2012 R2

- Instalación Sistema Operativo
- Configuración Controladores
- Configuración Firewall Windows
- Configuración IPV4

#### SERVICIOS DE RED:

- ADC
  - REPLICA
  - TOLERANCIA A FALLAS

#### CLIENTE A - WINDOWS 8.1

- INSTALACIÓN SISTEMA OPERATIVO CON WDS
- CONFIGURACIÓN CONTROLADORES
- CONFIGURACIÓN FIREWALL WINDOWS



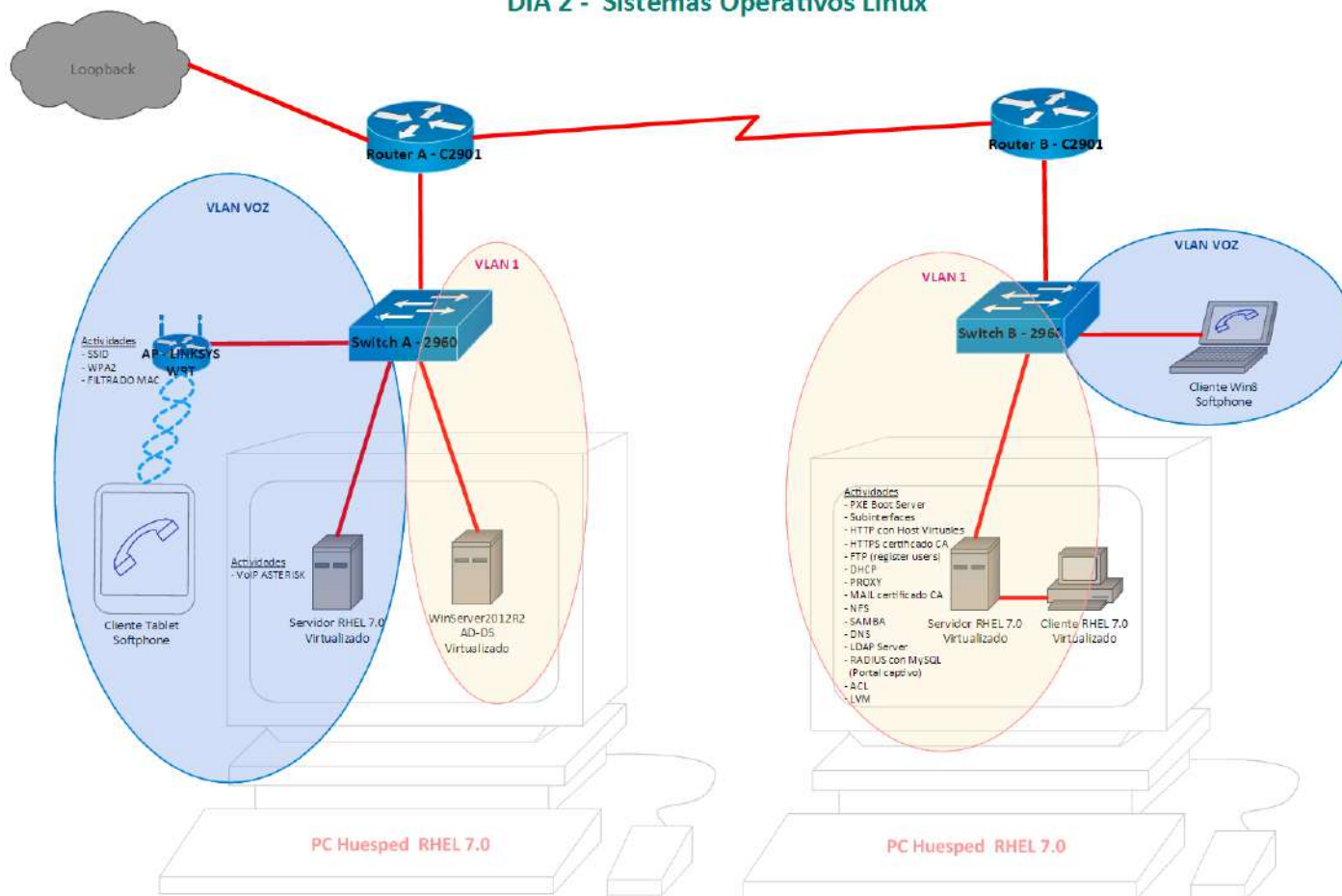
○ CONFIGURACIÓN IPv4

**JORNADA DÍA 2**

(35% del total posible en el conjunto de las 3 pruebas)

**Proceso: SISTEMAS OPERATIVOS LINUX**

**DIA 2 - Sistemas Operativos Linux**



Durante esta segunda Jornada, se trabajará con sistemas operativos **RHEL7.0 (RedHat Enterprise Linux 7.0)**, prueba e implementación de servicios de red para solución tecnológica de infraestructura, de la mediana y pequeña empresa.

**TEMAS A CONSIDERAR**

Creación de ambiente virtualizado sobre máquinas PC huésped que tengan instalado el sistema operativo

RHEL7.0 (*RedHat Enterprise Linux 7.0*), utilizando el gestor de virtualización nativo **VMM** (*Virtual Machine Manager*) que permita la conectividad con los dispositivos de interconexión según el requerimiento.

## SERVICIOS LINUX

**NOTA:** Todas las configuraciones en **RHEL7.0** se realizan con el módulo de seguridad **Security Linux** (**SELinux**) en modo **enforcing**, No se permite deshabilitar éste módulo o establecer en modo **permissive**.

- Realizar configuración básica de dispositivos de interconexión para garantizar conectividad entre las LAN.
- Configuración de **AP Linksys WRT300N**
  - SSID
  - WPA2
  - FILTRADO MAC

### SERVIDOR A – REDHAT ENTERPRISE LINUX 7.0

- Instalación RHEL 7 con particiones LVM según requerimientos
- Configuración de Repositorios de Paquetes Linux: Locales y Remotos
- Resolver FQN (*Fully Qualified Name*)
- Configuración de direccionamiento IP según requerimientos.
- Servidor de instalación PXE (*PXE Network Boot Server*)
  - Instalador remoto y desatendido de equipos RHEL7.0
- Servidor WEB (*WEB Server*)
  - Subinterfaces de Red
  - HTTP
    - Configurar Host Virtuales y asociarlos a direcciones IP de las Subinterfaces de Red para Cada Sitio Web.
  - HTTPS
    - Instalar módulos SSL
    - Generar Certificado CA (*Certificate Authority*)
    - Utilizar Certificado CA para acceso seguro a sitio web
    - Configurar Host Virtual del Sitio Web Seguro y asociarlo a dirección IP de una subinterfaz de Red.
- Servidor FTP (*FTP Server*)
  - Creación de usuarios FTP
  - Usuarios Registrados

- Usuario Enjaulado (Administrador FTP)
- Servidor DHCP (*DHCP Server*)
  - Configuración según requerimientos
  - Distinción de Interfaz de Red (DHCP multihomed)
- Servidor NFS (*NFS Server*)
  - Montaje Automático usando usando **fstab**
- Servidor DNS (*DNS Server*)
  - DNS Primario (Zonas directas – Zonas Inversas)
- Servidor MAIL Seguro (*MAIL Server*)
  - Instalación y configuración paquete POSTFIX
  - Instalación y configuración paquete DOVECOT
  - Utilizar Certificado CA para acceso seguro a WebMail
  - Uso de SQUIRRELMAIL como Gestor Webmail
  - Configuración de cliente de correo Windows *Outlook*
  - Configuración de cliente de correo Linux *Thunderbird* ó *Evolution*
- Servidor de Directorio (*LDAP Server*)
  - Creación/Uso de Certificado CA (*Certificate Authority*)
  - Creación de Grupos, Usuarios y Contraseñas
  - Migración de Grupos, Usuarios y Contraseñas
  - Directorios Compartidos NFS (para clientes LINUX-UNIX)
  - Usuarios y contraseñas SAMBA
  - Directorios Compartidos SAMBA (para clientes WINDOWS)
  - Directorios colaborativos controlados mediante ACL (*Access Control List*)
  - Instalación y configuración paquetes servidor LDAP
  - Importación de Unidades Organizacionales a servidor LDAP (Base, Grupos y Usuarios)
- Servidor PROXY (*PROXY Server*)
  - Instalación y configuración paquete SQUID
    - Filtrado de Palabras
    - Filtrado de Sitios
    - Filtrado de Horarios
- Servidor RADIUS (*RADIUS Server*)
  - Instalar y Configurar freeRADIUS con base de datos MySQL
  - Configurar Portal Captivo con autenticación a MySQL (daloradius, pfSense, Easy Hostpot u Otro)
- Administración de Volúmenes Lógicos (*LVM - Logical Volume Manager*)
  - Extender área de intercambio **swap**
  - Gestión de particiones con **fdisk**
  - Crear **Physical Volumes**

- Crear y/o Extender **Volume Groups**
- Crear y/o Extender **Logical Volumes**
- Formateo de particiones, volúmenes lógicos y áreas de intercambio *swap*.
- FIREWALLD
  - Apertura de Puertos y Servicios de Red desde CLI (no usar **iptables**)
- Booleanos SELinux
  - Habilitar booleanos SELinux a cada servicio de red desde CLI.

#### SERVIDOR B – REDHAT ENTERPRISE LINUX 7.0

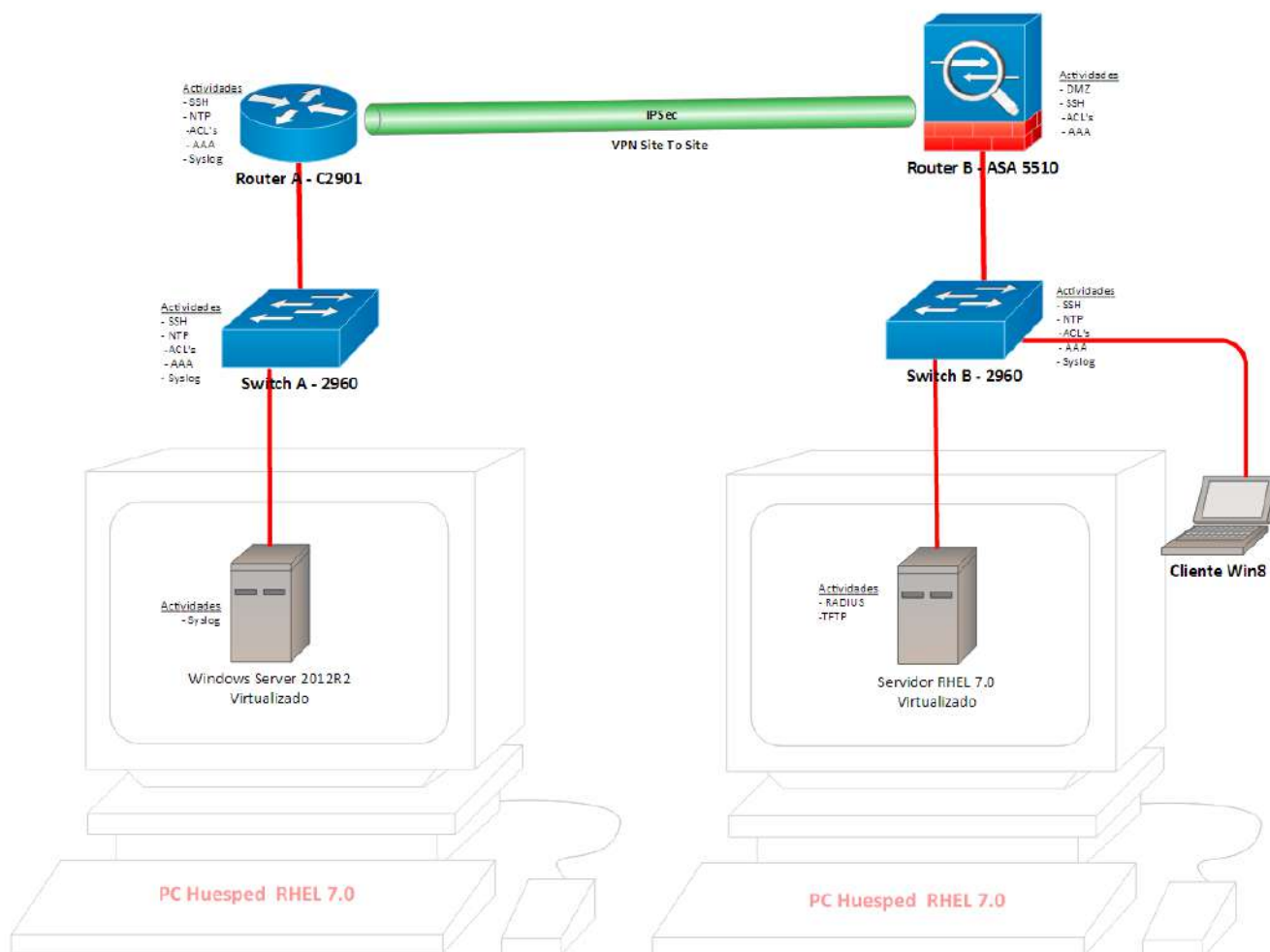
- Usar PXE para realizar instalación desatendida.
- Configuración de Repositorios de Paquetes Linux: Locales y Remotos
- Resolver FQN (*Fully Qualified Name*)
- Configuración de direccionamiento IP según requerimientos.
- Servidor VoIP
  - Instalación de paquetes ASTERISK sobre servidor virtual RHEL7.0
  - Configuración Servidor ASTERISK
  - Configuración de extensiones y usuarios
  - Instalación y configuración SOFTPHONE en cliente Windows (PC portátil)
  - Instalación y configuración SOFTPHONE cliente móvil (Tablet Android ó iPad)
- Cliente LDAP
  - Autenticación usando TLS Certificado CA y LDAP password.
  - Automontaje de directorios de usuarios LDAP
  - Acceso de cliente Linux a Servidor LDAP (modo CLI y modo GUI) en su directorio propio alojado en servidor.
  - Acceso de cliente Windows a Servidor LDAP en su directorio propio alojado en servidor
- Autenticación en Directorio Activo Windows Server 2010R2.
  - Instalación y configuración de paquetes para acceder como cliente linux a AD-DS de Windows.
- FIREWALLD
  - Apertura de Puertos y Servicios de Red desde CLI (no usar **iptables**)
- Booleanos SELinux
  - Habilitar booleanos SELinux a cada servicio de red desde CLI.

### 7.3 JORNADA DÍA 3

(30% del total posible en el conjunto de las 3 pruebas)

Proceso: SEGURIDAD EN REDES EMPRESARIALES Y TROUBLESHOOTING (*Solución de problemas*)

#### DIA 3 - Seguridad en redes empresariales y Troubleshooting



Esta tercera jornada se compone de dos partes, PARTE I donde se trabajará en la Implementación de soluciones tecnológicas alámbricas de tipo empresarial, se tendrán en cuenta los siguientes criterios:

#### PARTE I: IMPLEMENTACION DE SOLUCIONES TECNOLOGICAS SEGURAS

- ✓ Diseño de la red:
  - Integración direccionamiento IPv4
  - VLSM
  - Garantizar conectividad de extremo a extremo.
- ✓ Servidores
  - RADIUS sobre Linux Server
  - SYSLOG sobre Windows Server
- ✓ Configuración de dispositivos de red
  - ROUTER
    - SSH
    - NTP
    - ACL'S
    - AAA
    - SYSLOG
    - Endurecimiento de Capa 3
      - Bloqueo por Intentos Fallidos,
      - Establecimiento de Longitud de Contraseñas,
      - Periodo de Inactividad, Modo Silencioso,
      - Nivel de Privilegios,
      - Resiliencia IOS,
      - Respaldo IOS
      - Archivos de Configuración.
  - ASA (Adaptative Security Appliance)
    - VPN site to site, IPSEC
    - VPN AnyConnect
    - Zonas de seguridad
    - SWITCH
    - SSH
    - NTP
    - ACL'S
    - AAA
    - SYSLOG

## PARTE II: Troubleshooting (Solución de problemas)

Se trabajará en la solución y corrección de errores en la red, se asignará a cada grupo participante una red compleja, donde se pondrán a prueba sus habilidades en la corrección de errores, la red se

entregara en packet tracert, al finalizar la prueba el ejercicio se debe entregar con conectividad total, con los servicios y protocolos ejecutándose correctamente según las indicaciones dadas por la persona encargada del evento.

Las temáticas a evaluar en esta jornada, son:

- Ipv6
- STP
- PORTFAST
- GBLP
- HRPS
- QoS

## 7. COMPETENCIAS RELACIONADAS

- 220501013 -- Utilizar software de administración de red para garantizar accesibilidad de los servicios y optimizar los recursos.
- 220501017 -- Configurar los dispositivos activos de interconexión en la red que cumplan las condiciones de transmisión e intercambio de información requerida para la solución.
- 220501023 -- Administrar redes empresariales utilizando herramientas y metodologías existentes.
- 220501014 – Administrar hardware y software de seguridad en la red a partir de normas internacionales.

## 8. CRITERIOS DE EVALUACIÓN

Debido a que el evento se realizará en 3 jornadas, cada una tiene asignado un porcentaje de evaluación los cuales quedan distribuidos de la siguiente manera:



## 9.1 JORNADA DÍA 1

### CRITERIOS DE EVALUACIÓN:

#### PROCESO: NETWORKING Y SISTEMAS OPERATIVOS WINDOWS(35%)

NETWORKING (16%)			
TEMA	No.	CRITERIO A EVALUAR DE LA PRUEBA	PUNTAJE
Diseño de direccionamiento con ipv4	1	Crea un esquema de división en subredes que cumpla con la cantidad requerida de subredes y direcciones de host	1,5
	2	Asigna una dirección IP, una máscara de subred y un gateway predeterminado a las PC	0,5
	3	Configurar las interfaces Ethernet del router con una dirección IP y una máscara de subred	0,5
	4	Crea una interface loopback en el router A y configura una dirección IP y una máscara de subred	0,5
VLSM	5	Diseña el esquema de direcciones utilizando VLSM	2
	6	Cablea y configura la red IPv4	0,5
VLANs	7	Crea redes VLAN y asignar puertos de switch	1,0
	8	Enruta tráfico entre vlans	0,5
OSPF v2	9	Configura el routing OSPFv2	1,5
NAT	10	configura instrucciones de NAT estática	1
	11	Configura las interfaces internas y externas adecuadas	0,5
DHCP Relay	12	configura un servidor de DHCPv4 y un agente de retransmisión DHCP	1
VTP	13	Configura el protocolo de enlaces troncales (VTP) en los switches	1,5
	14	Crea las VLAN en el servidor VTP y distribuye la información de estas VLAN a los switches en la red	1
Port Security	15	Configura la seguridad de puerto Port Security en un puerto de acceso de los switch	0,5
DHCP Snooping	16	Configura DHCP snooping en los switch	1
SSID	17	Establece el nombre de la red (SSID) en el AP Linksys	0,5
Wpa2	18	Establece el modo de seguridad wpa2 en el AP Linksys	0,5
Filtrado Mac	19	Configura las opciones de filtrado MAC en el AP Linksys	0,5

SISTEMAS OPERATIVOS WINDOWS (19%)			
TEMA	No.	CRITERIO A EVALUAR DE LA PRUEBA	PUNTAJE
Instalación del Sistema Operativo Windows Server 2012R2.	20	Instala el sistema operativo WINDOWS SERVER 2012 R2 en SERVIDOR A, según las especificaciones determinadas en la prueba.	2
	21	Instala el sistema operativo WINDOWS SERVER 2012 R2 en SERVIDOR B, según las especificaciones determinadas en la prueba.	
Configuración del firewall del sistema operativo.	22	Configura el firewall del sistema operativo en los equipos SERVIDOR A, SERVIDOR B y CLIENTE A, de acuerdo a los servicios a configurar en la	1



		prueba.	
Configuración del esquema del direccionamiento IPv4	23	Diseña un esquema de direccionamiento IP versión 4, aplicando subredes y VLSM, aplicable a todos los dispositivos que componen la topología de la prueba, de acuerdo a los requerimientos de la prueba.	1
Configuración del servicio AD – DS.	24	Configura el servicio AD – DS en el sistema operativo WINDOWS SERVER 2012 R2 en el equipo SERVIDOR A, según las especificaciones técnicas de la prueba.	1
Configuración del servicio DNS.	25	Configura el servicio DNS en el sistema operativo WINDOWS SERVER 2012 R2 en el equipo SERVIDOR A, según las especificaciones técnicas de la prueba.	1
Configuración de unidades organizativas, grupos y usuarios.	26	Crea las Unidades Organizativas en el sistema operativo WINDOWS SERVER 2012 R2 en el equipo SERVIDOR A, según las especificaciones técnicas de la prueba.	1.5
	27	Crea los Grupos de Usuarios del Dominio en el sistema operativo WINDOWS SERVER 2012 R2 en el equipo SERVIDOR A, según las especificaciones técnicas de la prueba.	
	28	Crea los Usuarios del Dominio en el sistema operativo WINDOWS SERVER 2012 R2 en el equipo SERVIDOR A, según las especificaciones técnicas de la prueba.	
Configuración del servicio WDS.	29	Configura el servicio WDS en el sistema operativo WINDOWS SERVER 2012 R2 en el equipo SERVIDOR A, para la distribución de imágenes del Sistema Operativo Cliente (WINDOWS 8.1).	1
Instalación del sistema operativo cliente WINDOWS 8.1.	30	Instala el sistema operativo cliente WINDOWS 8.1 en CLIENTE A, según las especificaciones determinadas en la prueba, empleando el servicio WDS.	1
Configuración del servicio ADC.	31	Configura el servicio ADC en el equipo SERVIDOR B, según los parámetros establecidos en la prueba.	2
	32	Genera réplica y tolerancia a fallos del equipo SERVIDOR A en el equipo SERVIDOR B, según los parámetros establecidos en la prueba.	
Configuración de GPO.	33	Crea las GPO en el sistema operativo WINDOWS SERVER 2012 R2 en el equipo SERVIDOR A, según las especificaciones técnicas de la prueba.	1
Configuración del servicio https a través de Internet Information Services.	34	Configura el servicio HTTPS en el equipo SERVIDOR A, a través del servicio Internet Information Services, según los parámetros establecidos en la prueba.	1
Configuración del servicio ftps a través de Internet Information Services.	35	Configura el servicio FTPS en el equipo SERVIDOR A, a través del servicio Internet Information Services, según los parámetros establecidos en la prueba.	1
Configuración del servicio DHCP.	36	Configura el servicio DHCP en el equipo SERVIDOR A, a través del servicio Internet Information Services, según los parámetros establecidos en la prueba.	1
Configuración del servicio de correo electrónico.	37	Configura el servicio de correo electrónico en el equipo SERVIDOR A, a través del aplicativo EXCHANGE, según los parámetros establecidos en la prueba.	1
Configuración el servicio de impresión.	38	Configura el servicio de impresión en el equipo SERVIDOR A, empleando la impresora virtual del sistema operativo, según los parámetros establecidos en la prueba.	1
Configuración del servicio DFS.	39	Configura el servicio DFS en el equipo SERVIDOR A, creando el Nombre de Espacios mediante el servicio de archivos, según los parámetros establecidos en la prueba.	1.5
	40	Genera replicación en el servicio DFS del equipo SERVIDOR A, según los parámetros establecidos en la prueba.	

## 9.2 JORNADA DÍA 2

### CRITERIOS DE EVALUACIÓN:

#### PROCESO: SISTEMAS OPERATIVOS LINUX (35%)

**NOTA:** Todas las configuraciones en RHEL7.0 se realizan con el módulo de seguridad Security Linux SELinux en modo **enforcing**. Deshabilitar éste módulo o establecer en modo **permissive** descalificará a los participantes.

TEMA	No.	CRITERIOS A EVALUAR EN LA PRUEBA	PUNTAJE
Configuración básica networking	1	Configura nombres y contraseñas en routers y switches, según requerimientos	0.2
	2	Configura interfaces de red en los router, según requerimientos	0.3
	3	Configura protocolo de enrutamiento	0.3
	4	Configura VLAN's en según requerimientos	0.4
	5	Garantiza conectividad de la topología	0.3
Configuración Linksys WRT300N	6	Asigna nombre a la red SSID según requerimientos	0.1
	7	Asigna el modo seguridad y contraseña según requerimientos	0.3
	8	Asigna password al router según requerimientos	0.2
	9	Configura Filtrado MAC	0.2
	10	Garantiza conectividad desde dispositivo móvil a la red.	0.2
PC's Huésped RHEL7	11	Configura SELinux en modo <b>enforcing</b> . Ver <b>NOTA</b> al inicio.	0.1
	12	Crea networks modo bridge virtual	0.4
	13	Asigna cada interface de red física a cada Bridge virtual	0.3
	14	Garantiza configuración persistente de lad Bridge virtuales	0.2
Servidor RHEL7 Virtualizado	15	Asocia 1era. interfaz de red con bridge del PC huésped	0.1
	16	Configura en <b>VMM</b> una Red Virtual modo <b>Isolated</b> sin DHCP	0.2
	17	Utiliza la 2da. Interfaz de red como Red Virtual <b>Isolated</b>	0.1
	18	Utiliza la interfaz de red del cliente RHEL7 como Red Virtual <b>Isolated</b>	0.1
	19	Configura direccionamiento IP a interfaces según requerimientos	0.2
	20	Particiona disco duro virtual con <b>LVM</b> según requerimientos	0.2
	21	Asigna hostname usando <b>namePC.domain.ext</b>	0.2
	22	Configura SELinux en modo <b>enforcing</b> . Ver <b>NOTA</b> al inicio.	0.1
	23	Configura direccionamiento IP según requerimientos	0.2
	24	Configura <b>FQN</b> (Fully Qualified Name)	0.2
	25	Interfaz de red se encuentra activa y persistente	0.1
	26	Configura repositorio local de paquetes usando ISO de RHEL7	0.2
	27	Garantiza conectividad del Servidor con la networking.	0.1
Servicio DHCP multihomed	28	Instala paquete <b>dhcp</b> necesarios para el servicio	0.2
	29	Configura servicio con subnet, netmask, range IP, gateway, broadcast, domain para cada subinterfaz, según requerimientos.	0.6
	30	Incluye en la configuración la IP estática y MAC del servidor	0.2
	31	Arranca y deja persistente el servicio	0.3
	32	Servicio es funcional desde clientes en la LAN.	0.2
Servicio HTTP con Subinterfaces de Red y VirtualHost	33	Crea subinterfaces de red según requerimientos	0.2
	34	Garantiza conectividad de las subinterfaces desde otro dispositivo	0.1
	35	Instala paquete <b>httpd</b> necesario para el servicio	0.1
	36	Copia ejemplos de Sitios Web en directorio de trabajo del servicio	0.1
	37	Asigna permisos, propietarios y contextos a directorios de sitios web	0.1
	38	Configura <b>ServerName</b> con hostname del servidor.	0.1
	39	Configura <b>VirtualHost</b> del servicio con path y URLs de cada sitio web	0.3
	40	Configura <b>NameVirtualHost</b> del servicio con IP de cada sitio web	0.1
	41	Habilita firewall permanente para el servicio <b>http</b> . No deshabilitar o desinstalar <b>firewall-cmd</b> . No usar <b>iptables</b> .	0.1
	42	Habilita booleanos del <b>SELinux</b> del servicio web.	0.1
	43	Inicia y Deja persistente el servicio <b>httpd</b>	0.1
	44	Garantiza conectividad a sitios web usando solo IP ó URL sin directorio	0.1
Servicio de instalación PXE (desatendida)	45	Instala paquetes <b>httpd xinetd syslinux tftp-server</b> necesarios para el servicio	0.1
	46	Copia o monta contenido DVD en directorio de trabajo de servicio HTTP	0.1
	47	Crea archivo de configuración <b>pxe.conf</b> en directorio de configuración del servicio HTTP	0.2
	48	Copia <b>kernel</b> booteable e imagen <b>initrd</b> a directorio <b>tftpboot</b>	0.2
	49	Configura servicio <b>TFTP</b> habilitando el servicio	0.2
	50	Configura archivo <b>kickstart</b> y lo publica en servicio web	0.3
	51	Crea archivo de configuración del servidor PXE con opciones de instalación incluyendo opción con URL de archivo kickstart	0.3
	52	Incluye en la configuración DHCP línea de configuración PXE	0.1

Servicio HTTPS con Subinterfaz de Red	53	Inicia y deja persistente servicio xinetd, httpd y dhcp	0.2
	54	Habilita firewall permanente para los servicio xinetd, httpd y dhcp. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.2
	55	Garantiza instalación remota de RHEL7 usando PXE.	0.1
	56	Crea subinterfaz de red según requerimientos	0.1
	57	Garantiza conectividad de la subinterfaz desde otro dispositivo	0.1
	58	Instala paquetes httpd y mod_ssl necesarios para el servicio	0.1
	59	Crea su propio certificado CA (Certificate Authority self-signed)	0.2
	60	Copia ejemplo de Sitio Web Seguro en directorio de trabajo del servicio	0.1
	61	Configura archivo ssl.conf con ubicacion de certificado CA	0.2
	62	Configura VirtualHost de WebSeguro en archivo ssl.conf	0.2
	63	Configura NameVirtualHost de WebSeguro en archivo ssl.conf	0.1
	64	Habilita firewall permanente para el servicio httpd https. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.1
	65	Habilita booleanos del SELinux del servicio web.	0.1
	66	Inicia y Deja persistente el servicio httpd	0.1
Servicio FTP	67	Garantiza conectividad a Web Segura usando solo IP ó URL sin directorio ni socket con puerto 443	0.1
	68	Instala paquete vsftpd necesario para el servicio	0.1
	69	Crea usuarios registrados del FTP según requerimientos	0.1
	70	Garantiza permisos, propietarios y contextos de directorios de usuarios	0.1
	71	Configura servicio FTP solo para usuarios registrados.	0.4
	72	Desactiva acceso de usuario público Anonymous.	0.1
	73	Configura usuario enjaulado para administración del FTP.	0.2
	74	Habilita firewall permanente para el servicio ftp. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.1
	75	Habilita booleanos del SELinux del servicio ftp.	0.1
	76	Inicia y Deja persistente el servicio vsftpd.	0.1
Servicio NFS	77	Garantiza acceso de usuarios registrados a ftp desde maquina remota.	0.1
	78	Los usuarios ftp pueden subir archivos y/o crear directorios.	0.1
	79	Instala paquete nfs-utils necesario para el servicio	0.1
	80	Crea directorio a compartir según requerimientos	0.1
	81	Asigna permisos a directorio compartido	0.1
	82	Realiza configuración del servicio NFS en archivo exports	0.3
	83	Inicia y deja persistente servicio rpcbind y nfs-server	0.2
	84	Publica directorios compartidos en la red usando exportfs	0.2
	85	Habilita firewall permanente para servicio nfs. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.1
	86	Habilita booleanos del SELinux del servicio nfs.	0.1
Servicio SAMBA	87	Cliente linux instala paquete nfs-utils	0.1
	88	Cliente linux monta automática/ directorios compartidos en fstab	0.1
	89	Garantiza el acceso a directorio compartido	0.1
	90	Instala paquete samba-client y samba-winbind necesarios para el servicio	0.1
	91	Crea Usuarios samba segun requerimientos	0.2
	92	Asigna smbpasswd a usuarios samba	0.1
	93	Configura archvo smb.conf con mismo workgroup usado en Windows	0.2
	94	Asigna contexto samba_share_t a directorios de usuarios samba	0.3
	95	Habilita booleanos del SELinux del servicio samba.	0.1
	96	Habilita firewall permanente para servicios samba. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.1
Servicio MAIL seguro	97	Inicia y Deja persistente el servicios smb, nmb y winbind	0.1
	98	Configura y Garantiza acceso desde cliente Windows	0.3
	99	Crea usuarios regulares según requerimientos	0.05
	100	Instala paquete postfix necesario para el servicio	0.05
	101	Configura archivo main.cf con hostname, domain, network y directorio	0.1
	102	Inicia y Deja persistente el servicio postfix.	0.05
	103	Habilita firewall permanente para servicio postfix. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.1
	104	Desde cliente se puede enviar correo usando telnet protocolo smtp	0.1
	105	Instala paquete dovecot necesario para el servicio.	0.05
	106	Crea su propio certificado CA (Certificate Authority self-signed)	0.1

	107	Configura archivos 10-master.conf, 10-auth.conf y 10-mail.conf	0.1
	108	Configura archivos 20-pop3.conf y 20-imap.conf	0.1
	109	Configura certificado CA en archivo 10-ssl.conf	0.1
	110	Inicia y Deja persistente el servicio dovecot.	0.05
	111	Habilita firewall permanente para servicios pop3, pop3s, imap, imaps, smtp-ssl. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.1
	112	Desde cliente se puede revisar correo usando telnet protocolo pop3	0.15
	113	Instala paquetes httpd y mod_ssl necesarios para el servicio	0.1
	114	Instala paquetes php y squirrelmail	0.1
	115	Configura archivo ssl.conf con ubicacion de certificado CA	0.1
	116	Configura VirtualHost de Webmail en archivo ssl.conf	0.2
	117	Configura NameVirtualHost de Webmail en archivo ssl.conf	0.05
	118	Configura Server Address, domain y path en archivo config.php del squirrelmail	0.05
	119	Habilita booleanos del SELinux del servicio http y http sendmail.	0.1
	120	Habilita firewall permanente para servicios http y https. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.1
	121	Inicia y Deja persistente el servicio http.	0.1
	122	Garantiza desde cliente remoto el acceso al Webmail para envío y revisión de correos recibidos en la bandeja de entrada.	0.2
	123	Configura en cliente remoto Linux paquete Thunderbird o Evolution para envío y revisión de correos recibidos en la bandeja de entrada.	0.1
	124	Configura en cliente remoto Windows aplicación Outlook para envío y revisión de correos recibidos en la bandeja de entrada.	0.1
Servicio DNS principal	125	Instala paquete bind necesario para el servicio	0.1
	126	Realiza configuración en archivo named.conf	0.2
	127	Archivo named.conf incluye los path de los archivos que contienen las zonas directas y zonas inversas.	0.1
	128	Configura archivo con zonas directas según requerimientos	0.3
	129	Configura archivo con zonas inversas según requerimientos	0.3
	130	Habilita firewall permanente para servicios dns. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.1
	131	Inicia y Deja persistente el servicio named.	0.1
	132	Verifica con comandos nslookup y dig resolución de nombres	0.2
	133	Asigna DNS a configuración IP de clientes y verificar conectividad. IP's y Hostnames NO deben aparecer en /etc/hosts de clientes.	0.1
Servicio PROXY	134	Configura máquina virtual con segunda interfaz de red	0.2
	135	Configura en VMM una Red Virtual modo Isolated sin DHCP	0.2
	136	Utiliza la 2da. Interfaz de red como Red Virtual Isolated	0.1
	137	Utiliza la interfaz de red del cliente RHEL7 como Red Virtual Isolated	0.1
	138	Configura direccionamiento IP a interfaces según requerimientos. Cliente debe resolver IP mediante DHCP.	0.1
	139	Habilite IP Forwarding en el kernel.	0.2
	140	Configura la 1er. interfaz en la zona externa	0.1
	141	Configura la 2da. Interfaz en la zona interna	0.1
	142	Habilita firewall permanente para servicios dns, http y https en la zona interna. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.1
	143	Habilita firewall permanente para MASQUERADE, NAT y POSTROUTING. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.2
	144	Habilita firewall permanente del puerto 3128/tcp en la zona interna. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.2
	146	Habilita firewall permanente para bloquear respuesta a ping en la zona interna. No deshabilitar o desinstalar firewall-cmd. No usar iptables.	0.2
	147	Instala paquete squid necesario para el servicio	0.1
	148	Configura archivo squid.conf con reglas ACL's según requerimientos	0.3
	149	Inicia y Deja persistente el servicio squid.	0.1
	150	Garantiza navegación del cliente Linux solo con proxy en la red.	0.2
Servidor LDAP	151	Crea su propio certificado CA (Certificate Authority self-signed)	0.2
	152	Publica certificado CA en servicio web	0.1
	153	Crea Grupos, Usuarios y Contraseñas según requerimiento	0.1
	154	Instala paquete samba-client y samba-winbind necesarios para el servicio	0.1
	155	Crea Usuarios samba	0.1
	156	Asigna smbpasswd a usuarios samba	0.1

	157	Configura archivo <b>smb.conf</b> con mismo <b>workgroup</b> usado en Windows	0.1
	158	Asigna contexto <b>samba_share_t</b> a directorios de usuarios samba	0.1
	159	Habilita booleanos del <b>SELinux</b> del servicio <b>samba</b> .	0.1
	160	Habilita firewall permanente para servicios <b>samba</b> . No deshabilitar o desinstalar <b>firewall-cmd</b> . No usar <b>iptables</b> .	0.1
	161	Inicia y Deja persistente el servicios <b>smb</b> , <b>nmb</b> y <b>winbind</b>	0.1
	162	Instala paquete <b>migrationtools</b> necesarios para el servicio	0.1
	163	Configura archivo <b>migrate_common.ph</b> con el Domain Component	0.1
	164	Configura archivo <b>migrate_passwd.pl</b> con ruta de passwords usuarios	0.1
	165	Extrae Grupos, Usuarios y Passwords que conforman las Unidades Organizacionales del LDAP	0.1
	166	Genera archivos <b>Idif</b> al migrar información de la Base, Grupos y Usuarios.	0.2
	167	Instala paquete <b>nfs-utils</b> necesarios para el servicio	0.1
	168	Realiza configuración del servicio <b>NFS</b> en archivo <b>exports</b> del directorio base donde se alojan los usuarios del LDAP.	0.1
	169	Inicia y deja persistente servicio <b>rpcbind</b> y <b>nfs-server</b>	0.1
	170	Publica directorio base de usuarios LDAP usando <b>exportfs</b>	0.1
	171	Habilita firewall permanente para servicio <b>nfs</b> . No deshabilitar o desinstalar <b>firewall-cmd</b> . No usar <b>iptables</b> .	0.1
	172	Habilita booleanos del <b>SELinux</b> del servicio <b>nfs</b> .	0.1
	173	Instala paquete <b>openldap-server</b> y <b>openldap-clients</b> necesarios para el servicio	0.1
	174	Genera contraseña LDAP	0.1
	175	Configura archivo <b>bdb.ldif</b> con domain component, contraseña LDAP y path de Certificados CA	0.1
	176	Configura archivo <b>monitor.ldif</b> el Domain Component, Common Name	0.1
	177	Habilita en archivo <b>slapd</b> el modo seguro <b>ldaps</b>	0.1
	178	Inicia y deja persistente servicio <b>slapd</b>	0.1
	179	Puertos <b>389</b> y <b>636</b> estan en modo LISTEN	0.1
	180	Habilita firewall permanente para puertos <b>389/tcp</b> y <b>636/tcp</b> . No deshabilitar o desinstalar <b>firewall-cmd</b> . No usar <b>iptables</b> .	0.1
	181	Adiciona archivos <b>Idif</b> migrados con anterioridad al LDAP	0.1
	182	Garantiza acceso desde cliente LDAP	0.2
Particiones LVM	183	Gestiona particiones utilizando <b>fdisk</b>	0.1
	184	Extiende área de intercambio <b>swap</b> según requerimientos	0.1
	185	Monta automática/ <b>swap</b> extendida en archivo <b>fstab</b>	0.1
	186	Extiende <b>Volume Group</b> según requerimientos	0.1
	187	Crea nuevo <b>Volume Group</b> según requerimientos	0.1
	188	Crea nuevos <b>Logical Volume</b> según requerimientos	0.2
	189	Monta automática/ nuevos <b>Logical Volume</b> en archivo <b>fstab</b>	0.15
	190	Extiende <b>Logical Volume</b> según requerimientos	0.15
Servicio <b>RADIUS</b> integrado con MySQL y Portal Captivo	191	Instala paquetes <b>httpd</b> y <b>httpd-devel</b> necesarios para el servicio	0.1
	192	Instala paquete <b>mariadb-server</b> necesario para el servicio	0.1
	193	Inicia y deja persistente servicio <b>mariadb-server</b>	0.1
	194	Configura acceso a gestor de base de datos	0.1
	195	Crea usuario <b>radius</b> con privilegios y base de datos <b>radius</b>	0.2
	196	Instala paquetes <b>php</b> necesario para el servicio	0.1
	197	Instala paquetes <b>freeradius</b> y <b>freeradius-utils</b> necesario para servicio	0.1
	198	Inicia y deja persistente servicio <b>radiusd</b> y <b>httpd</b>	0.1
	199	Importa <b>schema.sql</b> a la base de datos <b>radius</b>	0.2
	200	Configura modulo <b>sql</b> y cambia parámetros de conexión al DBMS	0.2
	201	Configura certificado en archivo <b>ca.cnf</b> , <b>client.cnf</b> y <b>server.cnf</b>	0.2
	202	Copia portal captivo ( <b>daloradius</b> ) en directorio de trabajo servicio web	0.1
	203	Asigna permisos, propietarios y contextos a directorio de portal captivo	0.1
	204	Importa tablas <b>sql</b> del portal captivo a la base de datos <b>radius</b>	0.2
	205	Asigna parámetros de conexión a base de datos a archivo de configuración <b>.php</b> del portal captivo.	0.1
	206	Habilita firewall permanente para servicio <b>HTTP</b> y puerto <b>1812</b> . No deshabilitar o desinstalar <b>firewall-cmd</b> . No usar <b>iptables</b> .	0.1
	207	Habilita booleanos del <b>SELinux</b> del servicio <b>HTTPD</b> .	0.1
	208	Gestor de Administración Web de Portal captivo es funcional	0.1
	209	Asigna identificación e IP del servidor Radius al router inalámbrico	0.1



Servicio VoIP ASTERISK	210	Garantiza que la conexión WiFi utiliza autenticación Radius usando el portal captivo.	0.1
	211	Instala grupo paquetes <b>Development Tools</b> necesarios para servicio	0.2
	212	Instala paquetes <b>ncurses uuid-devel libuuid-devel libxml2-devel sqlite-devel bison</b> necesarios para el servicio	0.2
	213	Compila e instala de librería <b>libjansson</b>	0.4
	214	Compila e instala fuentes de <b>asterisk-13</b>	0.4
	215	Configura y adiciona Addons <b>format_mp3</b> y <b>Core-Sounds Packages</b>	0.2
	216	Inicia y deja persistente servicio <b>asterisk</b>	0.2
	217	Habilita firewall permanente para puertos 4569, 5038, 5060, 5061, 10000 y 20000. No deshabilitar o desinstalar <b>firewall-cmd</b> . No usar <b>iptables</b> .	0.2
	218	Crea usuarios y extensiones en archivo <b>sip.conf</b>	0.2
	219	Instala aplicación <b>softphone</b> (ekiga u otro) en PC portátil y Tablet	0.1
	220	Configura clientes SIP en aplicación <b>softphone</b>	0.2
	221	Garantiza comunicación VoIP entre usuarios	0.2
Cliente LDAP	222	Instala paquete <b>openldap-clients</b> necesario para servicio	0.1
	223	Instala paquetes <b>nfs-utils</b> y <b>autofs</b> necesarios para servicio	0.1
	224	Instala paquete <b>authconfig-gtk</b> y <b>nss-pam-ldapd</b> necesario para servicio	0.1
	225	Crea directorio local compartido de los usuarios LDAP	0.2
	226	Configura <b>automounter</b> para directorios de usuarios LDAP	0.4
	227	Inicia y deja persistente servicio <b>autofs</b>	0.1
	228	Configura autenticación mediante TLS con certificado CA de servidor LDAP con método LDAP password	0.3
	229	Obtiene información de usuario LDAP mediante <b>getent</b>	0.1
	230	Se loguea como usuario LDAP desde la terminal y en modo gráfico.	0.1
Acceso de Cliente RHEL7 a AD-DS Windows2012	231	Instala paquete <b>realmd</b> necesario para servicio	0.1
	232	Instala paquetes <b>oddjob oddjob-mkhomedir sssd adcli samba-common</b> necesarios para el servicio	0.2
	233	Se une al dominio ingresando la contraseña del administrador	0.2
	234	Configura archivo <b>sshd_config</b> para permitir credenciales Kerberos usando <b>ssh</b>	0.3
	235	Accede al dominio usando <b>ssh</b>	0.2

### 9.3 JORNADA DÍA 3

#### CRITERIOS DE EVALUACIÓN:



PROCESO: **SEGURIDAD EN REDES EMPRESARIALES Y TROUBLESHOOTING (30%)**

SEGURIDAD EN REDES EMPRESARIALES (20%)			
TEMA	No.	CRITERIOS A EVALUAR EN LA PRUEBA	PUNTAJE
Cliente WIN8	1	Conectoriza los cables de red de acuerdo a las especificaciones dadas.	0.13
	2	Configura la dirección IP requerida.	0.13
	3	El acceso remoto con SWITCH-B es exitoso	0.13
	4	La prueba de conectividad (PING) con SERVIDOR RADIUS es exitosa.	0.13
	5	El acceso remoto con ASA es exitoso.	0.13
	6	El acceso remoto con ROUTER-A es exitoso	0.13
	7	El acceso remoto con SWITCH-A es exitoso.	0.13
	8	La prueba de conectividad (PING) con SERVIDOR SYSLOG es exitosa.	0.13
SWITCH-B	9	Configura el servicio de Acceso Remoto Seguro (SSH).	0.40
	10	Configura NTP para la sincronización de tiempos de los dispositivos de interconexión, de acuerdo al diagrama de la red.	0.40
	11	Filtra el tráfico permitiendo el acceso remoto seguro desde CLIENTE WIN8 a través de ACL'S.	0.40







	12	Configura el servicio de Autenticación, Autorización y Auditoria (AAA) de acuerdo a los requerimientos.	0.40
	13	Configura el servicio de Monitoreo (SYSLOG) de acuerdo a los requerimientos.	0.40
SERVIDOR RADIUS	14	Habilita y configura el Servidor RADIUS de acuerdo a los requerimientos.	1
	15	Permite o Deniega el acceso a los clientes, de acuerdo a los requerimientos.	1
	16	Permite o Deniega el acceso a los clientes, de acuerdo a las credenciales almacenadas.	1
SERVIDOR TFTP	17	Configura el servidor TFTP de acuerdo a los requerimientos.	0.40
	18	Crea la copia de seguridad de los archivos de configuración inicial del dispositivo ASA.	0.40
	19	Crea la copia de seguridad de los archivos de configuración inicial del dispositivo ROUTER-A.	0.40
	20	Crea la copia de seguridad de los archivos de configuración inicial del dispositivo SWITCH-B.	0.40
	21	Crea la copia de seguridad de los archivos de configuración inicial del dispositivo SWITCH-A.	0.40
ASA	22	Conectoriza los cables de red de acuerdo a las especificaciones dadas.	0.10
	23	Establece nombre al dispositivo según las especificaciones dadas.	0.10
	24	Configura la dirección IP de las interfaces de red según requerimientos.	0.10
	25	Crea las zonas o niveles de seguridad de acuerdo a los requerimientos.	0.50
	26	Configura el servicio de Acceso Remoto Seguro (SSH).	0.50
	27	Configura el servicio de Autenticación, Autorización y Auditoria (AAA) de acuerdo a los requerimientos.	0.50
	28	Implementa el Túnel IPSEC (VPN SITE TO SITE) de acuerdo a los requerimientos dados.	2
	29	Configura la Política IKE de acuerdo a los requerimientos.	0.30
	30	Configura el SET de TRANSFORMACIONES del túnel de acuerdo a los requerimientos.	0.30
	31	Configura el CriptoMapa del túnel de acuerdo a los requerimientos.	0.30
	32	Configura las ACL's para permitir tráfico a través del túnel y de acuerdo al requerimiento.	0.30
ROUTER-A	33	Conectoriza los cables de red de acuerdo a las especificaciones dadas.	0.10
	34	Establece nombre al dispositivo según las especificaciones dadas.	0.10
	35	Configura la dirección IP de las interfaces de red según requerimientos.	0.10
	36	Configura el servicio de Acceso Remoto Seguro (SSH).	0.20
	37	Configura el servicio de Autenticación, Autorización y Auditoria (AAA) de acuerdo a los requerimientos.	0.20
	38	Implementa el Túnel IPSEC (VPN SITE TO SITE) de acuerdo a los requerimientos dados.	1
	39	Configura la Política IKE de acuerdo a los requerimientos.	0.20
	40	Configura el SET de TRANSFORMACIONES del túnel de acuerdo a los requerimientos.	0.20
	41	Configura el CriptoMapa del túnel de acuerdo a los requerimientos.	0.20
	42	Configura las ACL's para permitir tráfico a través del túnel y de acuerdo al requerimiento.	0.20
	43	Configura NTP para la sincronización de tiempos de los dispositivos de interconexión, de acuerdo al diagrama de la red.	0.20
	44	Filtra el tráfico permitiendo el acceso remoto seguro desde CLIENTE WIN8 a través de ACL'S.	0.20
	45	Configura el servicio de Monitoreo (SYSLOG) de acuerdo a los requerimientos.	0.20
SWITCH-A	46	Configura el servicio de Acceso Remoto Seguro (SSH).	0.40
	47	Configura NTP para la sincronización de tiempos de los dispositivos de interconexión, de acuerdo al diagrama de la red.	0.40
	48	Filtra el tráfico permitiendo el acceso remoto seguro desde CLIENTE WIN8 a través de ACL'S.	0.40







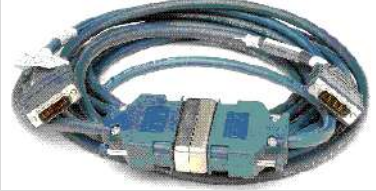
	49	Configura el servicio de Autenticación, Autorización y Auditoria (AAA) de acuerdo a los requerimientos.	0.40
	50	Configura el servicio de Monitoreo (SYSLOG) de acuerdo a los requerimientos.	0.40
SERVIDOR SYSLOG	51	Habilita y configura el Servidor SYSLOG de acuerdo a los requerimientos.	2
	52	Reporta Intento de acceso exitosos	
	53	Reporta Intento de acceso fallidos	
	54	Reporta Bloqueo de Inicio de Sesión	
TROUBLESHOOTING (10%)			
TEMA	No.	CRITERIOS A EVALUAR EN LA PRUEBA	PUNTAJE
Resuelve exitosamente los retos planteados en el estudio de caso propuesto en Packet Tracer.	55	IPv6	1.66
	56	GBLP	1.66
	57	HRPS	1.66
	58	STP	1.66
	59	PortFast	1.66
	60	QoS	1.66




## 9. MATERIALES, EQUIPOS Y HERRAMIENTAS.

ÍTEM	ELEMENTO	IMAGEN	CANTIDAD	OBSERVACIONES
1	SO Windows 8.1 PRO		1	Debe estar instalado en el equipo de cada pareja participante
2	S.O Windows server 2012 r2		1	Imágenes ISOs Archivos copiados en el computador de cada pareja



3	SO REDHAT ENTERPRISE LINUX 7.0		1	Imágenes ISOs Archivos copiados en el computador de cada pareja
4	Programa Virtualizador VMM (Virtual Machine Manager)		1	Paquetes instalados en computador de cada pareja
5	Software: Cisco Packet Tracer 6.3 o superior		1	Instalado en el equipo de los participantes
6	Computador Portátil Core I5, RAM de 4Gb, D.D. 500gb; o superior		1	Cada pareja debe traer sus equipos desde el centro de formación origen (equipos previamente formateados)
7	Tablet Android o iPad con app softphone preinstalado (Ekiga, xLite u otro)		1	Cada pareja debe traer sus equipos desde el centro de formación origen (equipos previamente formateados)
8	Computador de escritorio Core I5, RAM de 4GB, HDD 500GB; o superior		2	Debe traer dos tarjetas de red Ethernet preinstaladas. Cada pareja debe traer sus equipos desde el centro de formación origen (equipos previamente formateados y solos con el software requerido).

9	Router cisco 2900 series		2	Cada pareja debe traer este elemento desde el centro de formación origen
10	Switch cisco 2960		2	Cada pareja debe traer este elemento desde el centro de formación origen
11	Router Inalambrico (Linksys)		1	Cada pareja debe traer este elemento desde el centro de formación origen
12	ASA 5510		1	Cada pareja debe traer este elemento desde el centro de formación origen
13	Patch cords, tamaño 1,5 Mts		15	Cada pareja debe traer este elemento desde el centro de formación origen
14	Adaptador USB a Serial y cable de consola		2	Cada pareja debe traer este elemento desde el centro de formación origen
15	Enlace Serial DTE - DCE		2	Cada pareja debe traer este elemento desde el centro de formación origen

17	Driver del adaptador o cable de consola		2	Cada pareja debe traer este elemento desde el centro de formación origen
18	Software adicional:	 <ul style="list-style-type: none"> <li>• Ejemplos Sitios Web</li> <li>• Paquetes adicionales rhel7 php</li> <li>• Squirrelmail comprimido</li> <li>• Paquete rhel7 Thunderbird</li> <li>• Paquete rhel7 Evolution</li> <li>• Librería libjansson</li> <li>• Fuentes asterisk-13</li> <li>• Aplicación Windows Outlook</li> <li>• Aplicación Windows Ekiga</li> <li>• Aplicación Windows xLite</li> </ul>	1	Cada pareja debe traer este elemento desde el centro de formación origen
19	Multitomas de 6 servicios c/u		2	Cada pareja debe traer este elemento desde el centro de formación origen

## CONTROL DE DOCUMENTO

Actividad	Nombre	Cargo	Dependencia	Fecha
Redacción	Hector F. Ospina A. Yosip Van Leon Yurledy Muñoz Carlos E. Posso S.	Instructor Planta Instructor Contrato Instructor Contrato Instructor Contrato	Centro de Diseño e Innovación Tecnológica Industrial – Dosquebradas Risaralda	Marzo 10 de 2017
Revisión	José Gabriel Garavito Aponte	Instructor Líder Nacional	Centro de Tecnologías Agroindustriales	Marzo de 2017