

# **DOCUMENTO DE INFRAESTRUCTURA**

---

**PROYECTO FINAL**

**4o semestre Año 2022**

## INFORMACIÓN DEL DOCUMENTO

Nombre de Proyecto:		Proyecto Final
<b>Preparada por:</b>	Diaz, Ariadna Lopez, Federico Torena, Nahuel Vazquez, Christofer Santana, Joaquín	<b>Fecha:</b> 20/ 11 / 2022

### Versiones

Ver. No.	Fecha Ver.	Actualizado por:	Descripción
1.0	24/09/2022	The Boys	Sprint 1
3.0	22/10/2022	The Boys	Sprint 3
4.0	05/11/2022	The Boys	Sprint 4
5.0	20/11/2022	The Boys	Sprint 5



# CONTENIDO

CONTENIDO.....	3
OBJETIVOS.....	4
REQUERIMIENTOS .....	4
CONSIDERACIÓN DE DIRECCIONAMIENTO IP .....	5
SWITCHING .....	6
ENRUTAMIENTO .....	6
ESQUEMA FISICO DE RED.....	7
ELECCION DE MEDIOS .....	8
ELECCION DE UPS.....	8
UBICACIÓN DE DATA CENTER Y REFRIGERACIÓN.....	9
CONSOLIDACIÓN DE SERVIDORES .....	10
DATA CENTER PRINCIPAL.....	10
DATA CENTER DE RESPALDO .....	11
DIAGRAMA DE ELEMENTOS.....	12
ESTRUCTURA LOGICA DE RED.....	14
DIAGRAMA LOGICO DE RED.....	14
ORGANIZACIÓN DE ACTIVE DIRECTORY.....	15
ROLES Y SERVICIOS.....	15
IMPLEMENTACIÓN DE ACTIVE DIRECTORY.....	16
Roles establecidos .....	16
ORGANIZACIÓN DE ACTIVE DIRECTORY .....	17
DETALLE DE POLITICAS DE GRUPO (GPO).....	19
IMPLEMENTACIÓN DE POLITICAS DE GRUPO .....	21
ORGANIZACIÓN DEL BOSQUE.....	21
CONFIGURACION DE POLITICAS DE GRUPO .....	22
WINDOWS UPDATE.....	30
REPLICACIÓN DE ACTIVE DIRECTORY .....	31
CONFIGURACIÓN DE SERVIDOR DE APLICACIONES .....	33
CONFIGURACIÓN DE SERVIDOR DE BASE DE DATOS .....	35
SEGURIDAD FISICA.....	36
SEGURIDAD LOGICA.....	36
SEGURIDAD INTERNA Y EXTERNA.....	38
FIREWALL .....	38
CONFIGURACIÓN DE FIREWALL .....	38
POLITICAS DE DoS EN EL FIREWALL .....	43
DETALLE DE SISTEMAS DE AUDITORIA Y MONITOREO.....	45
MONITOREO SERVIDOR DE BASE DE DATOS.....	47
MONITOREO DE FIREWALL .....	48
HA EN EQUIPOS FORTIGATE.....	50
AUDITORIA.....	54
HERRAMIENTAS PARA LA AUDITORIA DE REDES.....	54
CONSIDERACIÓN DE SERVICIOS .....	55
DIAGRAMA DE FLUJO.....	59
CHECKLIST DE FUNCIONAMIENTO Y TESTEO COMPLETO .....	60
RDP.....	61
COSTOS DE EQUIPAMIENTOS .....	63
BACKUPS.....	63
OPORTUNIDADES DE MEJORA .....	64
CONCLUSION.....	65
ANEXOS .....	65
ESPECIFICACION TECNICA DE HARDWARE .....	65
DOCUMENTOS .....	65

## **OBJETIVOS**

Este documento representara toda la documentación pertinente al trabajo realizado por los integrantes del equipo The Boys para el área de Infraestructura con el fin de llevar a cabo un seguimiento del trabajo realizado en cada Sprint garantizando que se cumplan con los requerimientos solicitados en el Proyecto Final de Titulación intermedia.

## **REQUERIMIENTOS**

### **Objetivos**

- Representación e implementación de la red lógica, detallando los distintos objetos y sus relaciones.
- Vincular el AD con el sistema implementado en Programación.
- Detalle de Seguridad, Monitoreo y Contingencia de toda la implementación.
- Detalle de Consolidación de Servidores
- Implementar de manera práctica, parte de la solución propuesta.

### **Pautas Generales**

#### **Centralización de la información**

- Varios Nodos geográficamente distribuidos con replicación entre ellos
- Cada Nodo cuenta con AD/FSsystem/DB/Webserver
- Gestión centralizada de toda la Infra a nivel de NOS
- Securización y monitoreo de todos los Nodos
- PSI, y como se aplican los 3 pilares (C-Integ-Disp)
- Virtualización de la Infraestructura
- BCP (321, RPO, RTO)
- VPN
- C2S Road Warrior cargando información directo en el portal (único)
- S2S - Modelado en GNS3

#### **Requisitos mandatorios a ser entregados**

- Diagrama de toda la Infraestructura indicando los distintos Nodos
- Topología de Active Directory
- Detalle de estructura de relaciones y objetos del Active Directory
- GPO indicando su aplicación y sitios remotos
- Autenticación de sus sistemas contra el Active Directory
- Detalle de Servicios y su ubicación (DNS/DHCP/IIS/WSUS)

- Detalle de PSI
- Detalle de estrategia y mecanismos de seguridad (UTM/DMZ/SegEndPoint,etc)
- Manejo de Parches
- Monitoreo de sistemas
- Virtualización, detalle y representación de al menos 3 Hosts
- Detalle del BCP (Business Continuity Plan)
- FODA
- Estimación de la inversión

## CONSIDERACIÓN DE DIRECCIONAMIENTO IP

A continuación, se detallan las VLANs que hemos diseñado para la situación planteada y su correspondiente red. Con el diseño de estas redes no solo cubrimos los requerimientos de los puestos solicitados por piso (300) y el posible crecimiento inmediato (150 más), sino que además tenemos un margen aún para un eventual crecimiento posterior, ya que cada red tiene 510 host posibles.

Como los dispositivos de IoT pueden crecer bastante y no tenemos la cantidad que son con exactitud, a esta red la hemos diseñado más grande pudiendo crecer hasta 1022 dispositivos.

**Tabla de VLANS - Direccionamiento**

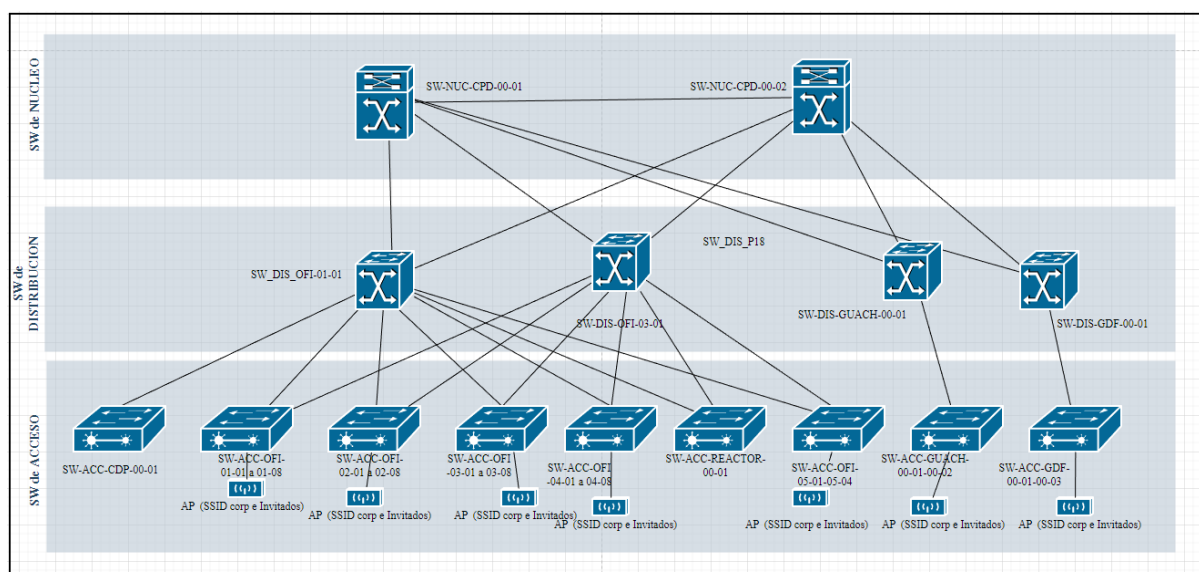
Departamento	VLAN	IP Red
SERVIDORES	VALN-110	192.168.10.0/24
GERENCIA	VLAN-120	192.168.20.0 /23
RRHH	VLAN-130	192.168.30.0 /23
CONTADURÍA	VLAN-140	192.168.40.0 /23
SANIDAD	VLAN-150	192.168.50.0 /23
LOGÍSTICA	VLAN-160	192.168.60.0 /23
SEGURIDAD	VLAN-170	192.168.70.0 /23
TELEFONÍA	VLAN-180	192.168.80.0 /23
DTI	VLAN-190	192.168.90.0 /23
ADMINISTRATIVO	VLAN-200	192.168.100.0 /23
IoT	VLAN-210	192.168.110.0 /22
WIFI CORP	VLAN-220	192.168.120.0/23
WIFI INVITADOS	VLAN-230	192.168.130.0/23

**Tabla de Direccionamiento de Servidores**

Planilla de IP de Servidores			
Nombre Servidor	IP	Mascara	Puerta de enlace
W2-SERVI-WEB-01	192.168.10.2	255.255.255.0	192.168.10.1
W2-SERVI-BD-01	192.168.10.3	255.255.255.0	192.168.10.1
W2-SERVI-TEL-IP-01	192.168.10.4	255.255.255.0	192.168.10.1
W2-SERVI-RESPA-01	192.168.10.5	255.255.255.0	192.168.10.1
W2-SERVI-CCTV-01	192.168.10.6	255.255.255.0	192.168.10.1
W2-SERVI-DC-01	192.168.10.7	255.255.255.0	192.168.10.1

## SWITCHING

En la siguiente imagen se visualiza el diagrama jerárquico de switches



**Capa Acceso:** Dispositivos finales, pc, impresoras...

**Capa Distribución:** Controla el flujo de tráfico. Es importante el rendimiento. Enruta Vlans. Dispositivos de alto rendimiento. Proporciona Disponibilidad y redundancia.

**Capa Núcleo (Core):** Se comunica con otras redes. Importante la Disponibilidad

## Beneficios de una Red Jerárquica

**Escalabilidad:** Facilidad para crecer y seguir manteniendo su estructura.

**Redundancia:** Muy importante cuando crece una red.

**Seguridad:** se mejora. Switch permite configurar seguridad de puerto.

**Rendimiento:** Mejora comunicación al utilizar switches de alto rendimiento.

**Fácil Administración:** Se puede copiar configuración de switches.

**Fácil Mantenimiento:** Por la modularidad, al escalar la red.

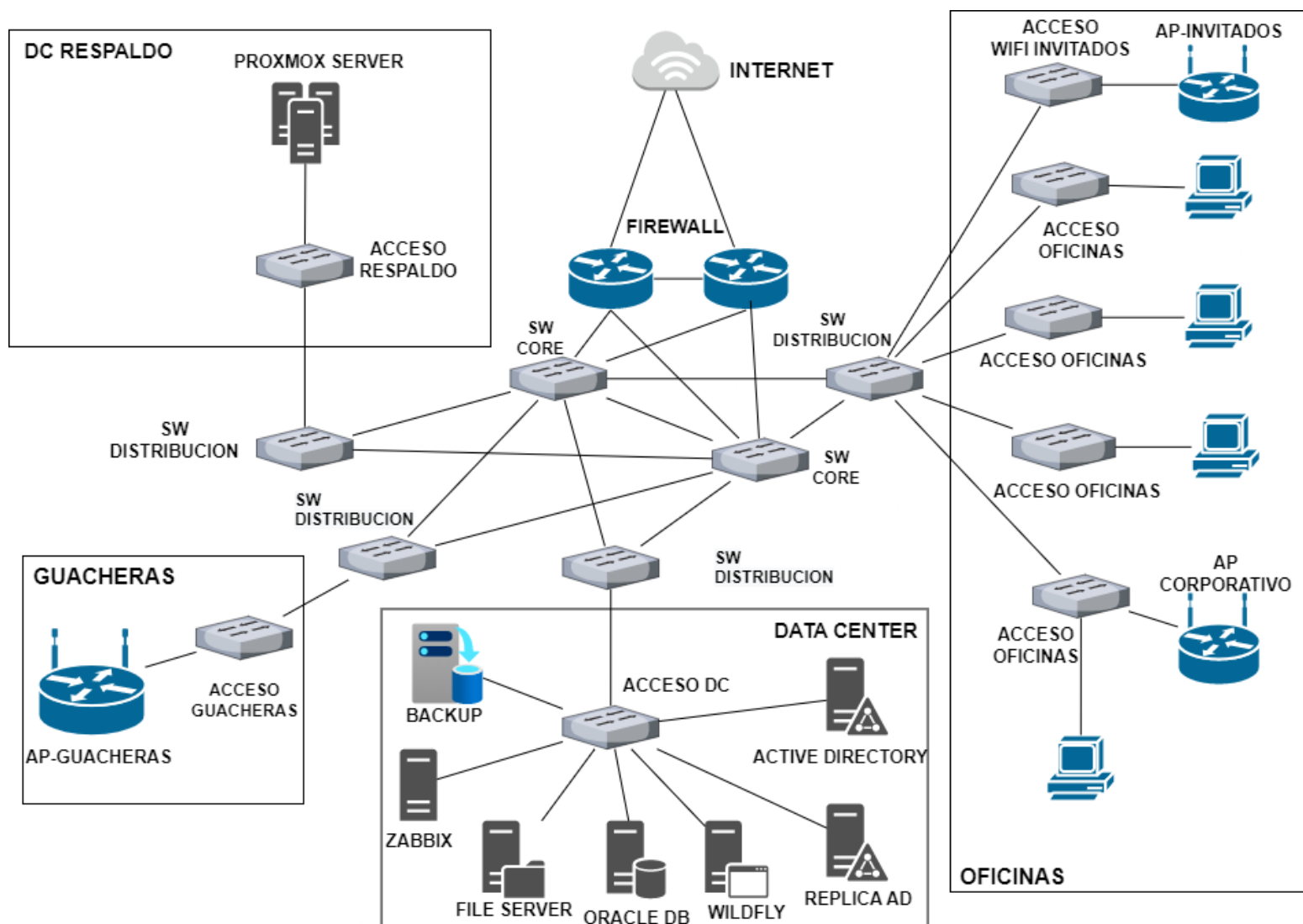
## ENRUTAMIENTO

La solución planteada es la de utilizar el enrutamiento dinámico ya que los protocolos de enrutamiento se usan para facilitar el intercambio de información de enrutamiento entre los routers. Estos protocolos permiten a los routers compartir información en forma dinámica sobre redes remotas y agregar esta información automáticamente en sus propias tablas de enrutamiento. Los protocolos de enrutamiento determinan el mejor camino hacia cada red, que luego se agrega a la tabla de enrutamiento. Uno de los principales beneficios de usar un protocolo de enrutamiento dinámico es que los routers intercambian información de enrutamiento cuando se produce un cambio de topología. Este intercambio permite a los routers obtener automáticamente información sobre nuevas redes y también encontrar rutas alternativas cuando se produce una falla de enlace en la red actual. El protocolo que se utilizará es RIP v2. RIP es un protocolo de vector distancia de tipo estándar. Su principal limitación está impuesta por la cantidad máxima de saltos que soporta (15).

Se configurará en el Firewall Core RIP v2 con el fin de garantizar que si surgen cambios en la topología de la red o si un enlace se cae este protocolo pueda identificar los cambios y redireccionar las rutas.

## ESQUEMA FISICO DE RED

A continuación, se detalla el Diagrama físico general de la red, donde podemos ubicar la distribución de cada dispositivo que conectaran a los servicios y clientes finales.



## ELECCION DE MEDIOS

Se ha optado por utilizar medios guiados de conexión para unir los (tres) 3 distintos puntos que se muestran en la imagen y que fueron tomados de referencias a partir del mapa satelital que se nos entregó. La conexión se realizará por enlaces de fibra óptica redundantes de cada sitio para con los otros dos, (conexión PTP(point to point)) formando una red totalmente conectada. La decisión se fundamenta en que es el medio que entendemos más adecuado para hacer estas conexiones, tomando en consideración varios factores que creemos prioritarios, como lo son distancia, velocidad, interferencias e inerte ante los cambios climatológicos. A su vez el tendido de la fibra de manera adecuada y subterránea (en caso de ser necesario) minimiza los posibles riesgos ambientales que puedan darse, no solo en el posible daño a la flora del lugar sino que también atendiendo a la fauna evitando contaminar más el aire con radiofrecuencias no necesarias, además aclarar que se realizará un plan de manejo mediante el cual al registrarlo, estaremos en condiciones de cuidar el monte nativo por dicho plan “para aprovechamiento de la madera” guiándonos por el decreto del poder ejecutivo en representación por el Ministerio de Ganadería aclarado en el Manual de Manejo de Bosque Nativo en Uruguay (Ministerio de Ganadería 2018,p. 19).

El tendido de las fibras ópticas entre los distintos puestos se realizará teniendo en cuenta estos temas ambientales, en cuanto al posible daño que pueda sufrir el monte nativo, ya que no prevemos ninguna tala innecesaria sobre el mismo.

Para las conexiones internas en cada punto, edificio de oficinas, galpones y depósitos, y guacheras la conexión en estos lugares será con UTP categoría 6, 6A y fibra óptica.

A su vez también contamos con medios no guiados para los dispositivos móviles, usando controladoras de red wifi, donde se publican 2 SSID distintos, uno para invitados y otro para corporativos. Ambos con su seguridad correspondiente según se entienda pertinente y en canales distintos, evitando lo más posible las interferencias conocidas en los canales de 2.4 Ghz.

## ELECCION DE UPS

### Consideraciones

- Equipamiento que se quiere proteger o mitigar una contingencia.
- Cuanta capacidad va a requerir para cubrir todo el estimado.
- Qué tipo de conexiones de entrada y salida de energía se necesitarán.
- De cuanta autonomía se quiere disponer.

Evaluado dichos parámetros, y analizando el contexto de nuestro proyecto, decidimos salir en busca de una marca líder en el mercado internacional. Se tomo en cuenta todo el equipo del DC a proteger, mas todos los sistemas críticos a mitigar. Se proveerá el DC con un servicio trifásico de UTE, donde se distribuirá en dos ATS generando bypass (A Y B).

Se dispondrá de 4 UPS rackeables para servidores, controladoras, robot de cinta, y dispositivos de red. De la marca APC modelo 3000VA Smart.

Para todo el predio, se instalará un sistema de baterías, el cual soportará todo el hardware critico por un periodo de 2 horas. Se analizo la posibilidad de instalar un generador a combustible, luego de evaluado los costos quedo descartado.



Con la solución propuesta, se logra un respaldo óptimo para nuestra implementación. No solo se estará cumpliendo con los requerimientos, sino que se estará salvaguardando toda la inversión antes fallas eléctricas.

## **UBICACIÓN DE DATA CENTER Y REFRIGERACIÓN**

Las salas contemplan un lugar para poder administrar los equipos remotamente. Equipos de aire acondicionado industriales (AA), bancos de sistema de alimentación ininterrumpida (UPS) y bancos de baterías (Baterías), todos por duplicados de manera de que si alguno de ellos falla el otro toma su lugar de forma automática.

A estas salas también se les alimenta con dos suministros de corriente distintos, uno de UTE y otro de Generador propio que comenzaría a funcionar en caso de corte del primer suministro energético (o sea ante una falla en la red de UTE), las baterías y UPS brindan la energía durante los minutos que dura en arrancar y poder dar suministro energético el generador.

En el centro de cada sala, y aislados con material adecuado se encuentran los racks de servidores y de telecomunicaciones. A esta parte se les inyecta aire frío y se les extrae el caliente con un sistema óptimo que evita lo más posible la mezcla de ambas corrientes de aires.

En los CPD se tiene previsto la instalación de un sistema de detección por detectores infrarrojos (bajo piso técnico y cielorraso), además en las salas existirán un sistema de detección temprana de aspiración. Estos estarán conectados a una central de incendio la cual tendrá un sistema de extinción por gas de agentes limpios con tiempo adecuado de evacuación en caso de personal dentro de los CPD.

Para la ubicación del montado de los DC, se consideraron tanto los requerimientos del propio proyecto, como las normas que rigen en el área, las cuales se detallan a continuación:

- Iluminación Led (utilizar led de bajo consumo).
- Consumo eléctrico.
- Prevención de incendios.
- Arquitectura (humedad, vibraciones, inundación etc).
- Libre de interferencias electromagnéticas.
- Posible expansión (Prever el crecimiento de los equipos).
- Fácil acceso (ejemplo equipos de gran tamaño).
- Barra de cobre TIERRA.

Para las medidas de los DC, es habitualmente recomendable que estos sean de 0,7 m2 por cada 10 m2 de área utilizable del edificio. Para aquellos casos en que no se cuenta con datos certeros, se puede estimar el área utilizable como el 75% del área total.

---

## CONSOLIDACIÓN DE SERVIDORES

La consolidación de servidores es la reestructuración de la infraestructura de una organización con el fin de reducir costos (Mantenimiento, consumo de energía y administración), volviéndose el área de TI más eficiente y eficaz, mejorando el control de sus recursos mediante la optimización.

### DATA CENTER PRINCIPAL

Utilizaremos servidores físicos para la base de datos, los servidores de monitoreo y los servidores de Active Directory y sus réplicas.  
También en nuestro caso vamos utilizar el servidor controlador de dominio con máquinas virtuales para la implementación de servidores de aplicación.

En el caso de VirtualBox que estamos las herramientas que componen la virtual son las siguientes.

#### Formatos de almacenaje virtual

Oracle VM VirtualBox, no solo tiene su propio formato de almacenaje, sino también tiene los siguientes formatos:

- **VDI - Virtual Disk Image:** Es el formato usado por defecto de **Oracle VM VirtualBox**.
- **VHD - Virtual Hard Disk:** Es el formato por defecto de **Virtual PC** suministrado por **Microsoft** o **XenServer** desarrollado por **Citrix**.
- **VMDK - Virtual Machine Disk:** Es el formato usado por los programas de virtualización de **VMware**.
- 

#### Formatos de configuración de red

- **NAT - Enmascaramiento de IP**
- **Adaptador puente:** Permite usar los recursos de Hardware de una tarjeta de red
- **Red Interna:** Monta una red interna entre máquinas virtuales
- **Adaptador sólo-anfitrión:** Permite configurar una tarjeta de red virtual que también pertenece a la máquina real "Anfitrión".

#### Ventajas de usar Oracle VM VirtualBox

- Te permite tener varios sistemas operativos funcionando a la vez en el mismo equipo, siempre teniendo en cuenta los recursos físicos de la máquina real.
- Permite interaccionar con las arquitecturas de 32 y 64 bits a la vez.
- Portabilidad de las máquinas virtuales, ya que pueden ser trasladadas y funcionales a través de USB.
- Gran ahorro en equipos, ya que con un solo equipo puedes tener varios sistemas funcionando. A día de hoy, es el futuro, una gran máquina suministrando con un único sistema operativo virtualizado muchos otros sistemas.

## Desventajas de usar Oracle VM VirtualBox

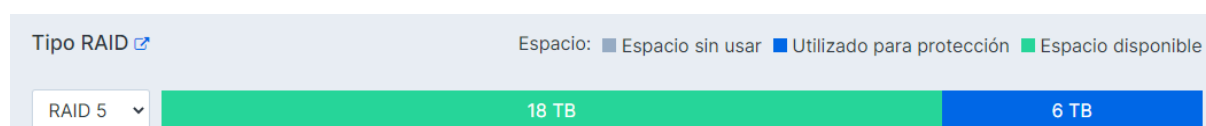
- Un equipo virtualizado tiene una potencia inferior a un equipo real. No es lo mismo un Hardware "**Emulado**" que uno "**Real**", tiene sus limitaciones.
- Carece de emulación de puertos paralelos, a día de hoy hay productos que siguen usando esta tecnología.
- La máquina real "**Anfitrión**" no puede tener fallos, sino todos los sistemas virtualizados en ella dejarán de funcionar. Por lo tanto, la máquina real se convierte en el "**Rol Crítico**" de una empresa.
- Evidentemente, el uso de "**Hardware Virtualizado**" provoca pérdidas en la venta de equipos nuevos ya que no es necesario invertir en tantos equipos/servidores.
- Desde la versión 6.0, **VirtualBox** no está disponible para sistemas operativos instalados "**Anfitrión/Real**" con arquitectura de **32 bits**. Deberán usar la versión 5.x que tenía soporte hasta el año 2020.

## DATA CENTER DE RESPALDO

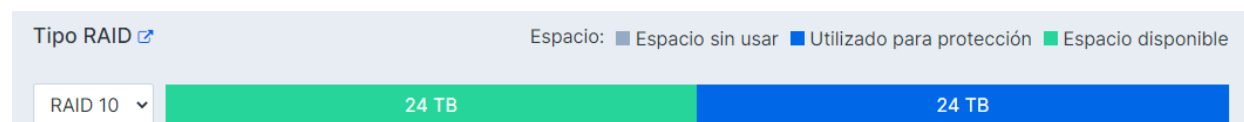
Para el Data Center de respaldo que implementaremos como contingencia a alguna falla que deje fuera de servicio al Data Center principal consideramos utilizar un servidor con el virtualizador Proxmox, también tenemos alternativas como Hyper-v y VMware vSphere pero nos inclinamos más a Proxmox ya que nos aporta flexibilidad, escalabilidad y agilidad a la hora de implementarlo. Además, reduce los costos y los gastos operativos al ser Open Source, nos aporta una alta disponibilidad, respalda la continuidad del negocio y la recuperación ante desastres ya que viene con su propio servidor de Backup integrado y también trae integrados su propio firewall donde se podremos establecer reglas y configuraciones complejas para proteger el sistema, también podremos hacer migraciones en caliente de un clúster a otro lo que nos facilita el trabajo de mover las maquinas que contienen dentro. Esta solución la consideramos ya que en el Data Center Principal utilizaremos mayoritariamente servidores físicos lo que genera un costo en Hardware mucho más elevado y como decidimos tener un Data Center de respaldo dentro de la organización no es fiable económicamente implementar servidores físicos dedicados en el Data Center de respaldo como si implementamos en el Data Center Principal, por esto contemplamos virtualizar los servidores en un único servidor dedicado utilizando Proxmox.

Considerando los requerimientos, optamos por servidores que ofrecieran, por ejemplo: doble procesador, característica "Hot Swap" en discos, fuentes y ventiladores. Cada servidor se encuentra vinculado a un servicio crítico y es por esto que consideramos la necesidad de equipos que pudieran permanecer encendidos todo el tiempo posible incluso en proceso de recambio de piezas defectuosas.

Para los servidores de aplicaciones web, telefonía IP, respaldo y DC decidimos poner servidores con 64 Gb de memoria RAM y discos en RAID 5, usaremos un total de 4 discos de 6T cada uno. Las decisiones se fundamentan en que el raid 5 para los primeros nos parece la mejor opción en cuanto a rendimiento y capacidad de almacenamiento y a su vez brinda una redundancia adecuada para estos servicios



Para los servidores de BD y Videovigilancia optamos por memoria de 128 GB y discos en raid 10, usaremos un total de 8 discos de 6T cada uno. En el caso de los de Raid 10, optamos por ellos porque entendemos que esos servicios demandan una velocidad en la lectura y escritura que se puede atender mejor con este tipo de raid que con el 5 y a su vez ambos necesitan más memoria para sus funciones.



### Aspectos fundamentales para garantizar servicios operativos 24/7

- Fuente de alimentación redundante.
- Ventiladores redundante.
- Hot Swap, nos permitirá cambiar discos averiados en caliente.
- Controladora de Raid por hardware, ya que son más fiables. Y con respecto a los RAID utilizados nos ofrecen mayor rendimiento.

## DIAGRAMA DE ELEMENTOS

### Distribución de rack de servidores y telecomunicaciones del CDP

Esquema de Racks (Comunicaciones Centro de Datos)				Esquema Racks (Servidores Centro de Datos)			
U42		Patchera FibraOptica (24 Fibras OM4)		U42		Patchera FibraOptica (24 Fibras OM4)	
U41		Patchera FibraOptica (24 Fibras OM4)		U41		Patchera FibraOptica (24 Fibras OM4)	
U40		Organizador de Cables		U40		Organizador de Cables	
U39		Organizador de Cables		U39		Organizador de Cables	
U38				U38			
U37		Router RT01		U37			
U36		Organizador de Cables		U36			
U35	O	ATS	O	U35	O		O
U34	R		R	U34	R		R
U33	G	Organizador de Cables	G	U33	G		G
U32	A	SwCore 48x10GBASE-T	A	U32	A		A
U31	N	Organizador de Cables	N	U31	N		N
U30	I	Organizador de Cables	I	U30	I	Consola de Administración	I
U29	Z	SwCore 48x10GBASE-T	Z	U29	Z		Z
U28	A	Organizador de Cables	A	U28	A		A
U27	D		D	U27	D		D
U26	O		O	U26	O	W2-SERVI-DC-01	O
U25	R		R	U25	R	W2-SERVI-CCTV-01	R
U24				U24		W2-SERVI-RESPA-01	
U23	D		D	U23	D	W2-SERVI-TEL-IP-01	D
U22	E		E	U22	E	W2-SERVI-BD-01	E
U21				U21		W2-SERVI-WEB-01	
U20	C		C	U20	C		C
U19	A		A	U19	A		A
U18	B		B	U18	B		B
U17	L		L	U17	L		L
U16	E		E	U16	E		E
U15				U15			
U14	V		V	U14	V		V
U13	E		E	U13	E		E
U12	R	Organizador de Cables	R	U12	R		R
U11	T	Sw Acceso 48xEthernet	T	U11	T		T
U10	I	Organizador de Cables	I	U10	I		I
U9	C		C	U9	C		C
U8	A		A	U8	A		A
U7	L		L	U7	L		L
U6		Patchera B (48 RJ45 Cat.6)		U6		Patchera B (48 RJ45 Cat.6)	
U5		Patchera A (48 RJ45 Cat.6)		U5		Patchera A (48 RJ45 Cat.6)	
U4				U4			
U3				U3			
U2				U2			
U1				U1			

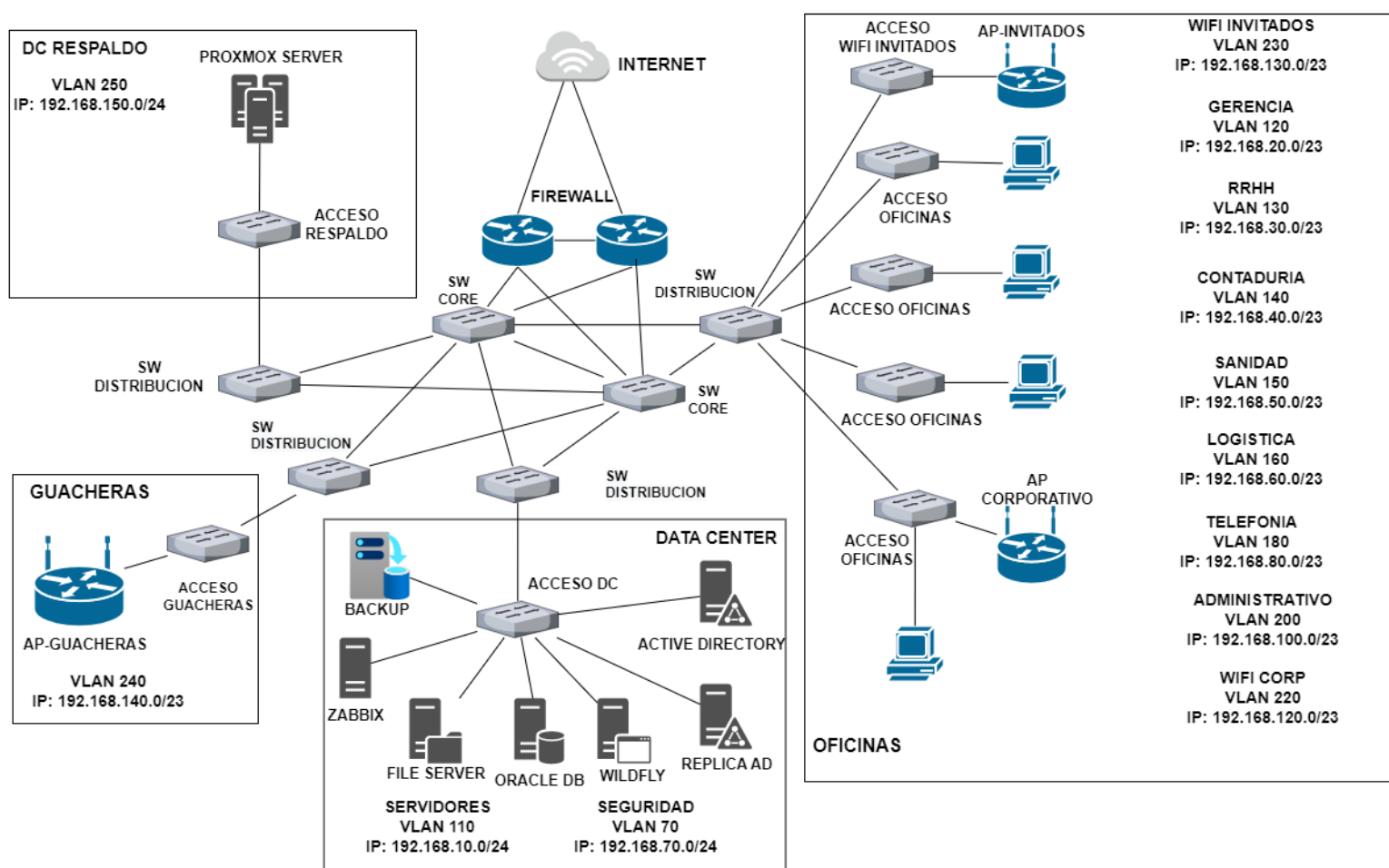
## Esquema de distribución para los pisos 1 y 3 (con SW de distribución)

Esquema de Racks (Pisos Con SW de Distribución)									
U42		Patchera FibraOptica (6 Fibras OM4)		U42		Patchera FibraOptica (12 Fibras OM4)		U42	
U41		Organizador de Cables		U41		Organizador de Cables		U41	
U40		Patchera Enlaces (24 RJ45 Cat.6a)		U40				U40	
U39		Organizador de Cables		U39				U39	
U38				U38		Organizador de Cables		U38	
U37		Controladora Red Wifi		U37		Patchera Enlaces (24 RJ45 Cat.6a)		U37	
U36		Organizador de Cables		U36		Organizador de Cables		U36	
U35	O	Sw Acceso 48xEthernet	O	U35	O	Organizador de Cables		U35	O
U34	R	Organizador de Cables	R	U34	R	Patchera Enlaces (24 RJ45 Cat.6a)		U34	R
U33	G	Organizador de Cables	G	U33	G	Organizador de Cables		U33	G
U32	A	Sw Acceso 48xEthernet	A	U32	A	Organizador de Cables		U32	A
U31	N	Organizador de Cables	N	U31	N	Patchera Enlaces (24 RJ45 Cat.6a)		U31	N
U30	I	Organizador de Cables	I	U30	I	Organizador de Cables		U30	I
U29	Z	Sw Acceso 48xEthernet	Z	U29	Z	Organizador de Cables		U29	Z
U28	A	Organizador de Cables	A	U28	A	Patchera Enlaces (24 RJ45 Cat.6a)		U28	A
U27	D	Organizador de Cables	D	U27	D	Organizador de Cables		U27	D
U26	O	Sw Acceso 48xEthernet	O	U26	O	Organizador de Cables		U26	O
U25	R	Organizador de Cables	R	U25	R	Patchera Enlaces (24 RJ45 Cat.6a)		U25	R
U24		Organizador de Cables		U24		Organizador de Cables		U24	
U23	D	Sw Acceso 48xEthernet	D	U23	D	Organizador de Cables		U23	D
U22	E	Organizador de Cables	E	U22	E	Patchera Enlaces (24 RJ45 Cat.6a)		U22	E
U21		Organizador de Cables		U21		Organizador de Cables		U21	
U20	C	Sw Acceso 48xEthernet	C	U20	C	Organizador de Cables		U20	C
U19	A	Organizador de Cables	A	U19	A	Patchera Enlaces (24 RJ45 Cat.6a)		U19	A
U18	B	Organizador de Cables	B	U18	B	Organizador de Cables		U18	B
U17	L	Sw Acceso 48xEthernet	L	U17	L	Organizador de Cables		U17	L
U16	E	Organizador de Cables	E	U16	E	Sw Distribucion 48x10GBASE-T		U16	E
U15				U15		Organizador de Cables		U15	
U14	V		V	U14	V			U14	V
U13	E		E	U13	E			U13	E
U12	R		R	U12	R			U12	R
U11	T	Patchera G (48 RJ45 Cat.6)	T	U11	T			U11	T
U10	I	Patchera F (48 RJ45 Cat.6)	I	U10	I			U10	I
U9	C	Patchera E (48 RJ45 Cat.6)	C	U9	C			U9	C
U8	A	Patchera D (48 RJ45 Cat.6)	A	U8	A			U8	A
U7	L	Patchera C (48 RJ45 Cat.6)	L	U7	L			U7	L
U6		Patchera B (48 RJ45 Cat.6)		U6				U6	
U5		Patchera A (48 RJ45 Cat.6)		U5				U5	
U4				U4				U4	
U3				U3				U3	
U2				U2				U2	
U1				U1				U1	

Como se mencionó los pisos 1 y 3, tienen los SW de distribución, además de los de SW de accesos correspondiente al piso, los SW de distribución que nuclea los SW de Acceso de varios pisos, (véase diagrama CDA), tienen su propio Rack.

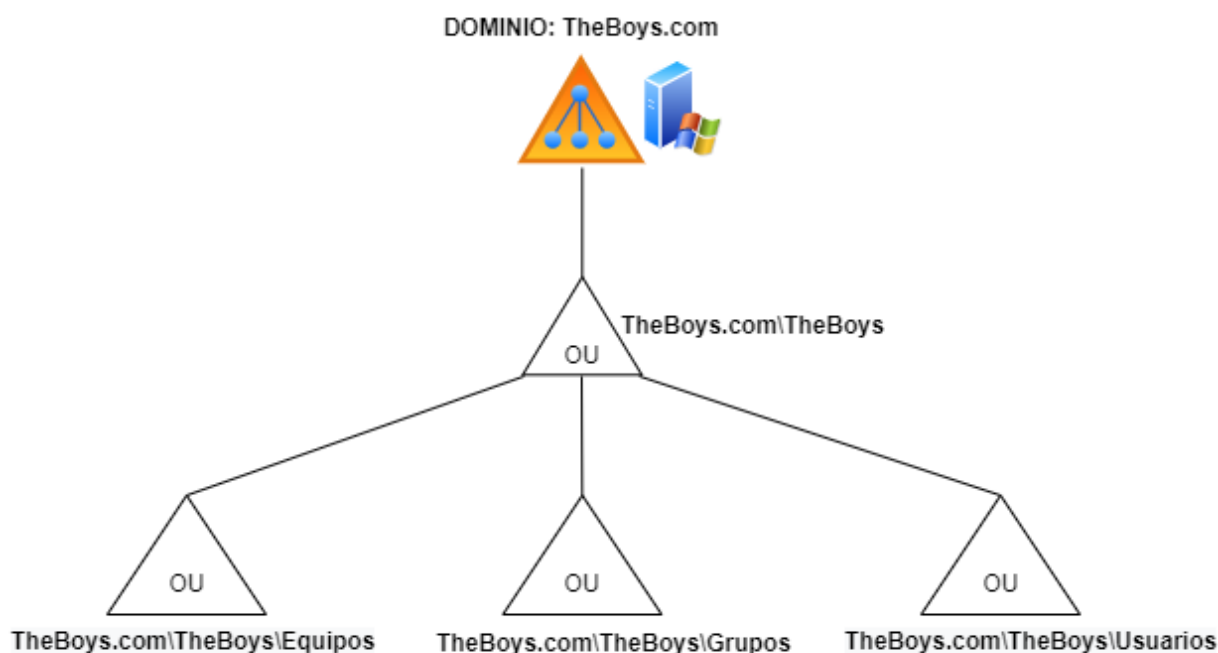
# ESTRUCTURA LOGICA DE RED

## DIAGRAMA LOGICO DE RED



## ORGANIZACIÓN DE ACTIVE DIRECTORY

En el controlador de dominio principal se establecieron tres Unidades Organizativas principales, una para cada uno de los usuarios que van a utilizar nuestra aplicación móvil y web. Dentro de cada unidad se crean grupos de usuarios y equipos que compartirán permisos, restricciones y recursos, según corresponda. De igual modo se especifican grupos de seguridad que englobarán las políticas establecidas para sus respectivos miembros.



## ROLES Y SERVICIOS

Con respecto a la implementación del Active Directory se partió desde la creación de un servidor con sistema operativo Windows Server 2012R2, al cual se le asignan los roles de AD, promoviéndolo a controlador de dominio, DNS, WSUS, IIS, Remote Access, File Server, RDP.

### DETALLES

Nombre	Windows Server
Ip estática	192.168.10.7
Mascara de red	255.255.255.0
Gateway	192.168.10.1
Dominio raíz	TheBoys.com.uy
Nivel Funcional	Windows Server 2012R2



## IMPLEMENTACIÓN DE ACTIVE DIRECTORY

A continuación, se representará la implementación del active directory en el servidor detallado en la tabla anterior.

### Roles establecidos

**Rol de AD:** Se estableció el rol de controlador de dominio, para la administración de las políticas que se aplicaran a los diferentes usuarios, departamentos y equipos que operen dentro del edificio.

**Rol DNS:** Se estableció el rol de DNS para la resolución de nombres de dominio para que los equipos de los diferentes departamentos se unan al dominio y utilicen al Active Directory como servidor de DNS.

**Rol acceso remoto:** Se estableció el rol de acceso remoto exclusivamente para el servidor de monitoreo que se detalla mas adelante en este documento.

**Rol escritorio remoto:** Se estableció el rol de escritorio remoto para la administración del servidor de forma remota ante la necesidad de solucionar o configurar el servidor sin trasladarse hasta el puesto de trabajo.

PROPIEDADES Para WIN-SERV-AD			
Nombre de equipo	WIN-SERV-AD	Últimas actualizaciones instaladas	Nunca
Dominio	theboys.com.uy	Windows Update	No configurado
		Últimas actualizaciones buscadas	Nunca
Firewall de Windows	Público: Desactivado	Informe de errores de Windows	Desactivado
Administración remota	Habilitado	Programa para la mejora de la experiencia del usuario	No participa
Escritorio remoto	Deshabilitado	Configuración de seguridad mejorada de IE	Activado
Formación de equipos de NIC	Deshabilitado	Zona horaria	(UTC-03:00) Montevideo
Ethernet	Dirección IPv4 asignada por DHCP, IPv6 habilitado	Id. del producto	00184-40000-00001-AA148 (activado)
Versión del sistema operativo	Microsoft Windows Server 2012 Datacenter Evaluation	Procesadores	Intel(R) Core(TM) i5-7200U CPU @ 2.50G
Información de hardware	innotek GmbH VirtualBox	Memoria instalada (RAM)	0 GB
		Espacio total en disco	19,66 GB

**EVENTOS**  
Todos los eventos | 18 en total

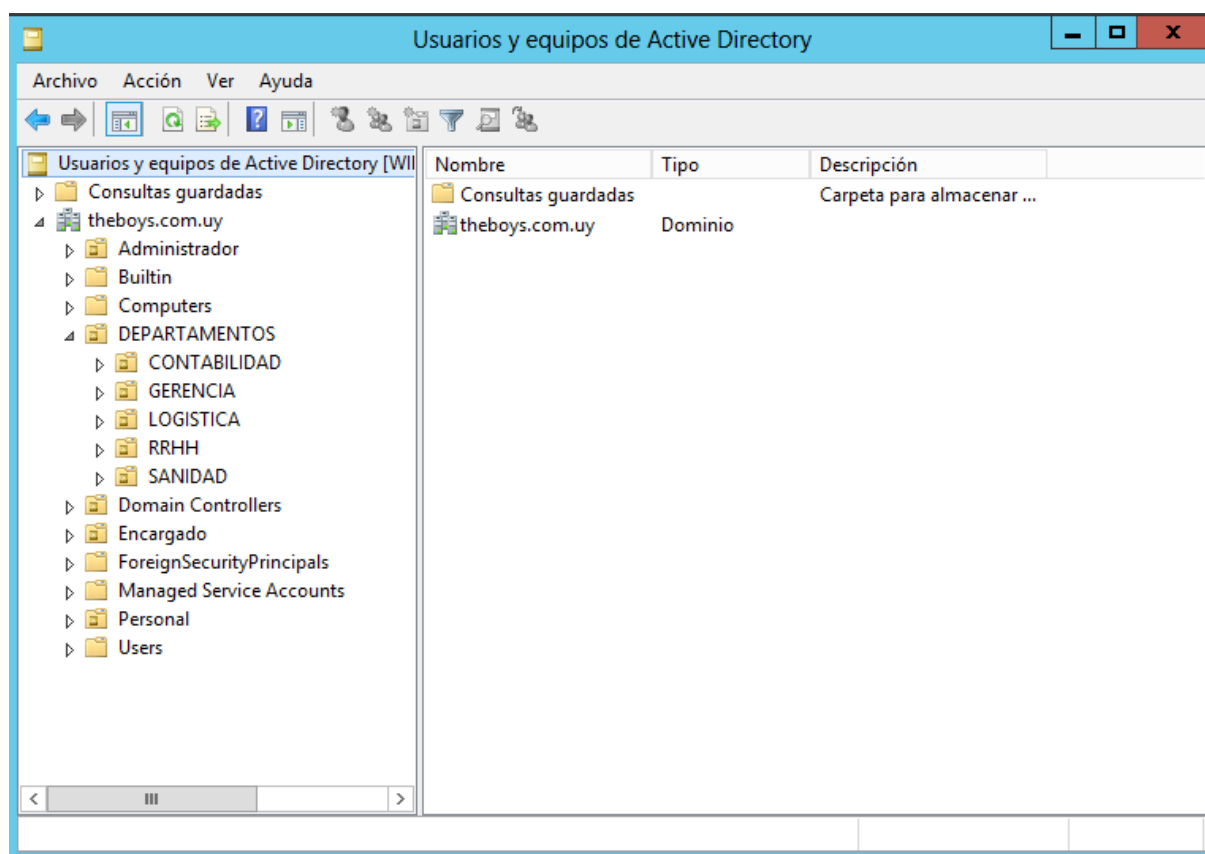


## ORGANIZACIÓN DE ACTIVE DIRECTORY

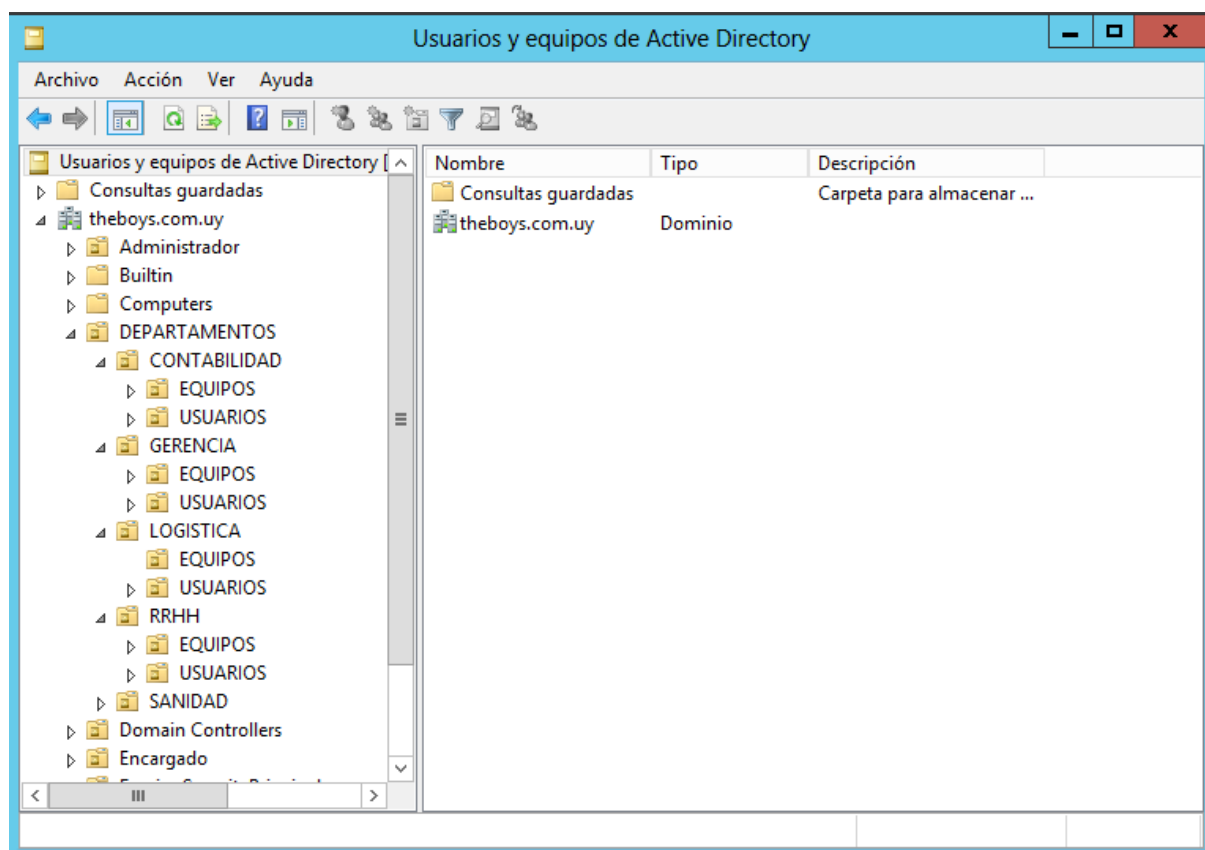
Se crearon unidades organizativas dentro del dominio **theboys.com.uy** con el motivo de organizar de mejor manera el Active Directory para posteriormente otorgarle mediante políticas de grupo diferentes accesos y prohibiciones dentro del dominio a los usuarios y equipos organizados en las diferentes unidades organizativas.

Para la aplicación web y mobile solicitada como parte del proyecto se crearon tres unidades organizativas detalladas a continuación.

NOMBRE	FUNCION
Administrador	Unidad organizativa para los roles de administradores de la aplicación web/mobile
Encargado	Unidad organizativa para los roles de encargados de la aplicación web/mobile
Personal	Unidad organizativa para los roles de usuarios que dentro de la aplicación web/mobile tienen menos permisos



Para los diferentes departamentos detallados en los requerimientos del proyecto, se creó una unidad organizativa exclusiva para los departamentos como se ve en la imagen debajo. Dentro de esa unidad organizativa se crearon otras para cada departamento y cada una de esas Unidades Organizativas contiene dentro unidades organizativas organizadas por usuarios y equipos para una mejor administración del Active Directory y para facilitarnos la aplicación de diferentes políticas de grupo a futuro.



## DETALLE DE POLITICAS DE GRUPO (GPO)

En cuanto a las políticas de grupos se considera la implementación de las siguientes en la tabla:

GPO	FUNCION
Bloqueo de puerto USB	No permitir que los usuarios conecten en los equipos dispositivos USB
Instalación de Software	Mediante la gpo se instalarán paquetes de software permitidos y aprobados por el departamento de TI
Cambio de contraseñas	Mediante esta política los usuarios al primer inicio de sesión deberán de cambiar la contraseña
Complejidad de contraseñas	Mediante esta política se le solicitara a los usuarios que ingresen contraseñas complejas
Prohibir la eliminación de software	Mediante esta política se les prohibirá a los usuarios eliminar aplicaciones del sistema operativo que sean de carácter importante
Desactivar Windows Update	Mediante esta política se deshabilita a los equipos de los departamentos la opción de actualizarse o que los usuarios finales actualicen el SO
Prohibir instalación	Mediante esta política los usuarios estarán impedidos de instalar software sin el permiso del departamento de TI.
Bloqueo de puerto Telnet	Mediante esta política se bloquea el puerto Telnet a los equipos finales con la finalidad de proteger a los diferentes equipos dentro del dominio.
Bloqueo del panel de control	Mediante esta política se le bloquea el panel de control a los usuarios que no tengan permitido.
Bloqueo de pantalla	Mediante esta política se establece que los equipos después de un determinado periodo de minutos donde el equipo no detecta que el usuario este utilizándolo, por ejemplo 10 minutos, se active el bloqueo de pantalla y el usuario deba desbloquearlo e ingresar con sus credenciales nuevamente.

Para la política de Grupo que se encarga de instalar software a los equipos del dominio se decidió que el equipo de TI será el encargado de gestionar que software será permitido o no, en el caso de que algún departamento requiera adquirir software que no este en la lista de consideraciones por parte del equipo de TI, este se encargara de verificar si el o los software no comprometan a la seguridad y sean de carácter licito, no se permiten aplicaciones de origen desconocido o que hayan sido modificadas por algún origen desconocido ni descargadas de sitios que no sean los oficiales y con el licenciamiento legal.

A continuación, se proporciona el listado de paquetes de software permitidos y su origen.

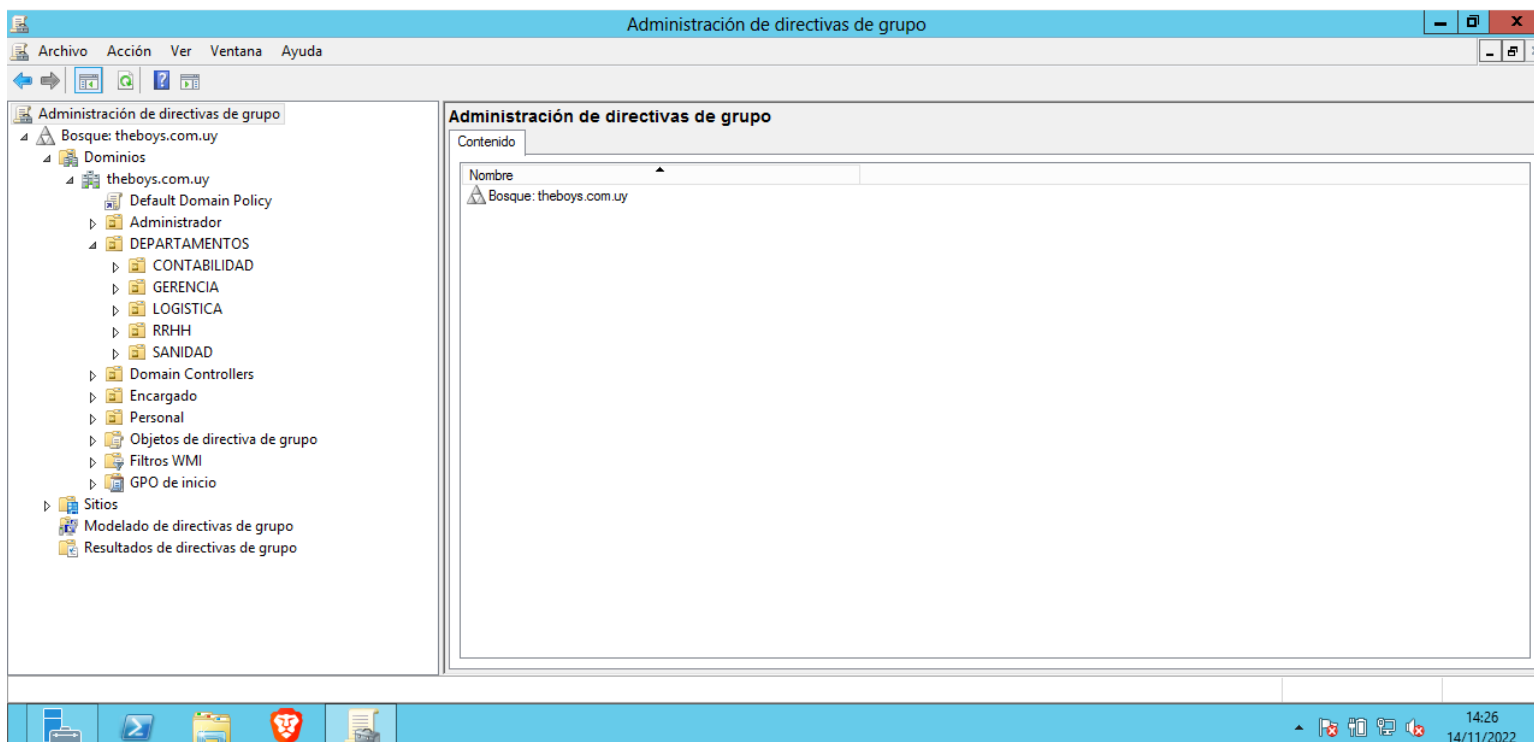
Nombre	Origen
Paquetes Office (Microsoft 365)	Microsoft
JDK Java	Oracle
Wildfly	Red Hat
Eclipse Environment	Eclipse Foundation
Oracle Database	Oracle
Git	Linus Torvalds
Navegador Brave	Brave
Zoom	Zoom
Trello	Trello Inc
Google Chrome	Google
Oracle SQL Developer	Oracle
Visual Studio Code	Microsoft
VirtualBox	Oracle
Docker	Docker

## IMPLEMENTACIÓN DE POLÍTICAS DE GRUPO

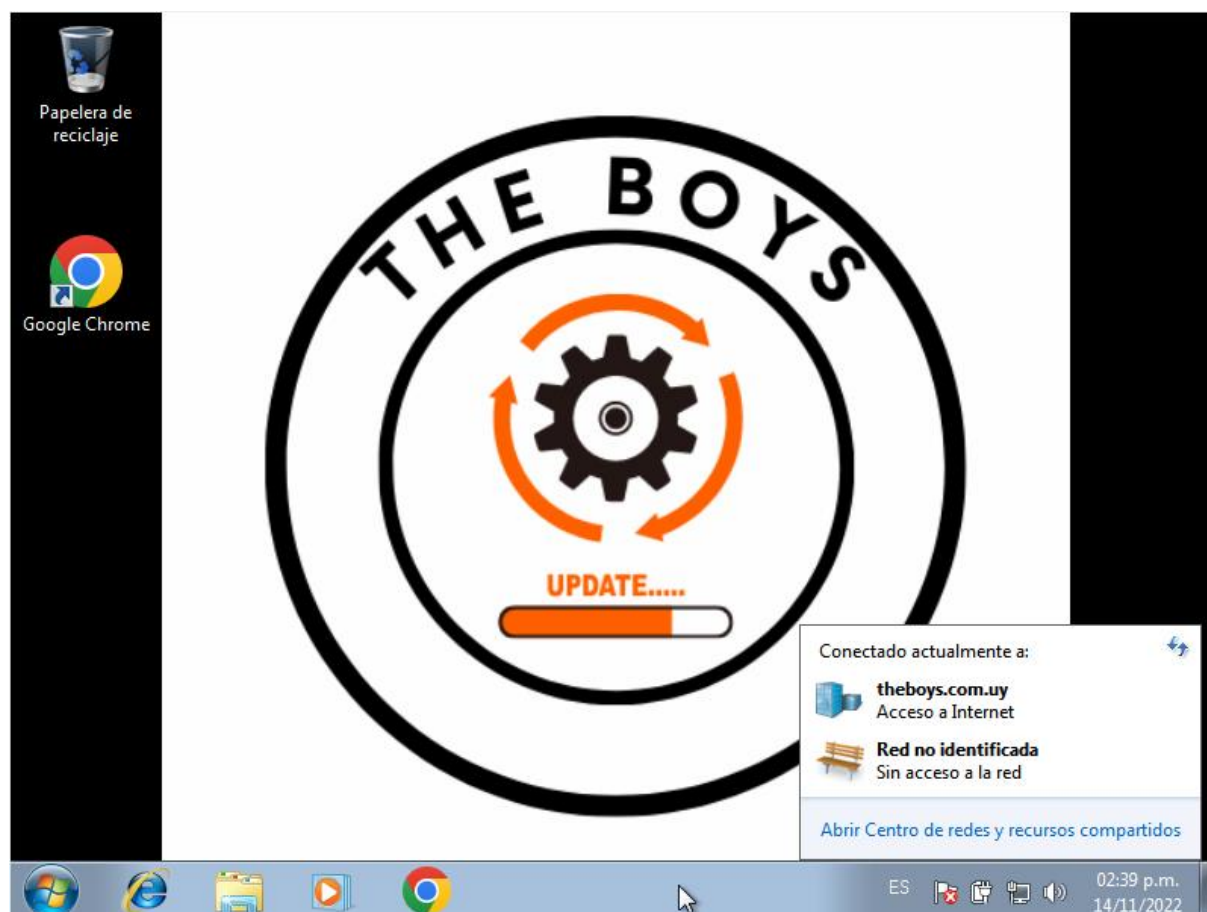
A continuación, se detalla la implementación de las políticas de grupo y la organización del bosque que contiene el dominio theboys.com.uy

### ORGANIZACIÓN DEL BOSQUE

Dentro del bosque se organizaron diferentes OU para organizar las políticas que se crearon de tal manera que cada OU tenga privilegios o prohibiciones y que no afecte al resto del dominio.



Para la verificación de que las políticas implementadas en las siguientes paginas funcionan correctamente se unieron equipos al dominio con sistema operativo Windows 7.



## CONFIGURACION DE POLITICAS DE GRUPO

A continuación, se detallan las políticas de grupo ya implementadas en el controlador de dominio mencionadas en la tabla de la página 19.

### Objetos de directiva de grupo en theboys.com.uy

Contenido Delegación

Nombre	Estado de GPO	Filtro WMI	Modificado
Admin	Habilitado	Ninguno	16/09/2022 15:44:10
Administrador	Habilitado	Ninguno	16/09/2022 15:27:20
Bloqueo de Panel de Control	Habilitado	Ninguno	14/11/2022 12:51:34
Bloqueo de pantalla	Habilitado	Ninguno	14/11/2022 12:58:20
Bloqueo de Puerto USB	Habilitado	Ninguno	14/11/2022 13:11:56
Default Domain Controllers Policy	Habilitado	Ninguno	30/10/2022 15:30:10
Default Domain Policy	Habilitado	Ninguno	15/09/2022 21:58:32
GPO bloqueo Telnet	Habilitado	Ninguno	14/11/2022 14:28:27
Gpo Desactivar Windows Update	Habilitado	Ninguno	14/11/2022 12:54:06
GPO instalacion de software	Habilitado	Ninguno	14/11/2022 13:11:30
GPO Wallpaper	Habilitado	Ninguno	14/11/2022 12:04:28
Prohibir instalacion	Habilitado	Ninguno	14/11/2022 11:32:26



Se estableció una política general que aplica para todo el dominio con el motivo de aplicarle a las contraseñas de todo el dominio la exigencia de que tengan la complejidad que trae por defecto el AD, además se estableció que las contraseñas tengan una longitud mínima de 7 caracteres y una vigencia máxima de 42 días.

Default Domain Policy	
<a href="#">Ámbito</a>	<a href="#">Detalles</a>
<a href="#">Configuración</a>	<a href="#">Delegación</a>
Directivas de cuenta/Directiva de contraseñas <a href="#">ocultar</a>	
Directiva	Configuración
Almacenar contraseñas usando cifrado reversible	Deshabilitado
Exigir historial de contraseñas	24 contraseñas recordadas
Las contraseñas deben cumplir los requisitos de complejidad	Habilitado
Longitud mínima de la contraseña	7 caracteres
Vigencia máxima de la contraseña	42 días
Vigencia mínima de la contraseña	1 días
Directivas de cuenta/Directiva de bloqueo de cuenta <a href="#">ocultar</a>	
Directiva	Configuración
Umbral de bloqueo de cuenta	0 intentos de inicio de sesión no válidos
Directivas de cuenta/Directiva Kerberos <a href="#">ocultar</a>	
Directiva	Configuración
Aplicar restricciones de inicio de sesión de usuario	Habilitado
Tolerancia máxima para la sincronización de los relojes de los equipos	5 minutos
Vigencia máxima de renovación de vales de usuario	7 días
Vigencia máxima del vale de servicio	600 minutos
Vigencia máxima del vale de usuario	10 horas
Directivas locales/Opciones de seguridad <a href="#">ocultar</a>	
Acceso a la red <a href="#">ocultar</a>	
Directiva	Configuración

**Bloqueo de Puerto USB:** a continuación, se muestra la configuración de la política que prohíbe a los usuarios utilizar dispositivos USB como forma de extraer o insertar información u otro tipo de archivos que comprometan la integridad y la seguridad del dominio.

Bloqueo de Puerto USB

Ámbito

Detalles

Configuración

Delegación

Estado

Bloqueo de Puerto USB

Datos recopilados el: 14/11/2022 14:30:41

Configuración del equipo (habilitada)

ocultar todo

Directivas

ocultar

Plantillas administrativas

ocultar

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

Sistema/Acceso de almacenamiento extraíble

ocultar

Directiva

Configuración

Comentario

Discos extraíbles: denegar acceso de ejecución

Habilitado

Configuración del usuario (habilitada)

ocultar

Configuración no definida.

**Bloqueo de Panel de control:** a continuación, se detalla la configuración de la política que le bloquea a los usuarios el uso del panel de control del equipo al cual inicien sesión.

**Bloqueo de Panel de Control**

Ámbito
Detalles
Configuración
Delegación
Estado

**Bloqueo de Panel de Control**  
Datos recopilados el: 14/11/2022 14:29:00 [ocultar todo](#)

**Configuración del equipo (habilitada)** [ocultar](#)  
Configuración no definida.

**Configuración del usuario (habilitada)** [ocultar](#)

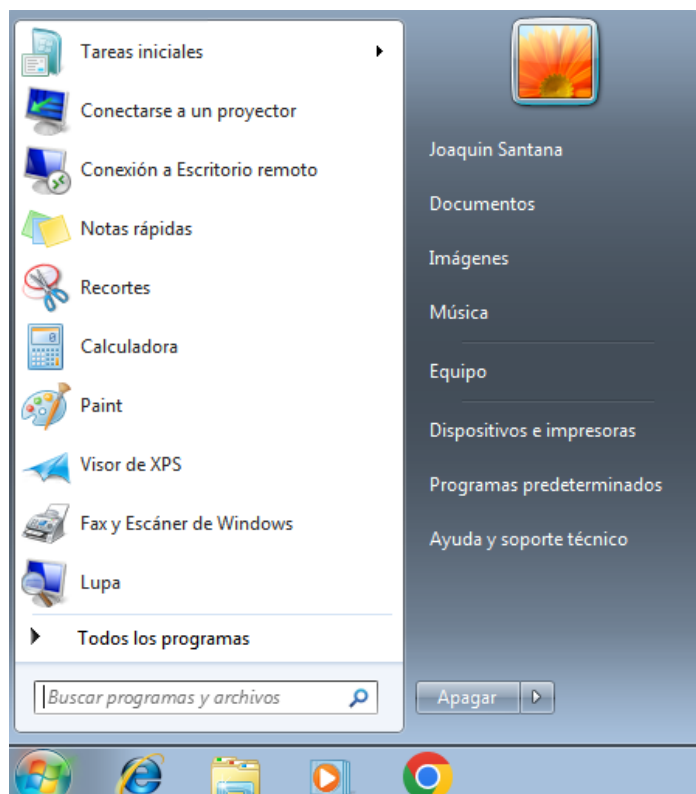
**Directivas** [ocultar](#)

**Plantillas administrativas** [ocultar](#)  
Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

**Panel de control** [ocultar](#)

Directiva	Configuración	Comentario
<a href="#">Prohibir el acceso a Configuración de PC y a Panel de control</a>	Habilitado	

A continuación, se detalla la aplicación de la política correctamente comprobando que el panel de control no está disponible para este equipo.







**Bloqueo de pantalla:** a continuación, se detalla la configuración de la política que bloquea la pantalla de los equipos después de un periodo determinado de tiempo de inactividad.

#### Bloqueo de pantalla

[Ámbito](#) [Detalles](#) [Configuración](#) [Delegación](#) [Estado](#)

**Bloqueo de pantalla**  
Datos recopilados el: 14/11/2022 14:29:53 [ocultar todo](#)

**Configuración del equipo (habilitada)** [ocultar](#)  
Configuración no definida.

**Configuración del usuario (habilitada)** [ocultar](#)

**Directivas** [ocultar](#)

**Plantillas administrativas** [ocultar](#)  
Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

**Panel de control/Personalización** [ocultar](#)

Directiva	Configuración	Comentario
Habilitar protector de pantalla	Habilitado	
Proteger el protector de pantalla mediante contraseña	Habilitado	
Tiempo de espera del protector de pantalla	Habilitado	
Número de segundos de espera hasta que se active el protector de pantalla		
Segundos:	10	

**Bloqueo de puertos:** a continuación, se detalla la configuración de la política que bloquea el puerto 23 Telnet, el puerto ssh 20 y puerto ftp 21 mediante firewall.

#### GPO bloqueo Telnet

[Ámbito](#) [Detalles](#) [Configuración](#) [Delegación](#) [Estado](#)

**Reglas de entrada** [ocultar](#)

Nombre	Descripción
Bloqueo de puertos	
Esta regla puede incluir algunos elementos que la versión actual del módulo de informe GPMC no puede interpretar	
Habilitado	Verdadero
Programa	Cualquiera
Acción	Bloquear
Equipos autorizados	
Usuarios autorizados	
Protocolo	6
Puerto local	23, 20, 21
Puerto remoto	Cualquiera
Configuración ICMP	Cualquiera
Ámbito local	Cualquiera
Ámbito remoto	Cualquiera
Perfil	Todo
Tipo de interfaz de red	Todo
Servicio	Todos los programas y servicios
Permitir cruce seguro del perímetro	Falso
Grupo	



**GPO Windows Update:** a continuación, se detalla la configuración de la política que desactiva el Windows update a los equipos.

**Gpo Desactivar Windows Update**

Ámbito Detalles Configuración Delegación Estado

Datos recopilados el: 14/11/2022 14:32:11 [ocultar todo](#)

**Configuración del equipo (habilitada)** [ocultar](#)

**Directivas** [ocultar](#)

**Plantillas administrativas** [ocultar](#)

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

**Componentes de Windows/Windows Update** [ocultar](#)

Directiva	Configuración	Comentario
<a href="#">Configurar Actualizaciones automáticas</a>	Deshabilitado	

**Configuración del usuario (habilitada)** [ocultar](#)

Configuración no definida.

**Prohibir Windows Installer:** a continuación, se detalla la configuración de la política que desactiva el Windows installer para que los usuarios no instalen software o cualquier tipo de archivo que pueda comprometer la seguridad del equipo.

**Prohibir instalacion**

Ámbito Detalles Configuración Delegación Estado

Datos recopilados el: 14/11/2022 14:34:46 [ocultar todo](#)

**Configuración del equipo (habilitada)** [ocultar](#)

**Directivas** [ocultar](#)

**Plantillas administrativas** [ocultar](#)

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

**Componentes de Windows/Windows Installer** [ocultar](#)

Directiva	Configuración	Comentario
<a href="#">Desactivar Windows Installer</a>	Habilitado	
Deshabilitar Windows Installer		Siempre

**Configuración del usuario (habilitada)** [ocultar](#)

Configuración no definida.



**Gpo fondo de escritorio:** a continuación, se detalla la configuración de la política que impide y aplica un fondo de escritorio designado por los administradores del dominio.

**GPO Wallpaper**

Ámbito Detalles Configuración Delegación Estado

**GPO Wallpaper**  
Datos recopilados el: 14/11/2022 14:34:21 [ocultar todo](#)

**Configuración del equipo (habilitada)** [ocultar](#)

Configuración no definida.

**Configuración del usuario (habilitada)** [ocultar](#)

**Directivas** [ocultar](#)

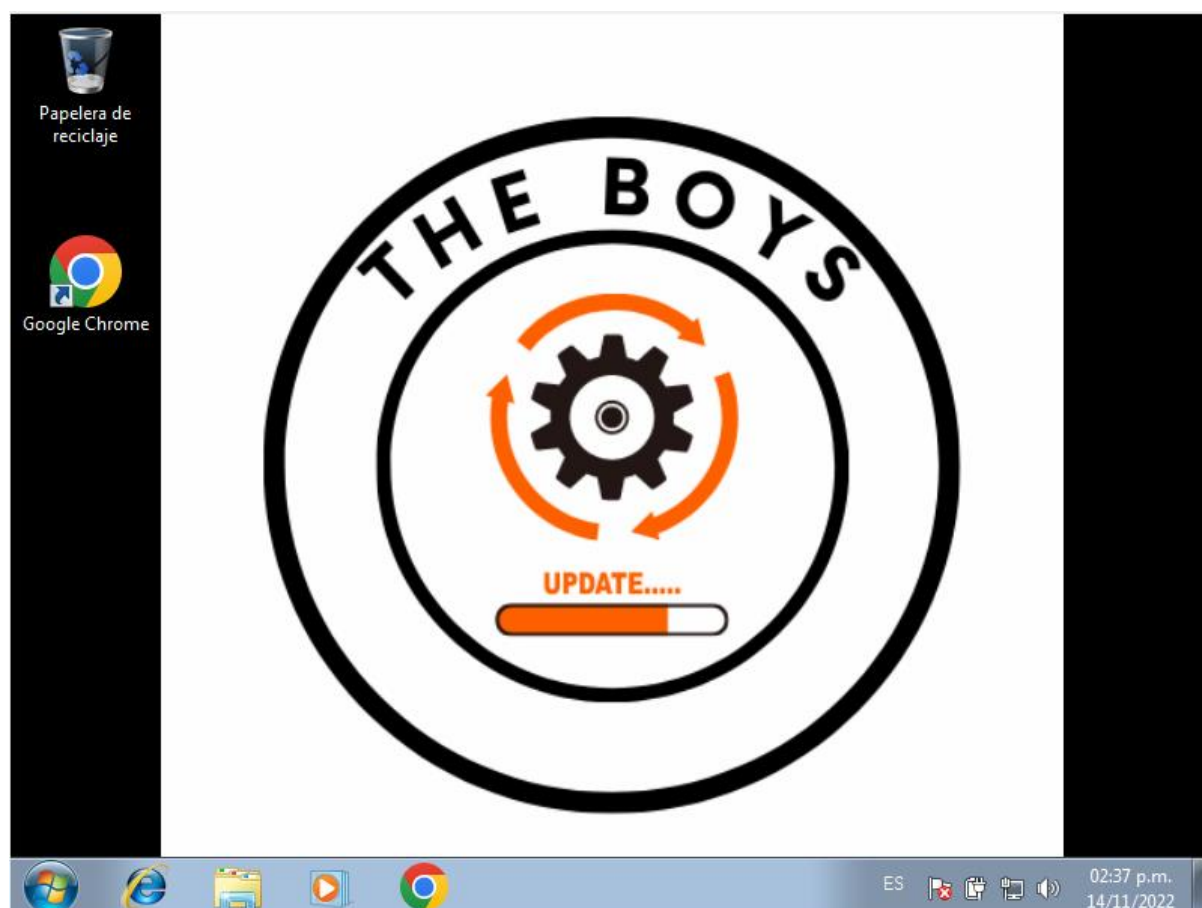
**Plantillas administrativas** [ocultar](#)

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

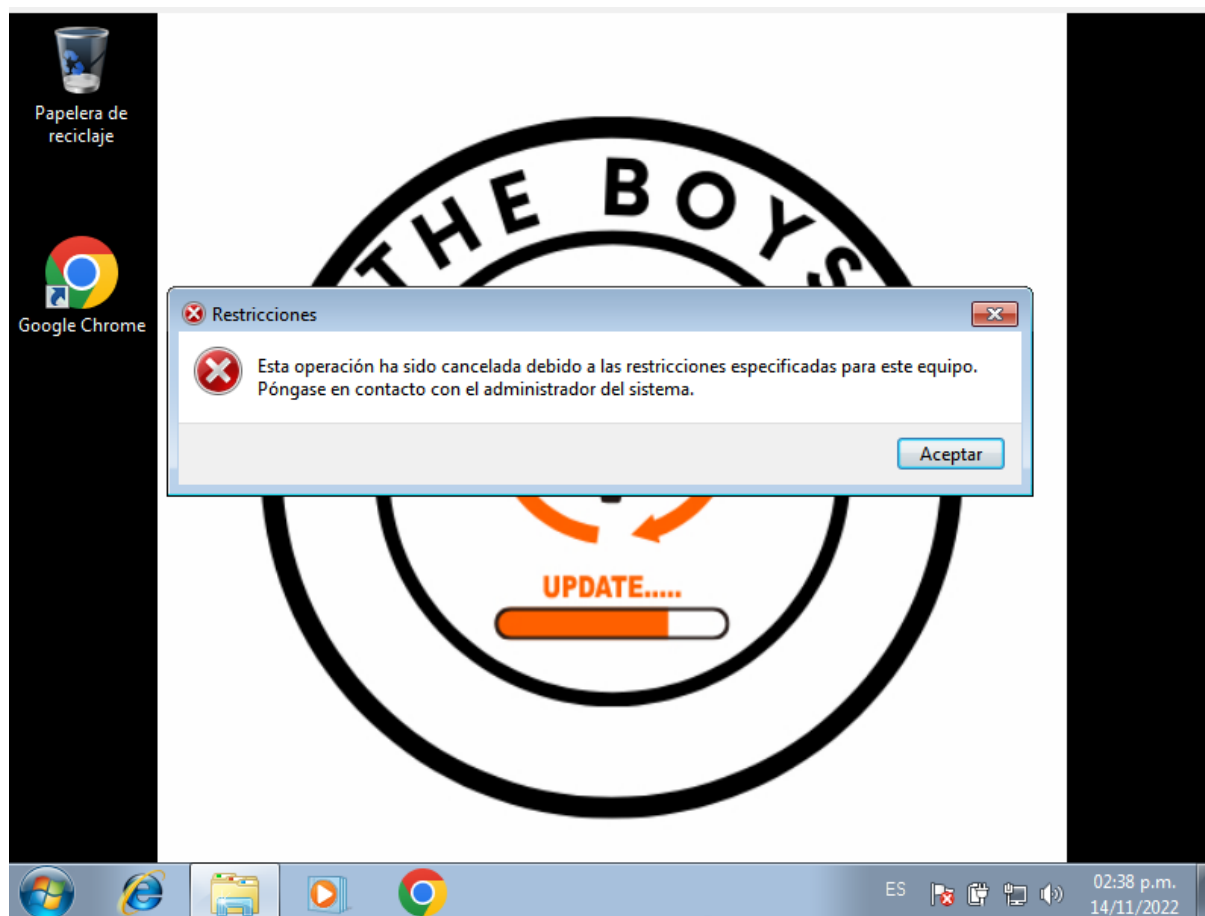
**Active Desktop/Active Desktop** [ocultar](#)

Directiva	Configuración	Comentario
Tapiz del escritorio	Habilitado	
Nombre del papel tapiz:	\\WIN-B5GOHFVK6MP\Images\theboysjp.jpg	
Ejemplo: con una ruta de acceso local: C:\windows\web\wallpaper\inicio.jpg		
Ejemplo: con una ruta de acceso UNC: \\Servidor\RecursoCompartido\Corp.jpg		
Estilo del papel tapiz:	Ajustar	

En la siguiente imagen vemos la aplicación de la política en un equipo unido al dominio.



Para verificar que la política se aplico correctamente se intento cambiar el fondo de pantalla y tuvimos el siguiente resultado.



**Instalación de software:** a continuación, se detalla la configuración de la política que instala el software aprobado por los administradores de red a cada equipo. En este caso uno de los navegadores aprobados fue Google Chrome.

**GPO instalacion de software**

Ámbito Detalles Configuración Delegación Estado

**Google Chrome** [ocultar](#)

**Información del producto** [ocultar](#)

Nombre	Google Chrome
Versión	69.32
Idioma	Inglés (Estados Unidos)
Plataforma	x86
Dirección URL de soporte	

**Información de implementación** [ocultar](#)

General	Configuración
Tipo de distribución	Asignada
Origen de implementación	\\WIN-B5GOHFVK6MP\Images\googlechromestandaloneenterprise.msi
Opciones de la interfaz de usuario de instalación	Máximo
Desinstalar esta aplicación cuando esté fuera del ámbito de administración	Deshabilitado
No mostrar este paquete en Agregar o quitar programas en el Panel de control	Deshabilitado
Instalar esta aplicación durante el inicio de sesión	Habilitado

Opciones avanzadas de implementación	Configuración
Omitir el idioma al implementar este paquete	Deshabilitado
Hacer que esta aplicación x86 de 32 bits esté disponible en equipos de Win64	Habilitado
Incluir información de clase OLE y de producto	Habilitado

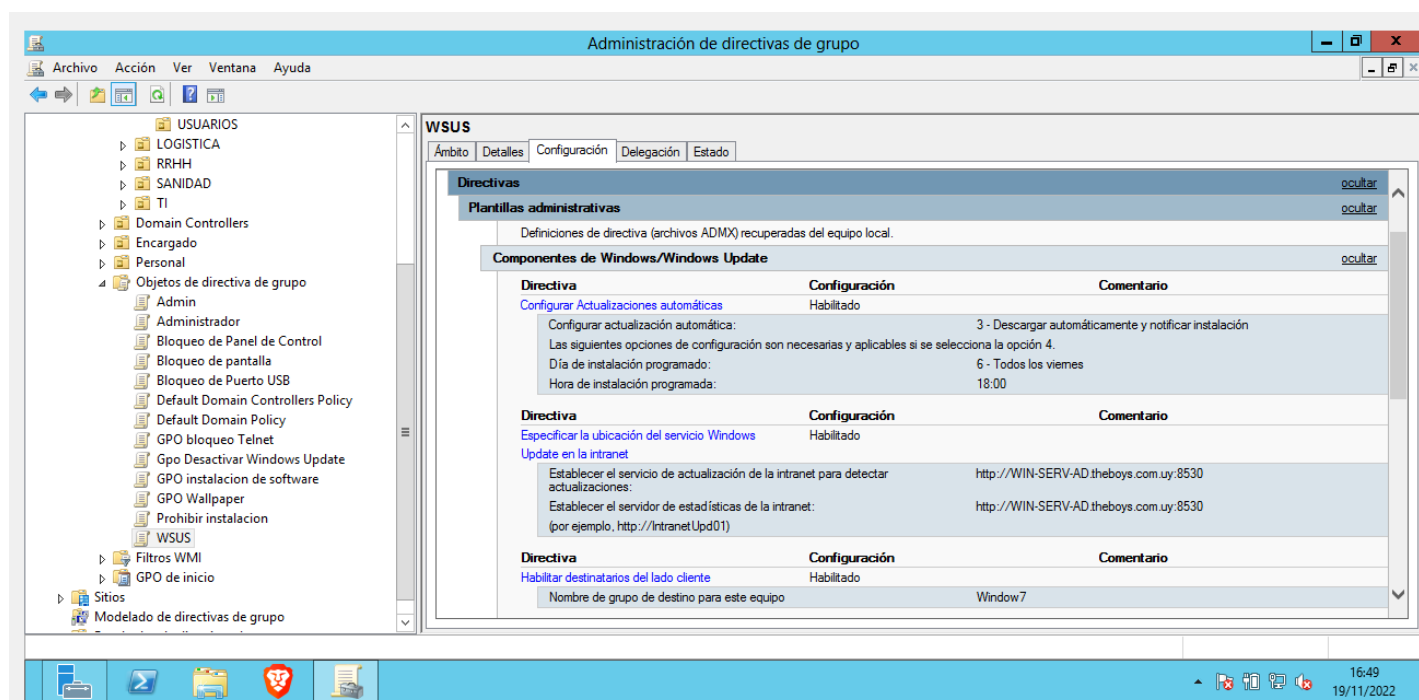
**Información de diagnóstico** [Configuración](#)

Administración de directivas de grupo

- ▲ Bosque: theboys.com.uy
  - ▲ Dominios
    - theboys.com.uy
      - Default Domain Policy
        - Administrador
        - DEPARTAMENTOS
          - CONTABILIDAD
          - GERENCIA
          - LOGISTICA
            - EQUIPOS
              - Bloqueo de Puerto USB
              - GPO bloqueo Telnet
              - Gpo Desactivar Windows Update
              - Prohibir instalacion
              - USUARIOS
                - Bloqueo de Panel de Control
                - Bloqueo de pantalla
                - GPO instalacion de software
                - GPO Wallpaper
              - RRHH
              - SANIDAD
            - Domain Controllers
            - Encargado
            - Personal
            - Objetos de directiva de grupo

## WINDOWS UPDATE

Para las actualizaciones de los sistemas operativos que pertenecen al dominio se instaló el rol de WSUS de esta forma tendremos un servicio que proporcionará las actualizaciones requeridas por los SO de manera centralizada y con el control adecuado de las actualizaciones. El equipo de TI será el encargado de gestionar estas actualizaciones y verificar si no comprometen a los equipos de dominio. Dentro de la consola de administración de WSUS se separarán a los equipos por grupos según la versión del Sistema operativo, por ejemplo, para los equipos con sistema operativo Windows 10 se creará un grupo específico para esos equipos para garantizar que las actualizaciones que se les otorgue sean compatibles con esa versión de sistemas operativos. También se creó una política de grupo para que los equipos hagan las consultas de actualizaciones al servidor que tiene el Rol de WSUS que en nuestro caso es el controlador de dominio principal, esto se hará sin que los usuarios tengan que realizar ninguna acción. Las actualizaciones serán extraídas de los servicios de actualización de Microsoft.



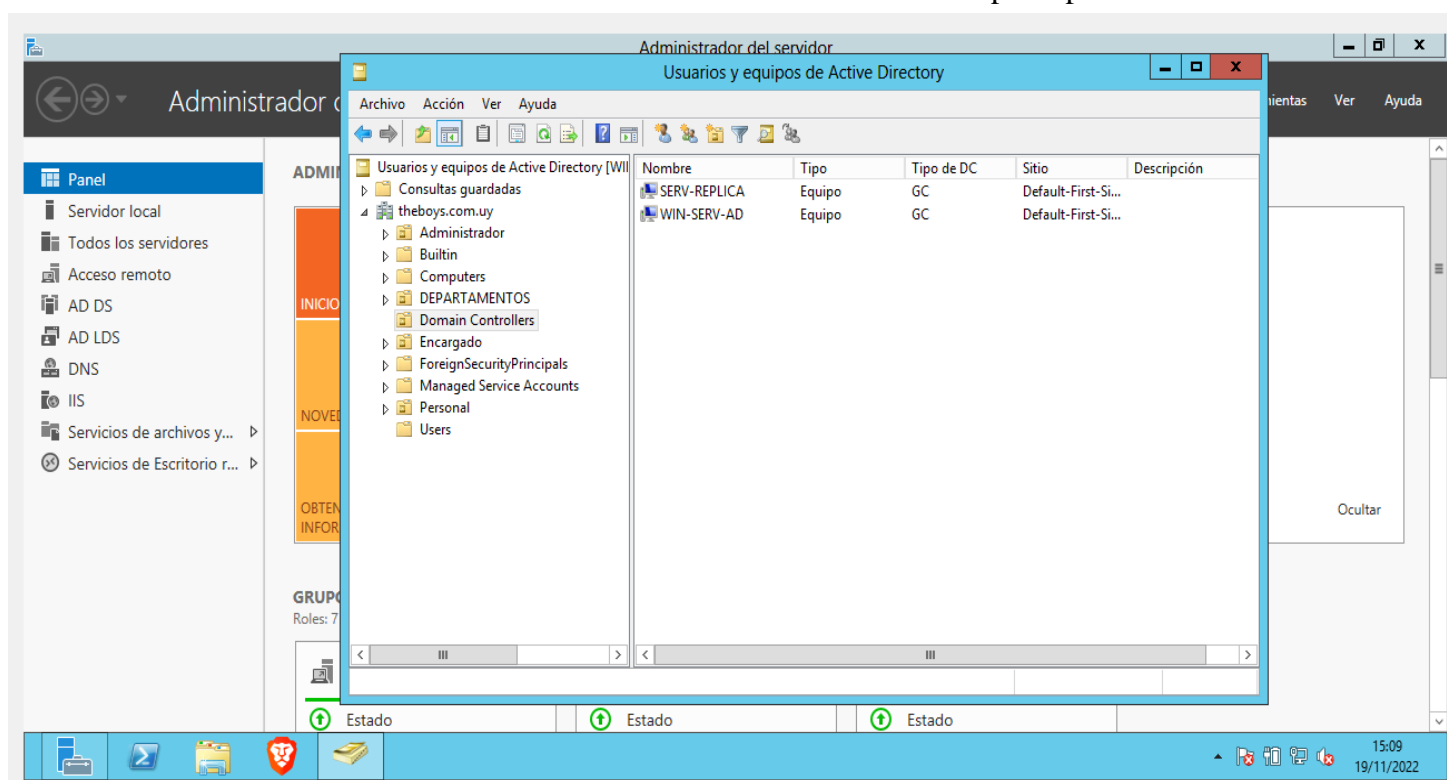
Las actualizaciones se harán automáticamente en los equipos finales, los días viernes fuera del horario laboral y sin que los usuarios tengan que aceptarlas o reiniciar los equipos para que estas se instalen, sino que se hará de forma automática en el día y la hora estipulada.

## REPLICACIÓN DE ACTIVE DIRECTORY

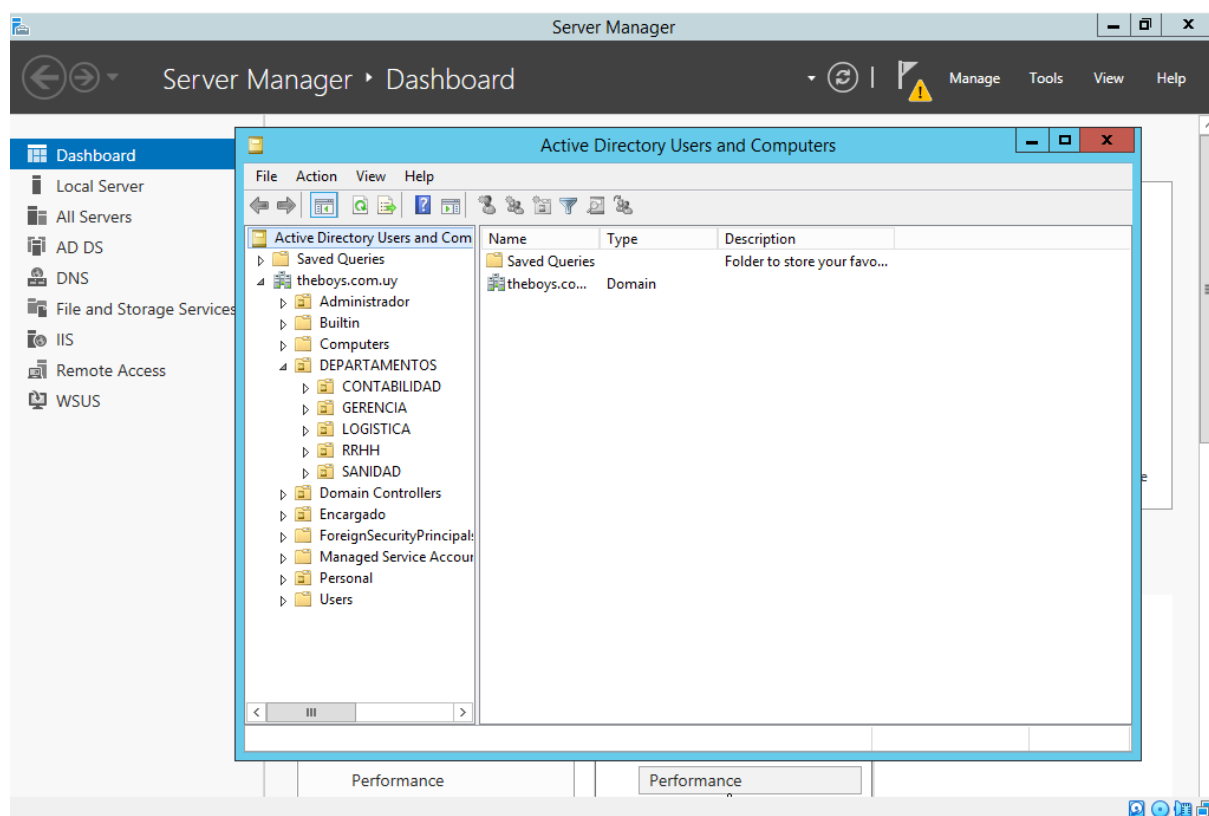
Teniendo en cuenta que en cualquier momento pueden surgir problemas en cuanto al hardware o software y que comprometan al correcto funcionamiento del Active Directory se decidió implementar un segundo Active Directory replicando al Servidor principal, de esta forma nos garantizamos de que si el AD principal no funciona el segundo AD suplante su lugar y sea capaz de gestionar a los equipos y usuarios de la red sin perjudicar las actividades correspondientes al negocio.

Para esto tendremos un segundo Windows Server 2012r2 conectado al servidor principal para que estos se comuniquen entre sí y la replicación sea activa todo el tiempo. Se hará esto para garantizar la disponibilidad de los servicios y tener una respuesta rápida a la hora de detectar una falla en el servidor principal y poder rápidamente suplantar momentáneamente los servicios que este ofrece.

A continuación, detallamos las configuraciones realizadas para solucionar lo planteado en esta sección. Lo que hicimos fue instalar un nuevo Windows server 2012r2 e instalarle los roles de controlador de dominio, DNS, IIS y WSUS, luego agregamos este segundo servidor al dominio theboys.com.uy, después de hacer eso se procedió a replicar el servidor principal con el servidor de replica para que las configuraciones sean plasmadas en el segundo servidor. De esta forma tenemos dos controladores de dominio dentro del dominio principal.



Después de finalizado el proceso de replicación pudimos constatar que el servidor de respaldo ya esta funcionando correctamente y nos garantizamos de que si el principal deja de funcionar las actividades no se verán afectadas. En la siguiente imagen se muestra como quedo replicada la organización del Active Directory en el servidor de respaldo y este aplica las mismas políticas de grupo que el servidor principal.

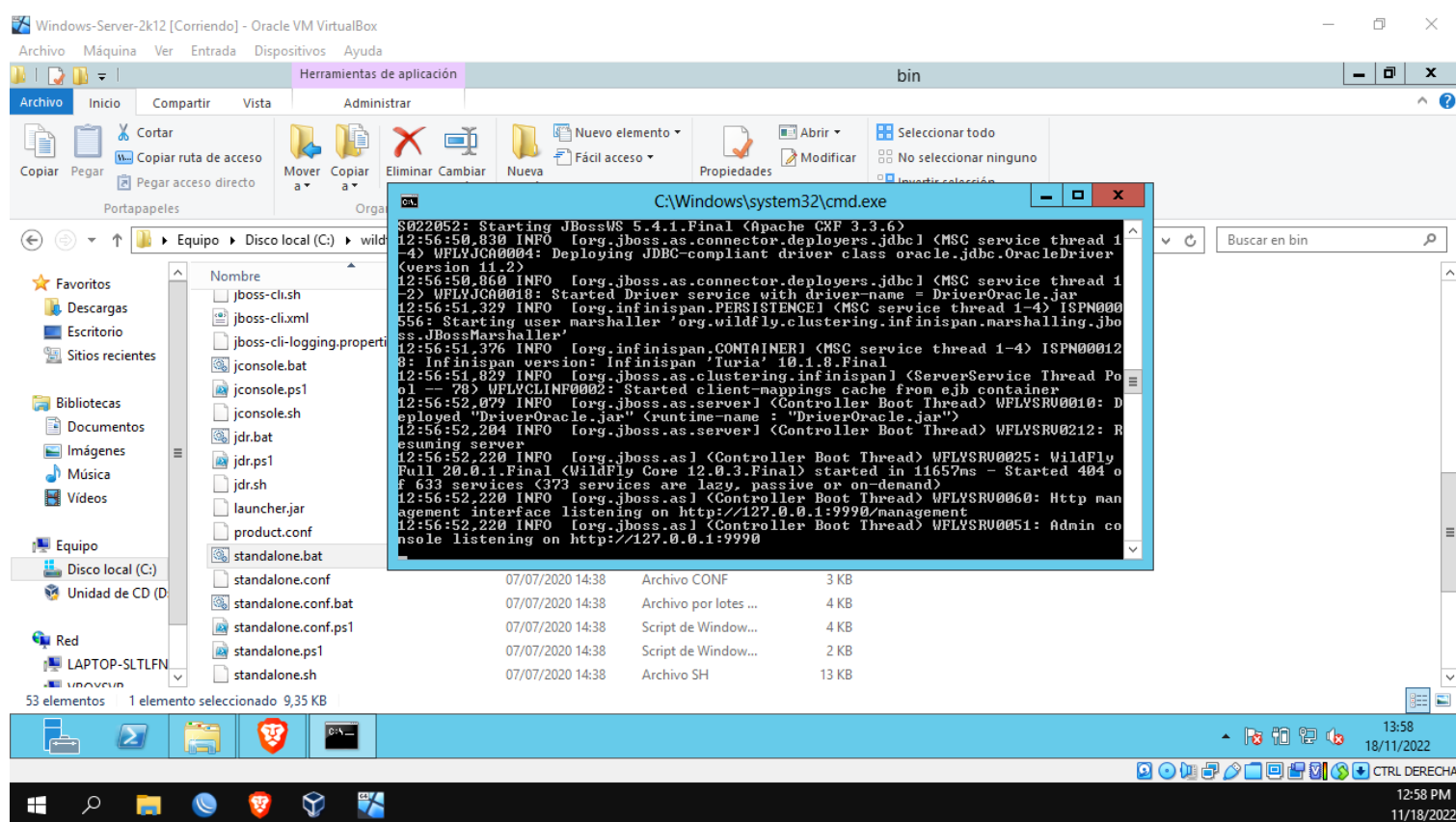




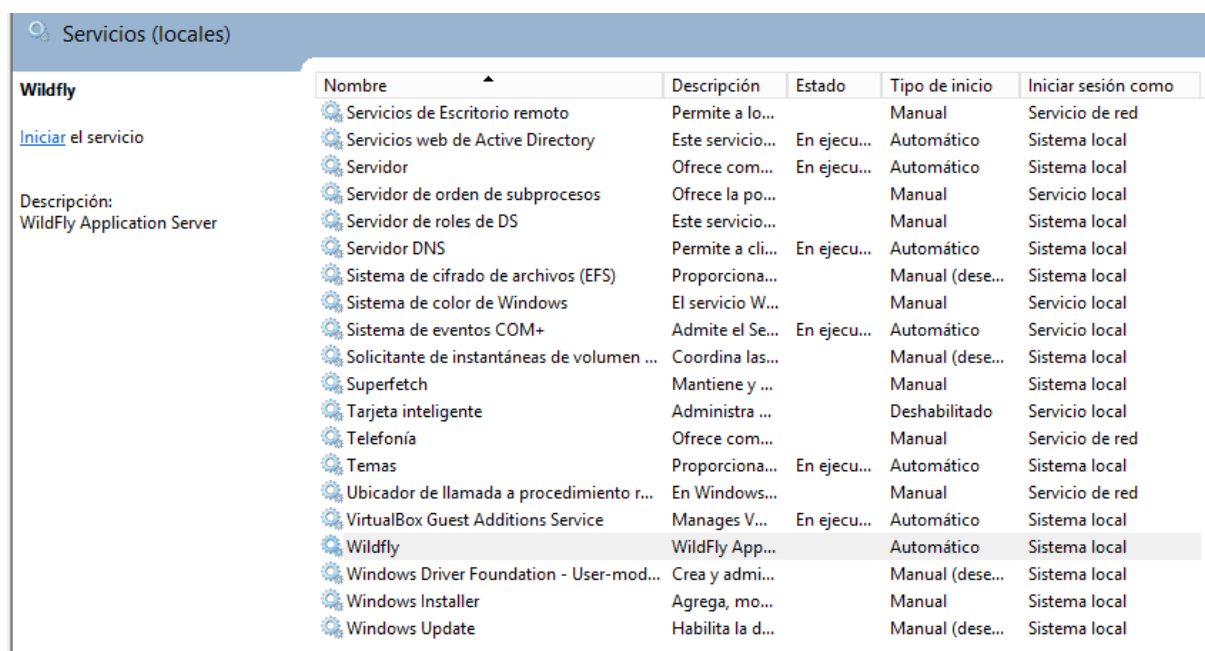
## CONFIGURACIÓN DE SERVIDOR DE APLICACIONES

Para que nuestra aplicación mobile y web este disponible para el uso de los empleados de la organización configuramos en el Windows Server controlador de dominio principal el servidor de aplicaciones Wildfly versión 20.0, en el puerto 8080 que a su vez para poder administrarlo se utilizara el puerto 9990 que es el puerto para acceder a la consola de administrador de Wildfly. Para facilitar el inicio del servidor de aplicaciones se lo agrego como un servicio del servidor en modo automático de esta manera el servidor de aplicaciones iniciara en conjunto con el controlador de dominio y no tendremos que ir a las configuraciones de Wildfly para iniciarlo.

A continuación, detallamos la implementación de lo mencionado en esta sección. En la siguiente imagen se detalla el servidor ya implementado.



En esta segunda imagen a continuación se detalla el servidor corriendo como un servicio.



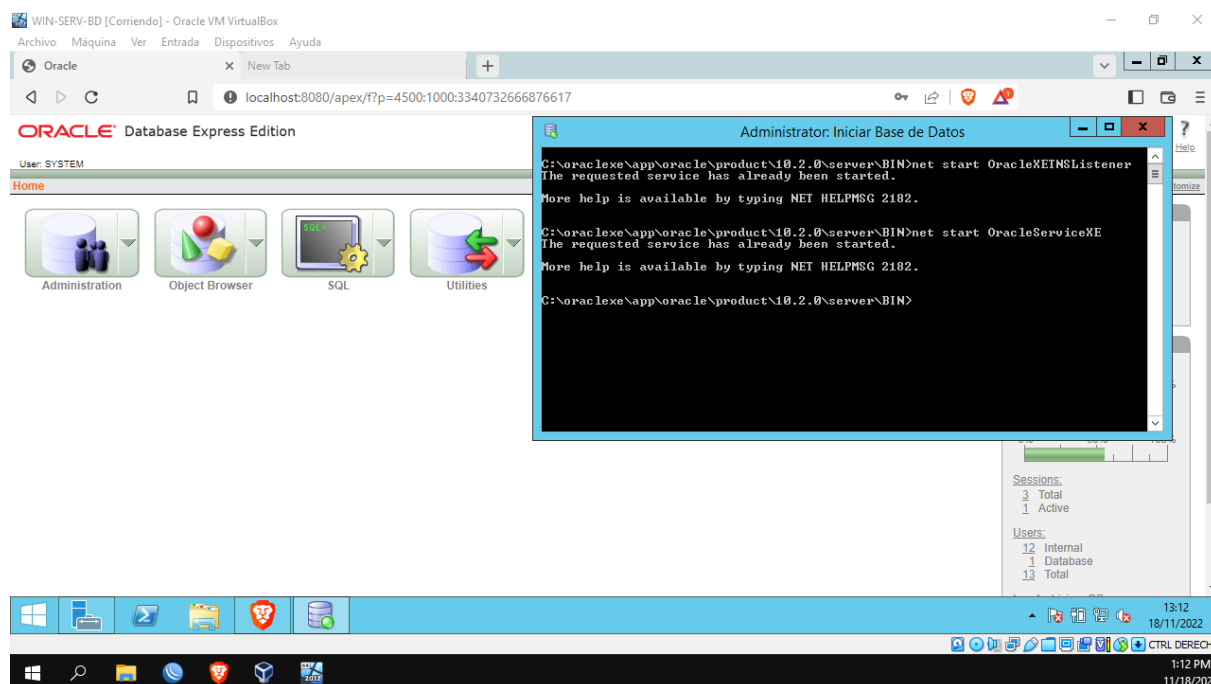
En la siguiente imagen se detalla la ip del servidor y el puerto 8080 que es el que utiliza Wildfy accediéndolo desde el navegador.



## CONFIGURACIÓN DE SERVIDOR DE BASE DE DATOS

Para la base de datos que requiere nuestra aplicación web/mobile se instalo un servidor de base de datos Oracle 10g en un sistema Windows Server 2012r2 que será el encargado de alojar la base de datos de nuestra aplicación y alojara la base de datos corporativa que es requerida para la extracción de vistas para su posterior análisis.

Como se detalla en la imagen de abajo comprobamos que Oracle esta corriendo correctamente en el servidor. Este servidor de base de datos tiene habilitado el puerto 1521/tcp que es el puerto que Oracle utiliza por defecto para comunicarse con las bases de datos.



También Oracle tiene el puerto 8080/tcp para poder acceder a la consola web de Oracle para poder administrar a los usuarios y privilegios que tienen dentro de las bases de datos además de gestionar el almacenamiento y otras funcionalidades propias de Oracle.



---

## SEGURIDAD FISICA

- La infraestructura contará con cámaras de seguridad, sensores de movimiento, sensores de temperatura, sensores de humo y personal de vigilancia. El sistema de seguridad será otorgado a una empresa de tercero y ellos se encargarán de una vez al mes hacer backups de los dispositivos de vigilancia.
- Cada integrante de la organización tendrá una tarjeta inteligente única que lo identifica para poder ingresar a los sectores que le esté permitido.
- Las puertas que comunican a sistemas sensibles de la compañía tendrán triple verificación: la tarjeta ya mencionada, huella dactilar y reconocimiento facial.
- Para evitar daños físicos en los equipos por dificultades eléctricas, se contratará un servicio de profesionales para trabajar en este tema, con el fin de evitar este tipo de inconvenientes.
- En el caso de ocurrir algún fenómeno meteorológico de grandes características (Ej: terremoto, tornado) que pueda ocasionar pérdidas importantes como un servidor en el cual estén alojados todos los datos, es necesario contar con un respaldo de todos estos registros. Para ello contaremos con un servidor espejo que cumplirá la función de back-up.
- El acceso al predio será solo a aquellos autorizados previamente y se dejará registro de cada visita de aquellas personas que no son usuarios funcionarios de la organización.
- La sala de servidores tendrá un equipamiento especial para mantener la humedad, temperatura y estática del lugar de modo de no alterar o poner en riesgo la información y disponibilidad de los servidores. Además, deberá contar con protección sobre fuego y humo.
- La sala de servidores estará con una temperatura controlada por monitores que indicarán al equipo de TI cualquier falla en el sistema de enfriamiento.
- Se contará con detectores de humo y extintores colocados de forma estratégica.

## SEGURIDAD LOGICA

Dentro de la seguridad Lógica, basaremos el acceso a la red en servidores con Dominio de la empresa el cual centralizará el acceso a los terminales de toda red.

Una de las técnicas que emplearemos para conseguir una seguridad óptima a este nivel, son la que se refiere al control de acceso. Con servidores de dominio y acceso a los terminales nos aseguramos de:

- Restringir usuarios.
- Aplicar políticas de acceso.
- Implementaremos contraseñas que cumplan con políticas de seguridad.
- Restricción de horarios de acceso de los usuarios.
- Actualizaciones centralizadas y software de seguridad, previamente testado en ambientes de prueba, para la posterior aplicación de los mismos a la infraestructura.
- Respallos físicos en centro de datos.

Los respaldos físicos en el centro de datos tendrán un servidor el cual se utilizará para dicha función, teniendo como contingencia una implementación de discos redundantes como puede ser Raid 5.

Estos controles serán implementados en los diferentes equipos, sistemas operativos, aplicaciones, etc. Son de gran ayuda para proteger todo lo mencionado de la utilización o modificaciones no autorizadas; y así lograr mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

También creemos que es conveniente considerar otras características, como por ejemplo las que detalla el NIST (National Institute for Standards and Technology), siendo requisitos mínimos de seguridad que todo sistema debe tener, dicho por ellos.

- Identificación y Autenticación
- Roles

El acceso a la información puede controlarse a través de la función o rol del usuario que requiere un determinado acceso. Algunos ejemplos de roles serían con los que estamos trabajando en nuestro sistema: Administradores, profesionales y comunes. Con esto conseguimos que los derechos de acceso pueden agruparse dependiendo del rol de los usuarios.

- Transacciones

Para cualquier tipo de transacciones, se implementarán controles, por ejemplo solicitando una clave al momento de querer realizar esta acción.

- Limitaciones de los servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de una determinada aplicación o preestablecidos por un administrador del sistema.

Por ejemplo, queremos que si por ejemplo un sistema permite la utilización simultánea de hasta dos personas (por alguna determinada licencia), existirá un control a nivel de sistema que no permita la utilización del producto a un tercer usuario.

- Ubicación y horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas.

Este tipo de controles nos permitirá limitar el acceso de los usuarios a determinadas horas del día o días de la semana. De esta forma se mantiene un control más restringido de los usuarios.

Por supuesto, hay un sin fin de maneras, pero por el momento, se trabajará principalmente en lo detallado.

---

## SEGURIDAD INTERNA Y EXTERNA

Podemos proteger tanto la seguridad interna como la externa de maneras similares. Por esta razón, decidimos detallar juntos estos dos puntos.

Creemos que un planteamiento seguro es usar en principio dos firewalls (dual firewall), ya que nos ayudará a prevenir el acceso desde la red externa a la interna.

### Ventajas

Protege de intrusiones, el acceso a ciertos segmentos de la red que solo se permite a equipos o usuarios autorizados. También optimiza la comunicación entre los elementos, definiendo distintos niveles de acceso a la información de manera que cada grupo de usuarios tenga solo acceso a los servicios e información que les está permitido.

### Políticas

Investigando y repasando conceptos vistos en las unidades curriculares de infraestructura, hay dos políticas básicas con las cuales vamos a trabajar.

- Políticas restrictivas: Denegamos todo el tráfico excepto el que está explícitamente permitido, hay que habilitar expresamente los servicios que se necesitan.
- Política permisiva: Permitiremos todo el tráfico, excepto el que está denegado. Cada servicio potencialmente peligroso necesitará ser aislado mientras que el resto de tráfico no será filtrado.

La política restrictiva es la más segura, ya que tiene control para no permitir tráfico peligroso. Sin embargo, la política permisiva es posible que no haya contemplado tráfico peligroso y sea aceptado por omisión.

## FIREWALL

Decidimos implementar dos Firewall de la marca Fortinet modelos FortiGate 60E para proteger la red, estos mismos no solo se encargarán de proteger la red sino también servirán como servidores DHCP y DNS, también dentro de sus configuraciones segmentamos la red con vlans con el fin de dividir a cada departamento y al Data Center para que no haya conflicto entre ellos y así garantizar que en cada área vaya el tráfico correspondiente. También por medio de políticas dentro de los Firewall permitiremos o rechazaremos el tráfico que cruce por ellos de tal forma que no afecte a la red interna y garantizarnos de que todo está protegido.

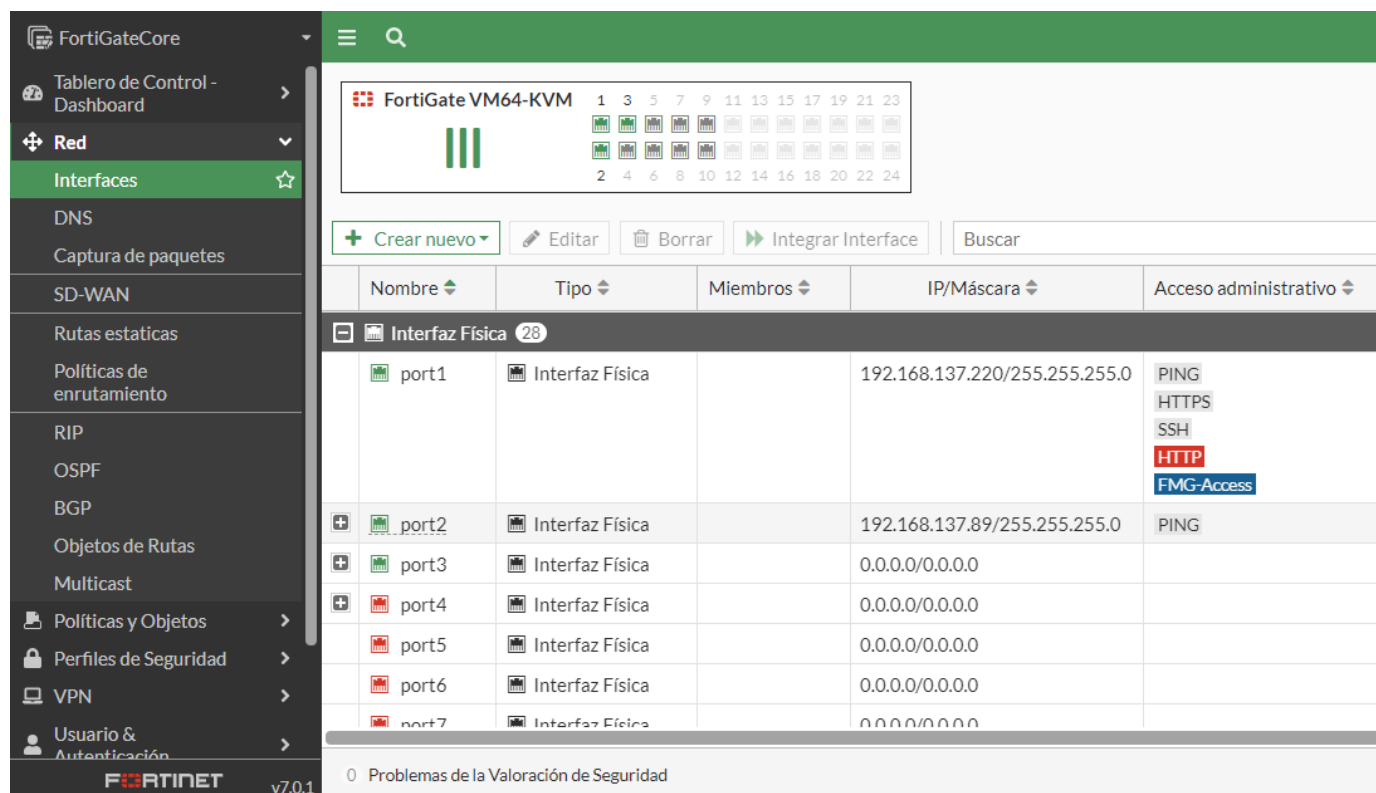
### CONFIGURACIÓN DE FIREWALL

En las siguientes secciones se detallará la configuración del firewall a implementar. En este caso decidimos implementar como mencionamos anteriormente equipos de la marca Fortinet ya que son reconocidos a nivel mundial y tienen herramientas muy potentes que nos facilitan el trabajo además de ser muy fáciles de configurar.

Por defecto los firewalls fortigate tienen dentro la configuración del puerto 1 como puerto de administración, como buena practica decidimos dejar ese puerto como el de administración que solo podrá ser accedido por los administradores del firewall.



Para la salida a internet de la LAN se configuro el puerto 2 del firewall.



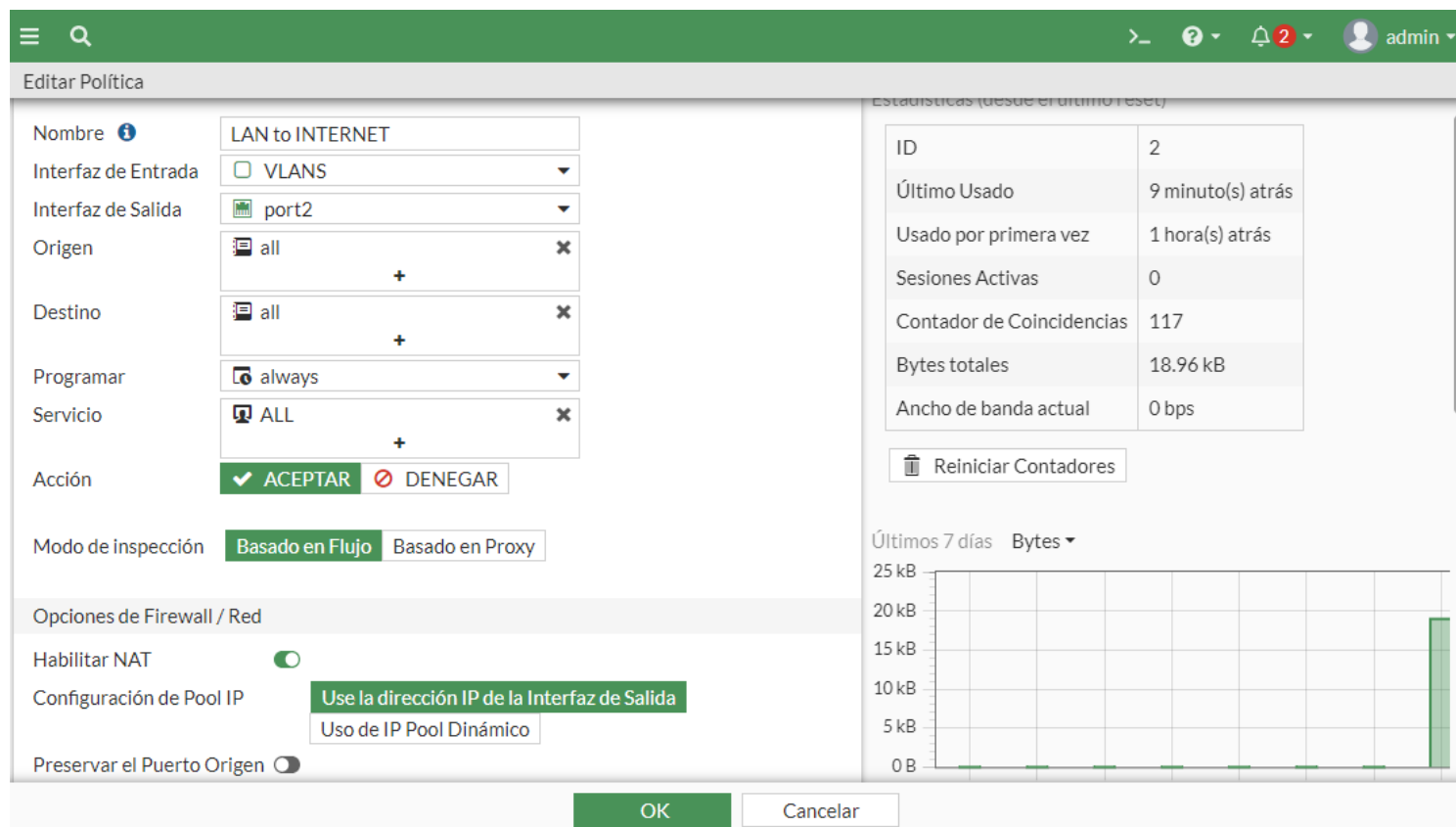
Nombre	Tipo	Miembros	IP/Máscara	Acceso administrativo
port1	Interfaz Física		192.168.137.220/255.255.255.0	PING, HTTPS, SSH, HTTP, FMG-Access
port2	Interfaz Física		192.168.137.89/255.255.255.0	PING
port3	Interfaz Física		0.0.0.0/0.0.0.0	
port4	Interfaz Física		0.0.0.0/0.0.0.0	
port5	Interfaz Física		0.0.0.0/0.0.0.0	
port6	Interfaz Física		0.0.0.0/0.0.0.0	
port7	Interfaz Física		0.0.0.0/0.0.0.0	

Para segmentar la red dentro del firewall se configuraron Vlans en el puerto 3, estas Vlans y su direccionamiento fueron consideradas de la tabla de direccionamiento de la pagina 5, cada una de estas Vlans cuentan dentro de su configuración con servidores DHCP facilitándonos así la configuración de direccionamiento de cada equipo dentro del edificio e instalaciones alrededor. En las Vlans que pertenecen a los servidores no se implementara DHCP, se configura manualmente el direccionamiento estático de los servidores.

En la siguiente imagen se detalla la implementación de lo nombrado anteriormente.

•	ADMINISTRATIVO (VLAN200)	VLAN		192.168.100.1/255.255.254.0	PING
•	CONTADURIA (VLAN140)	VLAN		192.168.40.1/255.255.254.0	PING
•	DTI (190)	VLAN		192.168.90.1/255.255.254.0	PING
•	IoT (VLAN210)	VLAN		192.168.110.1/255.255.252.0	PING
•	LOGISTICA (VLAN160)	VLAN		192.168.60.1/255.255.254.0	PING
•	RRHH (VLAN 130)	VLAN		192.168.30.1/255.255.254.0	PING
•	SANIDAD (VLAN150)	VLAN		192.168.50.1/255.255.254.0	PING
•	SEGURIDAD (VLAN170)	VLAN		192.168.70.1/255.255.254.0	PING
•	SERVIDORES (VLAN110)	VLAN		192.168.10.1/255.255.255.0	PING
•	TELEFONIA IP (VLAN180)	VLAN		192.168.80.1/255.255.254.0	PING

Para darle salida a Internet a la LAN se configuro una política con NAT habilitado, esta política hace que todo equipo que quiera salir a internet lo haga por el Puerto 2 del firewall. Para no hacer una política por cada VLAN, el firewall nos proporciona la creación de una zona, esta zona la nombramos VLANS y dentro de ella contiene las VLANS a las que les daremos acceso a internet.



**Editar Política**

Nombre: LAN to INTERNET

Interfaz de Entrada: VLANS

Interfaz de Salida: port2

Origen: all

Destino: all

Programar: always

Servicio: ALL

Acción: ☒ ACEPTAR ☐ DENEGAR

Modo de inspección: ☒ Basado en Flujo ☐ Basado en Proxy

Opciones de Firewall / Red

Habilitar NAT: ☒

Configuración de Pool IP: ☒ Use la dirección IP de la Interfaz de Salida ☐ Uso de IP Pool Dinámico

Preservar el Puerto Origen: ☐

Estadísticas (desde el último reset)

ID	2
Último Usado	9 minuto(s) atrás
Usado por primera vez	1 hora(s) atrás
Sesiones Activas	0
Contador de Coincidencias	117
Bytes totales	18.96 kB
Ancho de banda actual	0 bps

Reiniciar Contadores

Últimos 7 días Bytes

25 kB

20 kB

15 kB

10 kB

5 kB

0 B

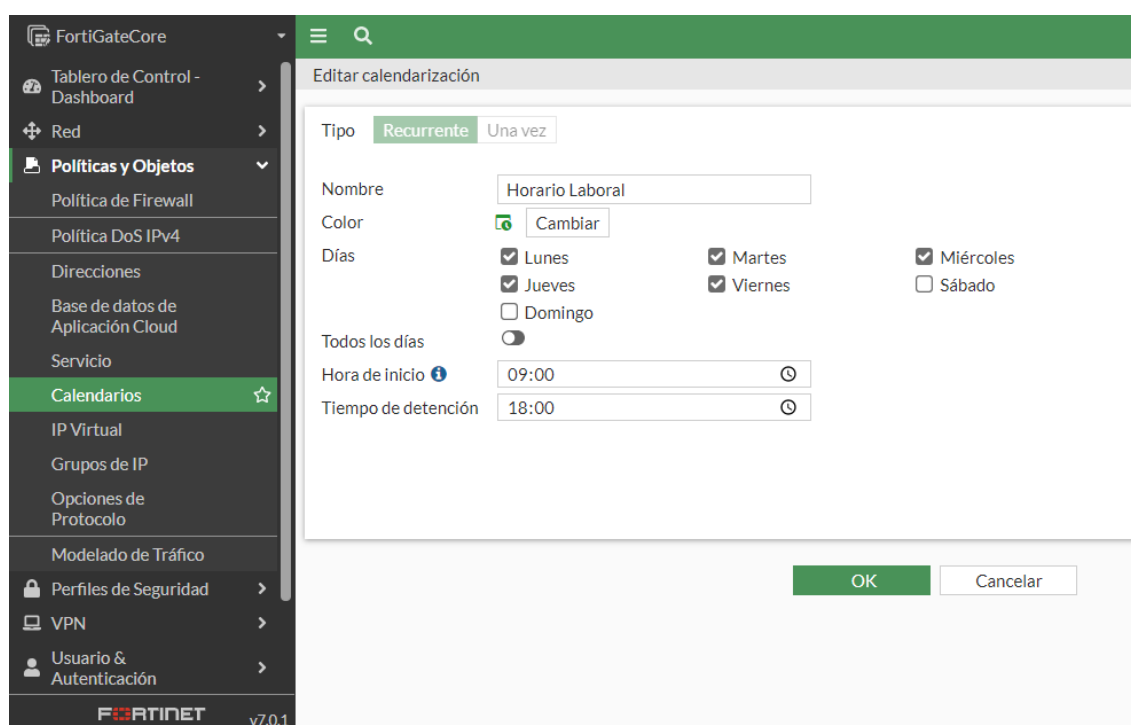
OK Cancelar

Para el filtrado de consultas DNS o sitios potencialmente peligrosos se configuro en el firewall un perfil de Web Filter, que nos proporciona mediante la base de datos de FortiGuard de Fortinet un listado de sitios web potencialmente peligrosos y nosotros poder habilitar o deshabilitar el acceso a esos sitios. FortiGuard viene integrado como un servicio en la licencia de Fortinet y es una herramienta que nos facilita enormemente el filtrado de sitios al que le queremos dar acceso o no a los usuarios de la LAN. También se configuro un perfil de antivirus para que el firewall analice cada archivo o paquete que pasa por el ayudándonos a prevenir que la red o los equipos se infecten con virus o malwares provenientes de internet.



Nombre		Comentarios
WEB	default	Default web filtering.
WEB	monitor-all	Monitor and log all visited URLs, flow-based.
WEB	Sitios bloqueados	
WEB	wifi-default	Default configuration for offloading WiFi traffic.

Para ayudar al Active Directory con el horario de acceso a los equipos del dominio, el firewall nos proporciona una herramienta que controla el acceso a internet a los equipos de la red, esto nos ayuda a que podamos configurar una hora de inicio y hora fin para que los equipos tengan acceso a internet, pasada esa hora estipulada el firewall bloqueara cualquier intento de conexión a internet fuera de ese horario, esta configuración se debe aplicar a la una política de salida a internet. En nuestro caso configuramos un horario de 9:00 a.m a 18:00 p.m.



También dentro del firewall configuramos algunas políticas para bloquear cierto tráfico dentro de la LAN misma, decidimos bloquear el tráfico de la VLAN de wifi de invitados a la VLAN de servidores que consideramos que no es importante que los invitados puedan acceder a los recursos de los servidores, también bloqueamos el tráfico de wifi invitados a las oficinas ya que tampoco es relevante que los invitados puedan conectarse con los equipos provenientes de las oficinas.

A continuación, detallamos las políticas implementadas dentro de la LAN

Como mencionamos anteriormente decidimos bloquear el tráfico de la VLAN 230 de wifi Invitados hacia la VLAN 110 de los servidores y viceversa.

Editar Política

Nombre	Wifi Invitados to Servers	
Interfaz de Entrada	<input type="checkbox"/> VLANS	
Interfaz de Salida	<input type="checkbox"/> VLANS	
Origen	<div>  VLAN230 address </div> <div>+</div>	
Destino	<div>  VLAN110 address </div> <div>+</div>	
Programar	<input checked="" type="checkbox"/> always	
Servicio	<div>  ALL </div> <div>+</div>	
Acción	<input checked="" type="checkbox"/> ACEPTAR <input checked="" type="checkbox"/> DENEGAR	

Nombre	servers to wifi	
Interfaz de Entrada	<input type="checkbox"/> VLANS	
Interfaz de Salida	<input type="checkbox"/> VLANS	
Origen	<div>  VLAN110 address </div> <div>+</div>	
Destino	<div>  VLAN230 address </div> <div>+</div>	
Programar	<input checked="" type="checkbox"/> always	
Servicio	<div>  ALL </div> <div>+</div>	
Acción	<input checked="" type="checkbox"/> ACEPTAR <input checked="" type="checkbox"/> DENEGAR	

☐ Registros de violación de Tráfico

Comentarios  0/1023

La siguiente política es la que bloquea el tráfico de la VLAN 230 de Wifi Invitados hacia las oficinas y viceversa.

wifi to oficinas	VLAN230 address	VLAN 120 address VLAN 130 address VLAN140 address VLAN150 address VLAN160 address VLAN170 address VLAN180 address VLAN200 address VLAN210 address	always	ALL	DENEGAR
------------------	-----------------	---	--------	-----	---------

## POLITICAS DE DoS EN EL FIREWALL

Los firewalls fortigate nos proporcionan entre tantas de sus configuraciones políticas de DoS, estas políticas nos ofrecen la posibilidad de bloquear el escaneo de diferentes puertos y protocolos desde Internet, es decir mediante la implementación de estas políticas le decimos al firewall que no permita que un host proveniente de Internet haga escaneos de puertos tratando de encontrar alguna puerta abierta para intentar vulnerar nuestro firewall o la red. Estas políticas prohíben tanto el escaneo de protocolos tcp como udp e icmp estos escaneos se utilizan para una gran cantidad de ataques, que comprometen la seguridad de nuestros dispositivos y redes. Para aprovechar esta funcionalidad que nos proporciona el Firewall, creamos dos políticas de DoS, una de ellas es para bloquear el escaneo de puertos desde internet y la otra es bloquear el escaneo de puertos dentro de la LAN. A continuación, detallamos el detalle de las configuraciones de las políticas implementadas.

En la siguiente imagen detallamos la política DoS que bloquea el escaneo desde internet.

Nombre ⓘ
Interfaz de Entrada
Dirección origen
Dirección Destino
Servicio

DoS Internet
port2
all
all
ALL

+
+
+


✕
✕
✕

Anomalías L3

Nombre	Bitácoras	Acción			Umbral
		Deshabilitar	Bloquear	Monitor	
ip_src_session	<input type="checkbox"/>	Deshabilitar	Bloquear	Monitor	5000
ip_dst_session	<input type="checkbox"/>	Deshabilitar	Bloquear	Monitor	5000

tcp_syn_flood	<input type="checkbox"/>	<a href="#">Deshabilitar</a> <a href="#">Bloquear</a> <a href="#">Monitor</a>	<input type="text" value="200"/>
tcp_port_scan	<input type="checkbox"/>	<a href="#">Deshabilitar</a> <a href="#">Bloquear</a> <a href="#">Monitor</a>	<input type="text" value="10"/>
tcp_src_session	<input type="checkbox"/>	<a href="#">Deshabilitar</a> <a href="#">Bloquear</a> <a href="#">Monitor</a>	<input type="text" value="5000"/>
tcp_dst_session	<input type="checkbox"/>	<a href="#">Deshabilitar</a> <a href="#">Bloquear</a> <a href="#">Monitor</a>	<input type="text" value="5000"/>
udp_flood	<input type="checkbox"/>	<a href="#">Deshabilitar</a> <a href="#">Bloquear</a> <a href="#">Monitor</a>	<input type="text" value="100"/>
udp_scan	<input type="checkbox"/>	<a href="#">Deshabilitar</a> <a href="#">Bloquear</a> <a href="#">Monitor</a>	<input type="text" value="50"/>
udp_src_session	<input type="checkbox"/>	<a href="#">Deshabilitar</a> <a href="#">Bloquear</a> <a href="#">Monitor</a>	<input type="text" value="5000"/>
udp_dst_session	<input type="checkbox"/>	<a href="#">Deshabilitar</a> <a href="#">Bloquear</a> <a href="#">Monitor</a>	<input type="text" value="5000"/>
icmp_flood	<input type="checkbox"/>	<a href="#">Deshabilitar</a> <a href="#">Bloquear</a> <a href="#">Monitor</a>	<input type="text" value="50"/>
icmp_sweep	<input type="checkbox"/>	<a href="#">Deshabilitar</a> <a href="#">Bloquear</a> <a href="#">Monitor</a>	<input type="text" value="100"/>

En la siguiente imagen detallamos la política que bloquea el escaneo dentro de la LAN

Nombre 

Interfaz de Entrada

Dirección origen

Dirección Destino

Servicio

DoS

VLANS

all

all

ALL

Anomalías L3

Nombre	<input type="checkbox"/>	Acción			Umbral
		Deshabilitar	Bloquear	Monitor	
ip_src_session	<input type="checkbox"/>	<a href="#">Deshabilitar</a>	<a href="#">Bloquear</a>	<a href="#">Monitor</a>	<input type="text" value="5000"/>
ip_dst_session	<input type="checkbox"/>	<a href="#">Deshabilitar</a>	<a href="#">Bloquear</a>	<a href="#">Monitor</a>	<input type="text" value="5000"/>

Anomalías L4

OK

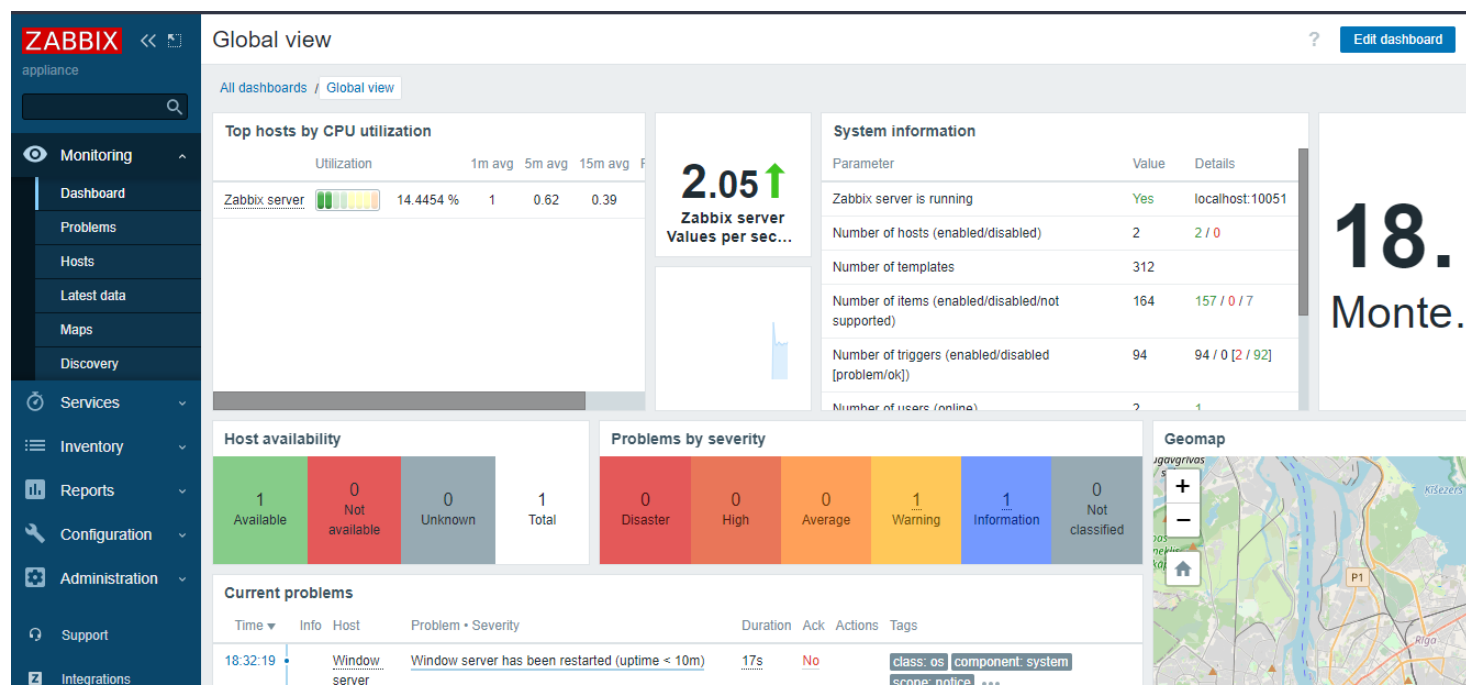
Cancelar

## DETALLE DE SISTEMAS DE AUDITORIA Y MONITOREO

Para el monitoreo de los servidores y dispositivos de la red se decidió implementar un servidor Zabbix, ya que nos ofrece la posibilidad de monitorear el rendimiento y la disponibilidad de los servidores, equipos, aplicaciones y bases de datos. En este paso el objetivo es anticipar lo que está pasando, ver cómo está trabajando la red tanto a nivel interno de las diferentes áreas, así como a nivel externo, además ver si hay equipos de nuestra organización que no estén trabajando de manera anormal (PC, Router, Switches, etc). Así podremos de forma centralizada monitorear nuestra red a través del administrador web que Zabbix nos ofrece, además entre sus ventajas están que es compatible con diferentes sistemas operativos, nos proporciona reportes en tiempo real a través de gráficas, datos y alertas visuales que muestran el estado y rendimiento de los servicios y equipos monitoreados, mapas de la red de nuestra arquitectura. Para esto se configuró en el Windows Server un rol de acceso remoto el cual le habilitamos por medio del Firewall el servicio SNMP (Protocolo Simple de Administración de red) es un protocolo de capa superior o aplicación que permite agilizar el intercambio de información de administración entre dispositivos de red. Por ejemplo, en un switch uno puede habilitar este protocolo que responda evento de SNMP, y todos lo que suceda dentro del switch ya sea eventos de información, alertas, errores, los administradores pueden supervisar el funcionamiento de la red, buscar y resolver los inconvenientes que suceden en la red.

Se decidió monitorear los servidores de Base de datos, el controlador de dominio y los firewalls, ya que para nosotros son de carácter crítico para el negocio y necesitan ser monitoreados continuamente para detectar cualquier irregularidad en su funcionamiento.

A continuación, se detallará la configuración e implementación de Zabbix.



Se configuró el controlador de dominio para esto se habilitó el servicio SNMP y se configuró una comunidad dentro del servidor, la cual la nombramos TheBoys.com, de esta forma Zabbix podrá con permisos de solo lectura hacerle consultas al servidor Windows. Se configuró en Zabbix un nuevo Host el cual lo nombramos Windows Server, mediante los



Templates que nos proporciona Zabbix elegimos que recursos del hardware y software le queremos consultar al Servidor Windows para su monitoreo. Luego colocamos la Ip del servidor a monitorear y el puerto que por defecto es el 161  
A continuación, se detallan las configuraciones hechas.

Host

Host

IPMI

Tags

Macros 1

Inventory

Encryption

Value mapping

\* Host name

Window server

Visible name

Window server

Templates

Name

Action

ICMP Ping

[Unlink](#) [Unlink and clear](#)

Windows SNMP

[Unlink](#) [Unlink and clear](#)

type here to search

Select

\* Host groups

WINDOW SERVER x

type here to search

Select

Interfaces

Type

IP address

DNS name

Connect to

Port

Default

SNMP

192.168.1.54

IP

DNS

161

☒ Remove

Add

Description

Update

Clone

Full clone

Delete

Cancel

Host

Host

IPMI

Tags

Macros 1

Inventory

Encryption

Value mapping

Host macros

Inherited and host macros

Macro

Value

{SNMP\_COMMUNITY}

TheBoys.com

T v

Add



Luego de hacer esas configuraciones podemos comprobar que ya estamos obteniendo datos del servidor a monitorear.

<input type="checkbox"/>	Host	Name ▲	Last check	Last value	Change	Tags	
<input type="checkbox"/>	Window server	C:\Label: Serial Number fc246e04: Space utilization ?	36s	61.5106 %		component: storage filesystem: C:\Label: ...	Graph
<input type="checkbox"/>	Window server	C:\Label: Serial Number fc246e04: Total space ?	51s	19.66 GB		component: storage filesystem: C:\Label: ...	Graph
<input type="checkbox"/>	Window server	C:\Label: Serial Number fc246e04: Used space ?	51s	12.09 GB		component: storage filesystem: C:\Label: ...	Graph
<input type="checkbox"/>	Window server	CPU utilization ?	51s	0 %		component: cpu	Graph
<input type="checkbox"/>	Window server	ICMP loss	51s	0 %		component: health component: network	Graph
<input type="checkbox"/>	Window server	ICMP loss	51s	0 %		component: health component: network	Graph
<input type="checkbox"/>	Window server	ICMP ping	51s	Up (1)		component: health component: network	Graph
<input type="checkbox"/>	Window server	ICMP ping	51s	Up (1)		component: health component: network	Graph
<input type="checkbox"/>	Window server	ICMP response time	51s	0.41ms	-0.043ms	component: health component: network	Graph
<input type="checkbox"/>	Window server	ICMP response time	51s	0.41ms	-0.043ms	component: health component: network	Graph
<input type="checkbox"/>	Window server	Interface ethernet_10(Ethernet): Bits received ?	1m 51s	224 bps		component: network description: Ethernet ...	Graph
<input type="checkbox"/>	Window server	Interface ethernet_10(Ethernet): Bits sent ?	1m 51s	296 bps		component: network description: Ethernet ...	Graph
<input type="checkbox"/>	Window server	Interface ethernet_10(Ethernet): Inbound packets dis... ?	1m 51s	0		component: network description: Ethernet ...	Graph
<input type="checkbox"/>	Window server	Interface ethernet_10(Ethernet): Inbound packets wit... ?				component: network description: Ethernet ...	Graph
<input type="checkbox"/>	Window server	Interface ethernet_10(Ethernet): Interface type ?				component: network description: Ethernet ...	Graph
<input type="checkbox"/>	Window server	Interface ethernet_10(Ethernet): Operational status ?	51s	up (1)		component: network description: Ethernet ...	Graph
<input type="checkbox"/>	Window server	Interface ethernet_10(Ethernet): Outbound packets d... ?				component: network description: Ethernet ...	Graph
<input type="checkbox"/>	Window server	Interface ethernet_10(Ethernet): Outbound packets ... ?				component: network description: Ethernet ...	Graph

## MONITOREO SERVIDOR DE BASE DE DATOS

A continuación, se detalla las configuraciones para el monitoreo del servidor de Base de Datos.

Host

Host

IPMI

Tags

Macros 1

Inventory

Encryption

Value mapping

\* Host name

Window server BD

Visible name

Window server BD

Templates

Name

ICMP Ping

Windows SNMP

type here to search

Action

Unlink Unlink and clear

Unlink Unlink and clear

Select

\* Host groups

WINDOW SERVER x

type here to search

Select

Interfaces

Type

IP address

DNS name

Connect to

Port

Default

SNMP

192.168.1.53

IP DNS

161

Remove

Add

Description

Update

Clone

Full clone



Luego de hacer esas configuraciones podemos comprobar que ya estamos obteniendo datos del servidor a monitorear.

<input type="checkbox"/>	Window server BD	Interface ethernet_10(Ethernet): Interface type ?	47s	ethernetCsmacd (6)	component: network	description: Ethernet ...	Graph
<input type="checkbox"/>	Window server BD	Interface ethernet_10(Ethernet): Operational status ?	47s	up (1)	component: network	description: Ethernet ...	Graph
<input type="checkbox"/>	Window server BD	Interface ethernet_10(Ethernet): Outbound packets d... ?			component: network	description: Ethernet ...	Graph
<input type="checkbox"/>	Window server BD	Interface ethernet_10(Ethernet): Outbound packets ... ?			component: network	description: Ethernet ...	Graph
<input type="checkbox"/>	Window server BD	Interface ethernet_10(Ethernet): Speed ?	47s	1 Gbps	component: network	description: Ethernet ...	Graph
<input type="checkbox"/>	Window server BD	Physical Memory: Memory utilization ?	42s	40.7461 %	component: memory		Graph
<input type="checkbox"/>	Window server BD	Physical Memory: Total memory ?	47s	1.8 GB	component: memory		Graph
<input type="checkbox"/>	Window server BD	Physical Memory: Used memory ?	47s	751.56 MB	component: memory		Graph
<input type="checkbox"/>	Window server BD	SNMP agent availability ?	6s	available (1)	component: health	component: network	Graph
<input type="checkbox"/>	Window server BD	SNMP traps (fallback) ?			component: network		History
<input type="checkbox"/>	Window server BD	System contact details ?	1m 47s		component: system		History
<input type="checkbox"/>	Window server BD	System description ?	1m 47s	Hardware: Intel64...	component: system		History
<input type="checkbox"/>	Window server BD	System location ?	1m 47s		component: system		History
<input type="checkbox"/>	Window server BD	System name ?	1m 47s	WIN-SERV-BD.Th...	component: system		History
<input type="checkbox"/>	Window server BD	System object ID ?	1m 47s	SNMPv2-SMI::ent...	component: system		History
<input type="checkbox"/>	Window server BD	Uptime (hardware) ?	17s	00:40:43 +00:00:30	component: system		Graph
<input type="checkbox"/>	Window server BD	Uptime (network) ?	17s	00:36:25 +00:00:30	component: system		Graph

## MONITOREO DE FIREWALL

A continuación, se detalla las configuraciones para el monitoreo del firewall, para esto tuvimos que configurar una comunidad en el firewall y dentro de la VLAN de servidores que es la 110 habilitar el acceso mediante SNMP.

Tipo

Interfaz

port3

VLAN ID

110

Editar

VRF ID

0

Rol

LAN

Dirección

Modo de direccionamiento

Manual

DHCP

FortiIPAM Auto-administrado

IP/Máscara

192.168.10.1/255.255.255.0

Crear objeto de direccionamiento para subred

Nombre

VLAN110 address

Destino

192.168.10.1/255.255.255.0

Dirección IP secundaria

Acceso administrativo

IPv4

☐ Prueba de Velocidad

☐ HTTPS

☒ PING

☐ FMG-Access

☐ SSH

☒ SNMP

☐ FTM

☐ Contabilidad de RADIUS

☐ Conexión de Security Fabric



FortiGateCore

Tablero de Control - Dashboard

Red

Políticas y Objetos

Perfiles de Seguridad

VPN

Usuario & Autenticación

Sistema 1

Administradores

Perfil de Acceso

Firmware

Configuraciones

HA

SNMP

Mensajes de Reemplazo

FortiGuard 1

Visibilidad de Característica

Fortinet

v7.0.1

SNMP

Descargar Archivo FortiGate MIB

Descargar Archivo de MIB Fortinet Core

Información de sistema

Agente SNMP

Descripción

Monitoreo

Ubicación

DC

Información de Contacto

Administrador

SNMP v1/v2c

+ Crear nuevo

Editar

Borrar

Estatus

Nombre	Consultas	Traps	Hosts	Eventos	Estado
fortigate.com	<div>v1 Habilitar</div> <div>v2 Habilitar</div>	<div>v1 Habilitar</div> <div>v2 Habilitar</div>	192.168.10.2/24	36	<div>Habilitar</div>

0 Problemas de la Valoración de Seguridad

1

Aplicar

En Zabbix agregamos las configuraciones para poder monitorear al firewall

Host

Host

IPMI

Tags

Macros 1

Inventory

Encryption

Value mapping

\* Host name

FortigateCore

Visible name

FortigateCore

Templates

Name

ICMP Ping

type here to search

Select

Action

Unlink Unlink and clear

\* Host groups

Virtual machines

type here to search

Select

Interfaces

Type

IP address

DNS name

Connect to

Port

Default

Update

Clone

Full clone

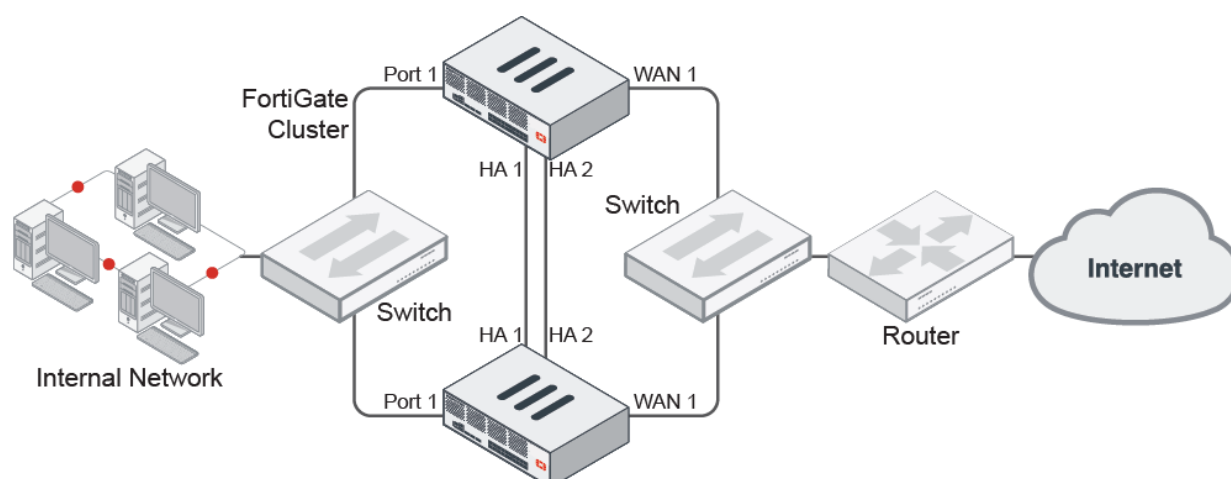
Delete

Cancel

<input type="checkbox"/>	FortigateCore	ICMP response time	29s	3.63ms	+0.48ms	component: health	component: network
<input type="checkbox"/>	FortigateCore	Interrupts per second				component: cpu	
<input type="checkbox"/>	FortigateCore	Load average (1m avg) ?				component: cpu	
<input type="checkbox"/>	FortigateCore	Load average (5m avg) ?				component: cpu	
<input type="checkbox"/>	FortigateCore	Load average (15m avg) ?				component: cpu	
<input type="checkbox"/>	FortigateCore	Number of CPUs ?	29s	0		component: cpu	
<input type="checkbox"/>	FortigateCore	SNMP agent availability ?	35s	available (1)		component: health	component: network
<input type="checkbox"/>	FortigateCore	SNMP traps (fallback) ?				component: network	
<input type="checkbox"/>	FortigateCore	System contact details ?	1m 29s	Administrador		component: system	
<input type="checkbox"/>	FortigateCore	System description ?	1m 29s	Monitoreo		component: system	
<input type="checkbox"/>	FortigateCore	System location ?				component: system	
<input type="checkbox"/>	FortigateCore	System name ?	1m 29s	FortiGateCore		component: system	
<input type="checkbox"/>	FortigateCore	System object ID ?	1m 29s	SNMPv2-SMI::ent...		component: system	
<input type="checkbox"/>	FortigateCore	Uptime (hardware) ?	29s	00:00:00		component: system	
<input type="checkbox"/>	FortigateCore	Uptime (network) ?	1m 29s	02:20:32		component: system	

## HA EN EQUIPOS FORTIGATE

Para garantizar la alta disponibilidad de los firewalls que vamos a implementar se decidió implementar HA en estos dispositivos para garantizarnos de que si existen fallas físicas o de software en estos equipos que son de carácter importante en nuestra red para poder comunicar las diferentes áreas y poder proteger a toda la red de las amenazas existentes en las redes, dentro de los firewall Fortigate que implementamos configuramos el servicio HA Activo-Pasivo que estos nos tipos de Firewall brindan de esta forma estos dos firewall Core que vamos a usar van a esta sincronizados uno con el otro escuchando y replicando las configuraciones o modificaciones que estos tengan y que los dos funcionen como un espejo, de esta forma si uno de estos firewall se cae va a ser casi imperceptible para los usuarios y equipos de la red porque rápidamente uno de estos dos Firewall Core seguirá funcionando como si se estuviese implementando un firewall solo.



A continuación, detallamos las configuraciones realizadas para garantizar la alta disponibilidad en estos equipos.

Para las configuraciones habilitamos el modo Activo-Pasivo y un nombre de grupo, este nombre de grupo es el que deben utilizar todos los firewalls que se quieran unir al clúster, es importante que el nombre y la contraseña sea la misma de otro modo no se podrá unir un firewall a un clúster, también debemos considerar que para configurar un cluster en Forti es necesario que todos los firewall utilicen los mismos puertos de conexión, en nuestro caso el puerto 1 pertenece a la administración del firewall, el puerto 2 a la salida hacia internet y el puerto 3 es el que conecta a la LAN.

Esta imagen representa las configuraciones del Firewall Core

Alta Disponibilidad

Modo: Activo-Pasivo

Prioridad de Dispositivo: 130

Configuración de Cluster

Nombre de grupo: FGT

Contraseña: ..... Cambiar

Retomar Sesión: ☐

Supervisar interfaces: port3

Interfaces de Heartbeat: port4

☒ Reserva de Interfaz de Administración

Interfaz: port1

Enlace: 0.0.0.0

Subred destino: 192.168.137.0 255.255.255.0

OK Cancelar

En la siguiente imagen representamos la configuración del Firewall que funciona como replica

Alta Disponibilidad

Modo

Activo-Pasivo

Prioridad de Dispositivo ⓘ

128

Configuración de Cluster

Nombre de grupo

FGT

Contraseña

••••••••

Cambiar

Retomar Sesión

☐

Supervisar interfaces

port3

+

×

Interfaces de Heartbeat

port4

+

×

☒ Reserva de Interfaz de Administración

Interfaz

port1

Enlace

0.0.0.0

Subred destino

0.0.0.0/0

+

OK

Cancelar

Después de finalizar las configuraciones en los dos Firewall procedemos a verificar que los dos estén sincronizados y que ya se hayan replicado las configuraciones en el Firewall de replica

FortiGate VM64-KVM

1 3 5 7 9 11 13 15 17 19 21 23

2 4 6 8 10 12 14 16 18 20 22 24

FortiGateCore (Primario)

Actualizar

Editar

✕ Quitar equipo del clúster Alta-Disponibilidad

Estatus	Prioridad	Nombre de Host	No. de serie	Rol	System Uptime	Sesión(es)	Rendimiento
✓ Sincronizado	130	FortiGateCore	FGVMEVG83RO4CE7F	Primario	1h 29m	70	109.00 kbps
✓ Sincronizado	128	FortigateCore2	FGVMEVP8G8R1Z17A	Secundario	18m 14s	44	49.00 kbps



FortiGateCore2

Tablero de Control - Dashboard

Red

Interfaces

DNS

Captura de paquetes

SD-WAN

Rutas estaticas

Políticas de enrutamiento

RIP

OSPF

BGP

Objetos de Rutas

Multicast

Políticas y Objetos

Perfiles de Seguridad

VPN

Usuario & Autenticación

FortiGate VM64-KVM

1 3 5 7 9 11 13 15 17 19 21 23

2 4 6 8 10 12 14 16 18 20 22 24

+ Crear nuevo

Editar

Borrar

Integrar Interface

Buscar

Nombre	Tipo	Miembros	IP/Máscara	Acceso administra
port1	Interfaz Física		192.168.137.23/255.255.255.0	HTTP
port2	Interfaz Física		192.168.137.145/255.255.255.0	PING
port3	Interfaz Física		192.168.240.15/255.255.255.0	PING
ADMINISTRATIVO (VLAN200)	VLAN		192.168.100.1/255.255.254.0	PING
CONTADURIA (VLAN140)	VLAN		192.168.40.1/255.255.254.0	PING
DTI (190)	VLAN		192.168.90.1/255.255.254.0	PING
IoT (VLAN210)	VLAN		192.168.110.1/255.255.252.0	PING
LOGISTICA (VLAN160)	VLAN		192.168.60.1/255.255.254.0	PING
RRHH (VLAN 130)	VLAN		192.168.30.1/255.255.254.0	PING

0 Problemas de la Valoración de Seguridad 20% 31 Actualizar

+ Crear nuevo

Editar

Borrar

Búsqueda de política

Buscar

Vista de pareja de inter

Nombre	Origen	Destino	Calendario	Servicio	Acción	NAT
+ SSL-VPN tunnel interface (ssl.root) → port3 1						
+ VLANS → port2 1						
+ VLANS → VLANS 4						
Wifi Invitados to Servers	VLAN230 address	VLAN110 address	always	ALL	DENEGAR	
Oficinas to servers	VLAN 120 address VLAN 130 address VLAN110 address VLAN140 address VLAN150 address VLAN160 address VLAN170 address VLAN180 address VLAN200 address VLAN210 address	VLAN110 address	always	ALL	ACEPTAR	Deshabilitado
servers to wifi	VLAN110 address	VLAN230 address	always	ALL	DENEGAR	
wifi to oficinas	VLAN230 address	VLAN 120 address VLAN 130 address	always	ALL	DENEGAR	

0 Problemas de la Valoración de Seguridad 0% 7 Actualizar

De esta forma tenemos la seguridad de que la red seguirá funcionando sin la necesidad de detener todos los servicios por alguna falla en alguno de los firewalls.

---

## AUDITORIA

Luego del monitoreo, se continúa con la auditoría, el objetivo de la misma es defender y proteger a nuestra organización o empresa. La auditoría se encarga de estudiar la red, los hosts más importantes con esto chequear que los enlaces que son más necesarios para la empresa no estén saturados, otro objetivo ligado a la auditoría es actuar frente a una amenaza que logró entrar y produjo un daño en nuestra empresa.

Podemos dividir la auditoría en tres partes:

- Física
- Lógica
- Sistemas

### Auditoría Física

En este aspecto es importante tener en cuenta qué servicios prestará la empresa y qué sistemas son considerados críticos para el negocio y sobre qué soportes físicos se encuentran, para controlar su correcto funcionamiento, temperatura adecuada, consumo de recursos, energía, control de humedad, estática, etc.

### Auditoría Lógica

Esta auditoría se encarga de verificar todo lo que son las aplicaciones críticas para la operativa tales como aplicaciones de escritorio en cada terminal, SQL Developer, web y móvil cumplan con todos los requerimientos, se controla la memoria que estás consumen y si están dentro de los parámetros de funcionamiento normal, sobre todo se busca que no presenten fallas a la hora de guardar un registro.

### Auditoría de Sistemas

La auditoría de sistemas se encarga de análisis de zonas y equipos. En este aspecto se deberá contemplar el consumo de recursos de los principales sistemas de la organización y el comportamiento de uso frente a otros recursos. Para el monitoreo de recursos, redes e infraestructura en general se utilizarán algunas herramientas de auditoría que permitirán recopilar información para su posterior análisis y toma de decisiones.

## HERRAMIENTAS PARA LA AUDITORIA DE REDES

**Nmap:** Nmap es una herramienta multiplataforma basada en software libre que permite hacer escaneos y auditorías de redes. El funcionamiento conceptual es bastante sencillo, funciona enviando una serie de paquetes predefinidos a un rango de direcciones IP para comprobar los puertos abiertos y tras analizar la respuesta proporcionada por cada equipo describir los servicios que se prestan en cada uno de ellos.

Entre las funcionalidades que presta, informa sobre si una IP está disponible, que sistema operativo ejecuta, que puertos tiene abiertos y que servicios presta. Esta herramienta es de

gran utilidad para comprobar que superficie de ataque tiene expuesta una máquina por lo que puede ser utilizada como auditoría de seguridad.

Cabe recordar, que sabiendo el sistema operativo que se está ejecutando y si un puerto está a la escucha, se puede buscar vulnerabilidades en bases de conocimiento para poder explotarlos posteriormente por lo que también es utilizada por los atacantes durante las fases de preparación del ataque.

**WireShark:** es una de las herramientas más conocidas y usadas dentro del mundo de la seguridad de redes. Es un analizador de protocolos que entre otras cosas se utiliza para saber cómo funcionan las comunicaciones y como se componen los paquetes TCP y UDP.

Esta herramienta, permite visualizar el tráfico de la red de la misma manera que lo hace “tcpdump”, pero eliminando complejidad al añadir un interfaz gráfico bastante simple.

Mediante la inspección del tráfico, que permite desencapsularlo y ver la estructura interna detalladamente, pudiendo llegar a gran nivel de detalle, por lo que ayuda a detectar problemas en comunicaciones de muy diverso origen.

**Kali Linux:** Kali Linux es una distribución de GNU/Linux diseñada para hacer pen-testing (test de penetración de sistemas) en sistemas y redes. No es una herramienta en sí, sino que es un compendio de ellas, de hecho, algunas herramientas de las que hemos hablado previamente están recogidas en esta distribución. Esta distribución GNU/Linux que puede ser auto arrancable, desde un CD o una memoria USB, o instalable. Contiene herramientas relacionadas con test de sistemas, de redes, etc. A pesar de ser una distribución GNU/Linux, arranca formato gráfico y la mayoría de las herramientas se pueden gestionar a través de interfaces gráficos sin grandes dificultades.

Entre las herramientas que podemos encontrar dentro de Kali Linux tenemos escáneres de puertos, herramientas para testear contraseñas, recolectores de información Web, analizadores de vulnerabilidades, inyectores de SQL, etc.

## CONSIDERACIÓN DE SERVICIOS

A continuación, en la siguiente tabla se mostrará las consideraciones de servicios implementadas en nuestra solución.

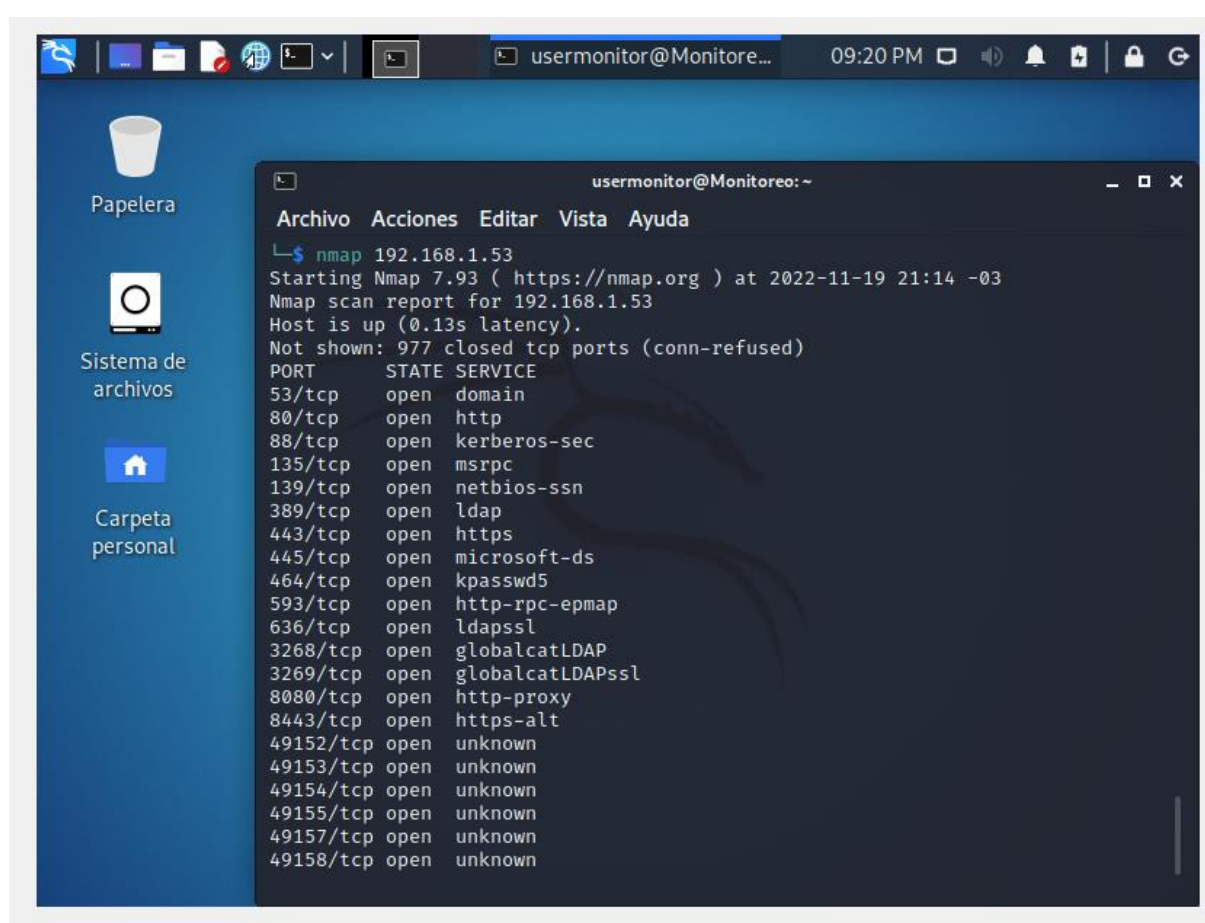
SERVIDOR	SERVICIO	IP SERVIDOR	PUERTO
Web	HTTP	192.168.10.7/23	80
	HTTPS		443
	Wildfly		8080
Base de Datos	Oracle XE	192.168.10.3	1521
Active Directory	Active Directory	192.168.10.7/23	389

Para un entorno de desarrollo ya que contemplamos que nuestra aplicación web y mobile seguirá avanzando en funcionalidades, decidimos implementar un entorno para los desarrolladores con un servidor de aplicaciones Wildfly y un servidor de base de datos Oracle en un mismo entorno, el servidor Wildfly en el puerto 8280 y la base de datos en el puerto 8080.

El resto de los puertos se hará un escaneo de los servidores utilizando una herramienta muy potente como es Kali Linux con el comando NMAP y la ip a la que queremos hacer un mapeo de puertos para ver los puertos mas vulnerados o potencialmente vulnerables y poder cerrarlos, uno de esos puertos va a ser el puerto 23 Telnet, el puerto 25 SMTP, 110 y 995 POP3.

A continuación, detallaremos el mapeo de puertos de los hosts que consideramos importantes mantenerlos lo más seguros posibles, para esto como mencionamos anteriormente se utilizó Kali Linux como herramienta.

Luego de la instalación y configuración de Kali Linux, se procedió a hacer un mapeo del servidor principal de controlador de dominio con el objetivo de verificar que puertos este host tiene habilitados.



Como vemos en la imagen el servidor tiene habilitados algunos puertos potencialmente vulnerables como el http 80/tcp que decidimos cerrarlo porque es un puerto que ya no se utiliza además de ser uno de los mas vulnerados en los últimos años, si dejaremos el puerto 443/tcp y el puerto 8080 que es donde el servidor de aplicaciones Wildfly funciona y el puerto 8180 que es el puerto para administrar el servidor Wildfly. Después tenemos puertos propios del Active Directory que decidimos dejarlos abiertos ya que sino de esta forma no funcionaria correctamente el servidor como son el puerto 389/tcp, el puerto 3268/tcp, puerto 3269/tcp



Lo siguiente que decidimos hacer un mapeo de puertos es del servidor de base de datos, es imprescindible que este servidor este lo mas seguro posible, ya que es critico para el negocio perder la información de la base de datos.

```
usermonitor@Monitoreo: ~  
Archivo Acciones Editar Vista Ayuda  
49157/tcp open unknown  
49158/tcp open unknown  
50000/tcp open ibm-db2  
50001/tcp open unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds  
  
(usermonitor@Monitoreo)-[~]  
$ nmap 192.168.1.54  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-19 21:46 -03  
Nmap scan report for 192.168.1.54  
Host is up (0.00044s latency).  
Not shown: 988 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
1521/tcp  open  oracle  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49157/tcp open  unknown  
49159/tcp open  unknown  
49161/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds  
  
(usermonitor@Monitoreo)-[~]  
$ ss
```

Como vemos en la imagen tenemos puertos que son de importancia para el funcionamiento del servidor además tenemos el puerto que escucha la base de datos como es el puerto 1521/tcp, esos puertos decidimos dejarlos abiertos.

A continuación, detallamos el mapeo de puertos del servidor de active directory que utilizamos como replica para el servidor de active directory principal

```
(usermonitor@Monitoreo)-[~]
$ nmap 192.168.1.58
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-19 21:57 -03
Nmap scan report for 192.168.1.58
Host is up (0.00037s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown

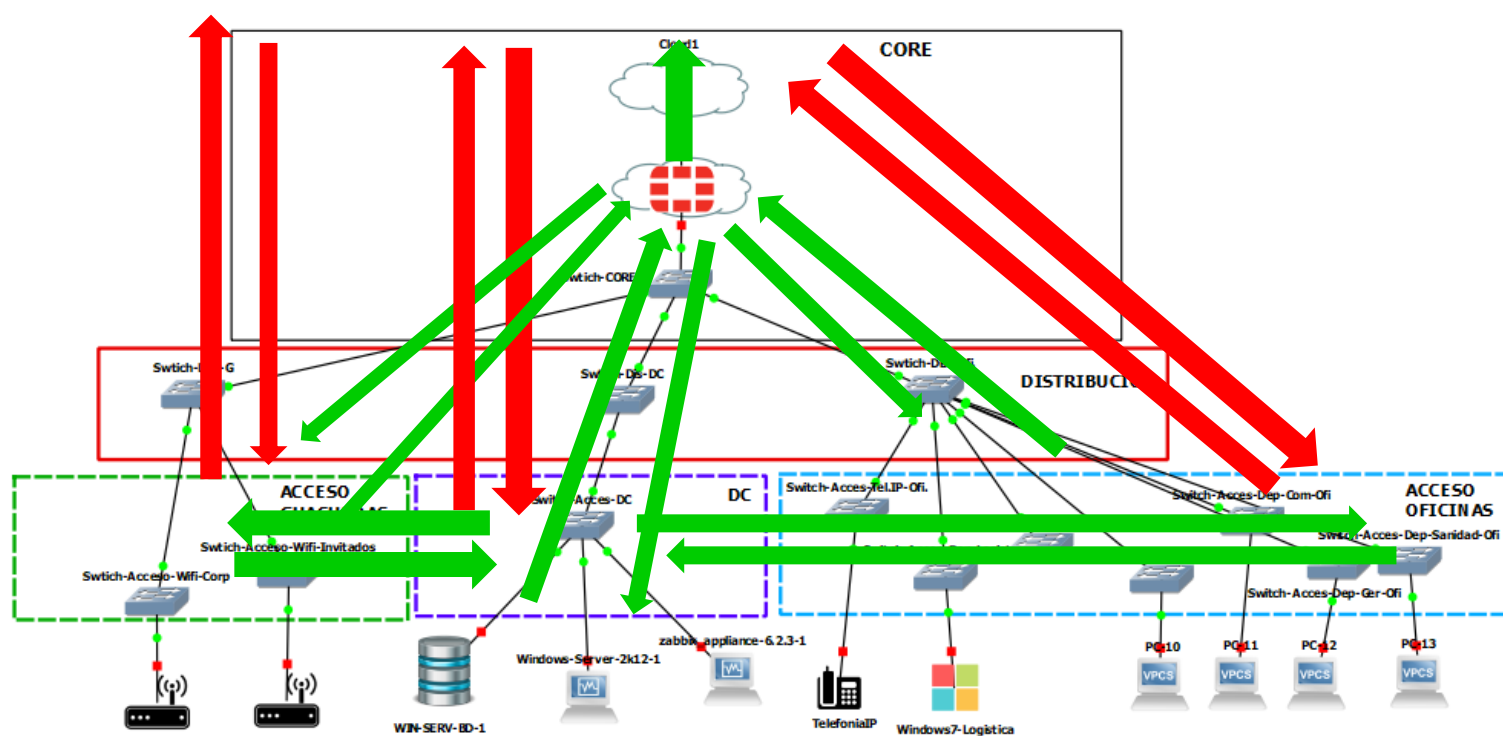
Nmap done: 1 IP address (1 host up) scanned in 2.06 seconds

(usermonitor@Monitoreo)-[~]
$
```

Como vemos los puertos utilizados por este servidor son los mismos que utiliza el servidor principal ya que este funcionara como contingencia en caso de que el servidor principal tenga una falla o este temporalmente inactivo. En este servidor también mantenemos a los puertos que son importantes para el funcionamiento del servidor y cerramos el puerto 80/tcp ya que no es recomendable utilizarlo.

## DIAGRAMA DE FLUJO

A continuación, se detalla el diagrama de flujo de tráfico permitido y no permitido.



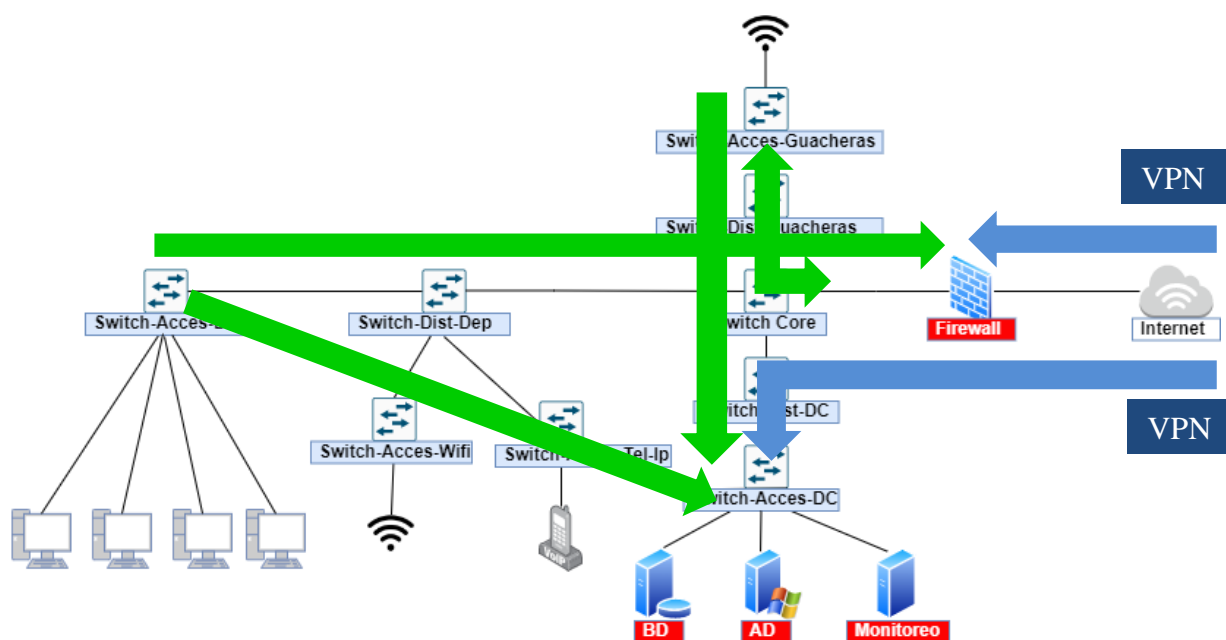
**PERMITIDO**  
**NO PERMITIDO**



## CHECKLIST DE FUNCIONAMIENTO Y TESTEO COMPLETO

A continuación, en la siguiente tabla se tiene como objetivo representar el listado de servicios necesarios para garantizarnos que el sistema está funcionando correctamente.

SERVICIO	FUNCIONAMIENTO	VERIFICACION
Firewall	Dar salida a internet a dispositivos de la LAN	Ping desde un equipo perteneciente a la LAN a Google.com ó 8.8.8.8
Firewall	Segmentación de VLANS para ver cómo están divididas y no se comunican	Ping desde un equipo perteneciente al departamento de Logística hacia el departamento Comercial
Active Directory	Añadir pc cliente al dominio TheBoys.com	En el pc cliente del departamento de Logística ingresar las credenciales para poder unirse al dominio
Active Directory	El controlador de dominio se encuentra ejecutándose	Ejecutar el comando nslookup desde la consola
Active Directory	Aplicar política GPO de papel tapiz a equipo cliente	Ingresar con las credenciales otorgadas por el AD en la pc cliente y verificar el cambio de fondo de pantalla mediante GPO
Usuarios aplicación web/mobile	El usuario esta creado dentro del AD y tiene permisos para loguearse al sistema	Ingresar al login de la aplicación web/mobile y colocar las credenciales asignadas desde el AD
Base de Datos	Base de datos Oracle iniciada en el servidor como servicio	Acceder desde la web a <a href="http://IpServer:8080/apex">http://IpServer:8080/apex</a>
Wildfly	Wildfly ejecutándose como servicio en el servidor	Acceder desde la web a <a href="http://IpServer:8080/">http://IpServer:8080/</a>  Resultado: Pagina de inicio del servidor Wildfly



## RDP

Para el acceso remoto y gestión de los servidores y dispositivos de la red se optó por crear una VPN SSL CLIENT en el firewall Fortigate de esta forma y de manera segura los administradores de la red podrán desde cualquier lugar remotamente poder administrar los servidores y dispositivos sin la necesidad de trasladarse a la estación de trabajo, para esto se configuró un direccionamiento ip específicamente para la VPN donde los administradores desde su IP publica y con las credenciales otorgadas para conectarse a la VPN de forma segura y navegar dentro del segmento de red que mediante políticas creadas en el firewall permitan comunicarse con el equipo o los equipos pertenecientes a esa VLAN. Para esto quienes estén permitidos conectarse remotamente mediante la VPN deberán instalarse el software FortiClient VPN que es un software gratuito proporcionado por Fortigate. Además, para poder conectarnos al servidor de aplicaciones y base de datos que requiere nuestro proyecto de desarrollo, se implementara una vpn exclusiva para ese servicio de tal forma que no tengamos que exponer el Active Directory en una DMZ ya que necesitamos del controlador de dominio para que la aplicación haga la autenticación de los usuarios que estén registrados en el dominio y tengan los permisos para poder loguearse.

Para el acceso remoto se implementó una VPN SSL en el firewall, a continuación, se muestra la configuración.

Proyecto Final – LTI

## COSTOS DE EQUIPAMIENTOS

En esta sección detallamos el costo de los equipamientos que utilizaremos para el desarrollo de nuestra infraestructura.

Hardware	Marca/Modelo	Costo	Total a utilizar	Total
Access Point	Fortinet FAP – 421EV	USD 700	5	USD 3500
Switches – Distribución	Fortiswitch 1024D	USD 10000	2	USD 20000
Switches - Acceso	Fortiswitch 124E-POE	USD 1000	5	USD 5000
Firewall	Fortinet 60E	USD 1000	2	USD 2000
Servidores	Lenovo SR630	USD 7000	5	USD 35000
UPS	APC 3000VA SMART	USD 2000	3	USD 6000

## BACKUPS

Para realizar los Backups, recuperación y replicación de los datos de nuestra infraestructura se decidió implementar el software Veeam, ya que nos posibilita recuperar hasta máquinas virtuales enteras, aplicaciones, restaurar bases de datos y más de forma más rápida que otras soluciones.

Para esto se obtendrá un licenciamiento otorgado por Veeam y luego nosotros configuraremos el entorno en nuestros servidores de tal forma que los servicios mas criticos como las bases de datos y la informacion critica del negocio esten guardados si llegase a ocurrir alguna circunstancia que afectaran estos activos.

Al mismo tiempo tendremos un segundo Data Center dentro de la infraestructura para suplantar al DC principal si ocurre que este esta afectado por alguna falla critica. En este segundo DC tambien se utilizara Veeam. Como tercera respuesta a una contingencia se penso en utilizar Azure o AWS conectado mediante una VPN punto a punto con estos servicios de forma que la conexión sea segura y controlada por nosotros.

.

---

## OPORTUNIDADES DE MEJORA

Consideramos que una infraestructura no tiene un techo limite a la hora de hacer mejoras tanto en Hardware como en Software, todos los años la industria se expande y esto nos lleva a nosotros a estar a la altura de los servicios que queremos implementar, mejorando la seguridad, la comunicación, la velocidad y todo lo que respecta a una red informática. Es por esto que consideramos implementar como mejoras a futuro ya que no queremos excedernos en presupuesto algunas tecnologías y herramientas que nos ayudaran a estar en mejora continua tratando de otorgar a los clientes finales un servicio viable y fiable en el que su información y sus activos estén seguros y disponibles en cualquier circunstancia. Algunas de las herramientas que detallaremos mas adelante ya se utilizan en gran cantidad de empresas y están en auge en los últimos años por temas de ciberseguridad que es una realidad actual que está tomando mucha relevancia es por esto que las consideramos como posibles mejoras a la hora de adquirirlas ya que nos ayudaran a seguir mejorando nuestra infraestructura.

La primera de estas herramientas seria implementar un HoneyPot, más conocido como “sistema trampa” o “señuelo”, es ubicado en la red para que su objetivo sea evitar un posible ataque al sistema informático. La función principal de esta herramienta es detectar y obtener información del ataque informático y, sobre todo, de dónde procede el ataque, para posteriormente tomar las medidas de seguridad necesarias. Actualmente los honeypot son realmente potentes, y nos permiten simular el comportamiento real de un sistema, haciendo creer a los ciber atacantes que han entrado a un sistema real, y que es fácil hacerse con el control. Sin embargo, estarán en un sistema aislado donde nosotros podremos ver exactamente qué es lo que están haciendo y qué vulnerabilidades están intentando explotar.

La segunda herramienta es FortiManager que es una solución que se encarga de administrar de forma centralizada los productos de Fortinet y provee una gestión impulsada por la automatización de los dispositivos desde una sola consola. Es decir, permite una completa administración y visibilidad de los dispositivos de red, a través de un aprovisionamiento optimizado y herramientas de automatización.

La tercera Herramienta es FortiAnalyzer que es un administrador de registros, análisis y plataforma de informes que proporciona a las empresas un panel único de orquestación y automatización para operaciones de seguridad simplificadas, identificación proactiva y remediación de riesgos, así como visibilidad de toda la superficie de ataque.



---

## CONCLUSION

Sin dudas para el equipo The Boys contar con una infraestructura que sea capaz de ofrecerle a los clientes finales un servicio viable es de suma importancia por eso durante la planificación de este proyecto utilizamos las mejores herramientas según nuestra consideración, herramientas muy utilizadas en el rubro de TI, tratando de cumplir con los requerimientos y poniendo foco en puntos importantes como son la seguridad y la continuidad del negocio. Mediante el análisis y la investigación concluimos que no existen infraestructuras perfectas, continuamente hay que estar actualizando el software y el hardware utilizado además de capacitar a los empleados en nuevas tecnologías y mantenernos al tanto de las noticias, la documentación, foros y eventos que los proveedores de Hardware y software nos brindan, también es de suma importancia que nosotros estemos continuamente actualizando la documentación con respecto a lo que se implementó o se implementara y continuar mejorando la documentación respectiva al negocio y a las políticas y recomendaciones que les damos a los clientes finales con respecto al uso correcto de los activos de la empresa. Sin dudas que hay que tener una visión muy amplia y no dejar por sentado nada porque todos los días hay atacantes que están tratando de vulnerar los sistemas y seguramente nos encontremos en el futuro con una situación donde un atacante quiera vulnerar nuestra infraestructura por eso la constancia de mejora es importante para proteger uno de los activos más importantes por las organizaciones, los datos.

## ANEXOS

### ESPECIFICACION TECNICA DE HARDWARE

Fortinet FortiAP U421EV

<https://www.avfirewalls.com/FortiAP-U421EV.asp>

**Fortinet FortiSwitch 1024D**

<https://www.avfirewalls.com/FortiSwitch-1024D.asp>

**Fortinet FortiSwitch 124E-POE**

<https://www.avfirewalls.com/FortiSwitch-124E-POE.asp>

**Lenovo SR630**

<https://www.lenovo.com/uy/es/data-center/servers/racks/ThinkSystem-SR630/p/77XX7SR63?orgRef=https%253A%252F%252Fwww.google.com%252F>

**APC 3000VA SMART**

<https://www.newtek.com.uy/catalog/apc-smart-ups-3000va-smt3000i-regulador-voltaje-usb-lcd-p-11499.html>

### DOCUMENTOS

**Políticas de Seguridad Informatica.pdf**

**Plan de continuidad de negocio.pdf**

**DRP.pdf**

**Videos Demostración**

[https://drive.google.com/drive/folders/1yOeaGY2a2b0yBe4UpgnUleNoZHoso5vK?usp=s\\_haring](https://drive.google.com/drive/folders/1yOeaGY2a2b0yBe4UpgnUleNoZHoso5vK?usp=s_haring)

