
**Clave:** TE 2036.501

**Implementación de redes seguras - Gpo 501**

# Actividad M5

# Estamos incomunicados desde hoy por la mañana!!

**Profesor:**
Ramiro Alejandro Bermúdez Uribe

**Integrantes:**
Alexis Gibrán Acosta Pánuco - A01639818

Elías Uriel Velázquez Rojas - A01639716

Fernando Cerriteño Magaña - A01702790

Misael Octavio Rodríguez Macías - A01639786

**Fecha de entrega:**

27 de Noviembre de 2022

- **Pruebas de conectividad**

★ Conexión desde Lan1 (Router RA) hasta MyISP

```
C:\>ping 151.101.1.67

Pinging 151.101.1.67 with 32 bytes of data:

Reply from 151.101.1.67: bytes=32 time=34ms TTL=125
Reply from 151.101.1.67: bytes=32 time=2ms TTL=125
Reply from 151.101.1.67: bytes=32 time=6ms TTL=125
Reply from 151.101.1.67: bytes=32 time=2ms TTL=125

Ping statistics for 151.101.1.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 34ms, Average = 11ms

C:\>
```

★ Conexión desde Lan2 (Router RA) hasta MyISP

```
C:\>ping 151.101.1.67

Pinging 151.101.1.67 with 32 bytes of data:

Reply from 151.101.1.67: bytes=32 time=40ms TTL=125
Reply from 151.101.1.67: bytes=32 time=19ms TTL=125
Reply from 151.101.1.67: bytes=32 time=2ms TTL=125
Reply from 151.101.1.67: bytes=32 time=2ms TTL=125

Ping statistics for 151.101.1.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 40ms, Average = 15ms

C:\>
```

★ Conexión desde Usuarios (Router RF) hasta MyISP

```
C:\>ping 151.101.1.67

Pinging 151.101.1.67 with 32 bytes of data:

Reply from 151.101.1.67: bytes=32 time=19ms TTL=126
Reply from 151.101.1.67: bytes=32 time=23ms TTL=126
Reply from 151.101.1.67: bytes=32 time=1ms TTL=126
Reply from 151.101.1.67: bytes=32 time=1ms TTL=126

Ping statistics for 151.101.1.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 23ms, Average = 11ms

C:\>
```

★ Conexión desde Servers (Router RF) hasta MyISP

```
C:\>ping 151.101.1.67

Pinging 151.101.1.67 with 32 bytes of data:

Reply from 151.101.1.67: bytes=32 time=21ms TTL=126
Reply from 151.101.1.67: bytes=32 time=21ms TTL=126
Reply from 151.101.1.67: bytes=32 time=12ms TTL=126
Reply from 151.101.1.67: bytes=32 time=2ms TTL=126

Ping statistics for 151.101.1.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 21ms, Average = 14ms

C:\>
```

★ Conexión desde Lan1 (Router RA) hasta Usuarios (Router RF)

```
C:\>ping 210.100.155.97

Pinging 210.100.155.97 with 32 bytes of data:

Reply from 210.100.155.97: bytes=32 time=15ms TTL=126
Reply from 210.100.155.97: bytes=32 time=1ms TTL=126
Reply from 210.100.155.97: bytes=32 time=15ms TTL=126
Reply from 210.100.155.97: bytes=32 time=11ms TTL=126

Ping statistics for 210.100.155.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 10ms

C:\>
```

★ Conexión desde Lan2 (Router RA) hasta Servers (Router RF)

```
C:\>ping 210.10.10.67

Pinging 210.10.10.67 with 32 bytes of data:

Reply from 210.10.10.67: bytes=32 time=15ms TTL=126
Reply from 210.10.10.67: bytes=32 time=12ms TTL=126
Reply from 210.10.10.67: bytes=32 time=12ms TTL=126
Reply from 210.10.10.67: bytes=32 time=1ms TTL=126

Ping statistics for 210.10.10.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 10ms

C:\>
```

- **Reporte**

a) Escribe en cada renglón de la Tabla 1 (exclusivamente notación punto decimal) las direcciones **IP** de cada una de las interfaces de los routers y la **Máscara** correspondiente que darán servicio a este esquema de direccionamiento.

| Router | S0/0/0 | S0/0/1 | G0/0 | G0/1 |
|---|---|---|---|---|
| **MyISP** | **134. 89. 254. 241**<br>**----------**<br>**255. 255. 255. 252** | **No se usa**<br>**----------**<br>**No se usa** | **151. 101. 1. 126**<br>**----------**<br>**255. 255. 255. 192** | **No se usa**<br>**----------**<br>**No se usa** |
| **RFrontera** | **134. 89. 254. 242**<br>**----------**<br>**255. 255. 255. 252** | 198. 68. 1. 249<br>----------<br>255. 255. 255. 252 | 210. 100. 155. 126<br>----------<br>255. 255. 255. 224 | **210.10.10.94**<br>**----------**<br>**255. 255. 255. 224** |
| **RA** | 198. 68. 1. 250<br>----------<br>255. 255. 255. 252 | **No se usa**<br>**----------**<br>**No se usa** | 210. 100. 130. 126<br>----------<br>255. 255. 255. 128 | 210. 100. 130. 190<br>----------<br>255. 255. 255. 192 |

b) Se te pide utilizar el formato **RCA** para realizar un análisis post-mortem, documentar todo lo identificado como incorrecto y documentar las acciones emprendidas para reconstruir las configuraciones. Utiliza toda la información disponible con la que cuentas para documentar el análisis post-mortem.

**Formato RCA (Root-Cause-Analysis)**

1. **Información General del Incidente**

| | | | |
|---|---|---|---|
| Impacto | Alto | Prioridad | Alto |
| Urgencia | Crítica | | |
| Reportado por | Santiago N. (Guardia de Seguridad del 3er turno) | Fecha Incidente | 24-11-22 |
| Atendido por | Director de la empresa | Fecha Reporte Final | 26-11-22 |
| Responsable del incidente | Empleado con camisa de cuadros de color café, rayas blancas y gorra azul | Fecha Cierre Reporte | 26-11-22 |

## 2. Historial de Revisiones

| Revisión | Descripción | Autor | Fecha |
|---|---|---|---|
| 1 | Reporte inicial del incidente : Las configuraciones tenían muchos errores de comandos, las ip estaban mal escritas al igual que las máscaras. | Fernando Cerriteño | 24-11-22 |
| 2 | Se realizaron las configuraciones adecuadas así como la corrección en los diferentes comandos del documento, además de las configuraciones de las ip. | Misael Rodriguez<br>Elias Velazquez | 24-11-22 |
| 3 | Se encontraron varios errores en las conexiones en los diferentes routers así como conexiones de red, se levantó el reporte y se contactó a un asesor del tema para el análisis | Misael rodriguez<br>Fernando Cerriteño | 25-11-22 |
| 4 | Se realizó un reporte detallando todo lo sucedido así como el análisis final sobre si fue un ataque o fue un error de un compañero. | Gibran Acosta<br>Elias Velazquez | 26-11-22 |

## 3. Detalle del Incidente

| | |
|---|---|
| Equipos Afectados: | Core cisco (equipos/servicios con falla) |
| Inicio del incidente (Fecha y Hora) | 24/11/2022 05:00:00 a.m |
| Fin del Incidente (Fecha y Hora) | 24/11/2022 06:30:00 a.m |
| Duración del impacto en servicios (Días/Horas/Minutos) | 14/10/00 |
| Descripción del Incidente | La madrugada del día de hoy, el guardia de seguridad de la empresa IT2 Networking Consulting reportó actividad sospechosa en el sitio donde se encuentran los servidores y equipos de ruteo de la compañía para la cual estamos realizando un proyecto de diseño y configuración de red. Este proyecto debe entregarse hoy mismo.<br>Se reporta haber visto en el Laboratorio de Infraestructura Computacional a un sujeto de camisa de cuadros de color café, rayas blancas y de gorra azul. Se observa que el sujeto está sentado en una mesa y realiza conexiones con un cable azul a unas cajas de color verde. Las cajas de color verde tienen unos foquitos de color verde encendidos. En ocasiones se ven parpadear. El sujeto se levanta de su silla y se retira a las 05:45. Se observa que deja la puerta abierta y no se lleva nada del lugar. |

| | |
|---|---|
| Usuarios Afectados | Compañía para la que se realiza el proyecto de diseño y configuración de red. |
| Equipos involucrados | Infraestructura computacional |

## 4. Resumen Ejecutivo

Actividad sospechosa en el sitio donde se encuentran los servidores y equipos de ruteo de la compañía para la cual se está realizando un proyecto de diseño y configuración de red. El proyecto debe de ser entregado ese mismo día. El director de la empresa recibió el reporte a las 8:00 am y después de leerlo, decidió pasar el caso a sus consultores estrella para que revisen las configuraciones de los equipos de interconexión y corrijan lo que tengan que corregir para garantizar la funcionalidad de la red.

## 5. Narrativa del Incidente

| No. | Fecha/Hora | Descripción |
|---|---|---|
| 1 | 24 nov 2022 05:00 | Un sujeto de camisa de cuadros de color café, rayas blancas y de gorra azul está sentado en una mesa y realiza conexiones con un cable azul a unas cajas de color verde. Las cajas de color verde tienen unos foquitos de color verde encendidos. En ocasiones se ven parpadear. El sujeto se levanta de su silla y se retira a las 05:45. Se observa que deja la puerta abierta y no se lleva nada del lugar. |
| 2 | 24 nov 2022 06:30 | El guardia de seguridad del 3er turno (Santiago N.) de la empresa IT2 Networking Consulting reporta actividad sospechosa en el site donde se encuentran los servidores y equipos de ruteo de la compañía para la cual se está realizando un proyecto de diseño y configuración de red. |
| 3 | 24 nov 2022 08:00 | El director de la empresa recibió el reporte y después de leerlo, decidió pasar el caso a sus consultores estrella para que revisen las configuraciones de los equipos de interconexión y corrijan lo que tengan que corregir para garantizar la funcionalidad de la red. |
| 4 | 11:30 | Se realizó una investigación sobre los errores en las diferentes configuraciones y conexiones para identificar el posible ataque realizado además de empezar a corregir las diferentes correcciones en las configuraciones |
| 5 | 11:50 | Se completaron todas las configuraciones y conexiones entre dispositivos se levantó el reporte sobre el incidente, se dio un análisis respecto a lo ocurrido así como nuestro asesoramiento como experto del tema tras los datos reunidos en los diferentes documentos y conexiones. |
| 6 | 12:10 | Cierre del incidente |

## 6. Análisis Causa Raíz

| No. | Pregunta | Descripción |
|---|---|---|
| 0 | ¿Qué? | La empresa sufrió un ataque cibernético por lo que diversos routers no están conectados o no funcionan, la oficina está incomunicada. |
| 1 | ¿Por qué? | Un sujeto no autorizado modificó y realizó unas conexiones entre los componentes, estas conexiones fueron erróneas y fueron el origen del error. |
| 2 | ¿Por qué? | Realizaba horas extras pero por el cansancio cometió varios errores en las diferentes configuraciones realizadas |
| 3 | ¿Por qué? | El cansancio hizo que cometiera varios errores en las configuraciones debido a las altas horas en las que se encontraba trabajando. |
| 4 | ¿Por qué? | Los routers tienen mal las ip respecto a la máscara con las que estaban configuradas |
| 5 | ¿Por qué? | Los routers no se pueden conectar ante los demás servidores de las oficinas por las malas configuraciones de las ip así como el mal funcionamiento de algunos dispositivos |

## 7. Acciones de seguimiento

| No. | Tarea | Responsable | Fecha Compromiso | Estatus |
|---|---|---|---|---|
| 1 | Revisar las configuraciones recuperadas | REDES | 24 Nov | TERMINADO |
| 2 | Corregir la configuración de un conjunto de equipos de interconexión (routers y switch) | REDES | 24 Nov | TERMINADO |
| 3 | Se levantó el reporte y se contactó a un asesor del tema para el análisis | REDES | 24 Nov | TERMINADO |
| 4 | Recuperar la conexión con Internet desde cualquier equipo de la LAN. | REDES | 25 Nov | TERMINADO |
| 5 | Realizar un reporte detallando todo lo sucedido así | MONITOREO | 26 Nov | EN PROCESO |
| 6 | Realizar un análisis final sobre si fue un ataque o fue un error de un compañero. | MONITOREO | 26 Nov | EN PROCESO |
| 7 | Entregar el reporte | MONITOREO | 27 Nov | EN PROCESO |

c) Argumenta, desde el punto de la Ética, la decisión que tomarás sobre su petición y qué harás con el reporte final que se te solicita. ¿Qué argumentos utilizarías para dar una respuesta a tu conocido? ¿Cuáles son las consecuencias de acceder a la petición de tu compañero?

Como se mencionó anteriormente debido a la altas horas de trabajo y a la horas extra que el compañero estaba haciendo este cometió errores en las configuraciones aparte de guardar una configuración errónea, por lo que nuestro compañero no planeó un ataque hacia la empresa y el solo cometió un error grande por culpa del cansancio por necesitar horas extras por su urgencia económica, no es nuestra obligación tomar la decisión pero el empleado solo necesita una llamada de atención fuerte por el error que cometió pero no consideramos necesario correrlo del trabajo y esto es ya que a pesar de lo sucedido con la llamada de atención el entenderá y aprenderá de su error para no volverlo a cometer.