



Universidad Nacional  
**ARTURO JAURETCHE**

# Seguridad de la Información

TP n° 5

Salvatori Emiliano

Julio del 2020

<i>ÍNDICE</i>	2
---------------	---

## **Índice**

<b>1. Objetivos</b>	<b>3</b>
<b>2. Escenario</b>	<b>3</b>
<b>3. Resolución de la problemática</b>	<b>3</b>
3.1. Materiales utilizados para el presente trabajo . . . . .	4

## 1. Objetivos

En el siguiente informe se realizarán distintas actividades con respecto al funcionamiento de las ACLs de los Firewalls para la materia **Seguridad de la información Comisión n° 1**.

## 2. Escenario

Usted forma parte del área de IT de la universidad ABC y se le ha asignado la tarea de configurar el firewall del organismo, el cual tiene que cumplir con algunos requerimientos, para ello se debe recordar que la política general se basa en el concepto *bloquear todo excepto lo solicitado*.

Se deben seguir los siguientes lineamientos:

1. El servidor del SIU necesita acceder al servidor de base de datos que es PostgreSQL
2. En las aulas, solo las computadoras de los docentes pueden navegar, usar correo y FTP por internet.
3. Las áreas de administración y alumnos pueden navegar por internet.
4. El área de IT tiene libre acceso hacia internet.
5. Todas las PC de las aulas y areas pueden acceder al FileServer de Windows.
6. Los equipos entre las aulas 1 y 2 pueden comunicarse libremente.
7. Las aulas, areas de administración, alumnos e IT deben poder acceder al mail server interno.
8. IT debe poder acceder por SSH a cualquier equipo de la red de servidores y DMZ.
9. IT debe poder acceder por RDP a las PCs de las aulas, áreas de administración y alumnos.
10. Todos los equipos deben poder consultar los DNS de google.

## 3. Resolución de la problemática

Para establecer una representación de la problemática a abordar, se procede a volcar las reglas con las que debe contar el Firewall en la siguiente tabla:

Regla	IP Origen	IP Destino	Puerto Origen	Puerto Destino	Acción
1	10.100.1.5	10.50.0.10	5432	5432	Permitir
2 <sub>1</sub>	10.10.1.100	Internet	*	*	Permitir
2 <sub>2</sub>	10.10.2.100	Internet	*	*	Permitir
2 <sub>3</sub>	10.10.3.100	Internet	*	*	Permitir
3 <sub>1</sub>	Administración	Internet	*	*	Permitir
3 <sub>2</sub>	Alumnos	Internet	*	*	Permitir
4	Área IT	Internet	*	*	Permitir
5 <sub>1</sub>	10.10.1.0/24	10.50.0.20	139	445	Permitir
5 <sub>2</sub>	10.10.2.0/24	10.50.0.20	139	445	Permitir
5 <sub>3</sub>	10.10.3.0/24	10.50.0.20	139	445	Permitir
6	10.10.1.0/24	10.10.2.0/24	*	*	Permitir
7 <sub>1</sub>	Area I	10.50.0.20	25	25	Permitir
7 <sub>2</sub>	Area II	10.50.0.20	25	25	Permitir
7 <sub>3</sub>	Area II	10.50.0.20	25	25	Permitir
7 <sub>4</sub>	Administración	10.50.0.20	25	25	Permitir
7 <sub>5</sub>	Alumnos	10.50.0.20	25	25	Permitir
7 <sub>5</sub>	IT	10.50.0.20	25	25	Permitir
8 <sub>1</sub>	IT	10.50.0.0/24	22	22	Permitir
8 <sub>2</sub>	IT	10.100.1.0/24	22	22	Permitir
9 <sub>1</sub>	IT	Aula I	3389	3389	Permitir
9 <sub>2</sub>	IT	Aula II	3389	3389	Permitir
9 <sub>3</sub>	IT	Aula III	3389	3389	Permitir
9 <sub>4</sub>	IT	Administración	3389	3389	Permitir
9 <sub>5</sub>	IT	Alumnos	3389	3389	Permitir
10 <sub>1</sub>	*	8.8.8.8	53	53	Permitir
10 <sub>2</sub>	*	8.8.4.4	53	53	Permitir

### 3.1. Materiales utilizados para el presente trabajo

Para la resolución del presente Laboratorio se utilizaron las siguientes herramientas:

1. Arch Linux V5.1.11
2. Para la composición del presente Informe se utilizó el paquete *texlive-latexextra* 2018.50031-1