

INFORME PRUEBA DRP – ACTIVACIÓN DE CANAL SECUNDARIO

Octubre 2024

CONTROL DE VERSIONES

Versión	Fecha	Comentarios	Por
1	18-10-2024	Elaboración del informe	ISEGURAS S.A.S

CONTENIDO

1 INTRODUCCIÓN 4

2 OBJETIVOS 5

2.1 OBJETIVO GENERAL 5
2.2 OBJETIVOS ESPECÍFICOS 5

3 ALCANCE 5

3.1 EXCLUSIONES 5

4 EJECUCIÓN DE LA PRUEBA 6

4.1 FECHA DE REALIZACIÓN 6
4.2 PARTICIPANTES INTERNOS 6
4.3 PARTICIPANTES EXTERNOS: PROVEEDORES 7
4.4 PROCEDIMIENTOS DE CONTINUIDAD A PROBAR 8
4.5 INDICADORES DE GESTIÓN 8
4.6 RECURSOS 8

5 DESARROLLO DE LA PRUEBA 9

6 EVIDENCIAS ACTIVIDADES DEL MINUTOGRAMA 10

7 CONCLUSIONES 18

1 INTRODUCCIÓN

El Plan de Continuidad del Negocio establece que se debe asegurar el compromiso institucional en la actualización e implementación del PCN, así como con la ejecución del programa de pruebas definido para cada año. Dicho compromiso involucra a los servidores del Instituto para el Desarrollo de Antioquia - IDEA, así como a los actores externos que participan en los procesos críticos de la entidad ante cualquier tipo de interrupción o crisis.

El plan de pruebas del DRP contempla lo siguientes tipos de pruebas:

- **Tecnica:** Consiste en una prueba cerrada (sin participación de usuarios) de las capacidades técnicas de la plataforma y de los equipos de recuperación de los servicios de tecnología.

- **Funcional:** Consiste en la prueba de las aplicaciones y servicios críticos de TI. En un entorno controlado con la participación de usuarios finales para la validación.

- **Integral:** Consiste en la incorporación de terceras partes en el desarrollo de las pruebas, por ejemplo, proveedores de servicio, entes reguladores u otras partes interesadas.

2 OBJETIVOS

2.1 Objetivo General

Garantizar la recuperación del acceso a Internet y las VPNs Site to Site, ante la materialización de un evento disruptivo, con el fin de restablecer la prestación de sus servicios en el menor tiempo posible, cumpliendo con los tiempos esperados de recuperación – RTO, identificados en el análisis de impacto al negocio.

2.2 Objetivos específicos

- Verificar la preparación del personal para restablecer los canales de internet ante un incidente de interrupción.
- Probar que los servicios recuperados funcionan adecuadamente.
- Garantizar la seguridad de la información en un escenario de contingencia.

3 ALCANCE

El alcance de la prueba tiene como propósito mitigar el siguiente escenario de desastre:

No.	Escenario de Desastre	Causas	BCP	DRP
1.	Indisponibilidad del canal principal de acceso a internet y VPNs	• Falla en canales de comunicación: Corte de fibras. • Daño de dispositivos de comunicación. Routers. • Acceso físico no autorizado. • Errores humanos. • Amenazas naturales.		X

3.1 Exclusiones

La prueba no incluye la participación de usuarios finales.

4 EJECUCIÓN DE LA PRUEBA

4.1 Fecha de realización

La prueba se realizó el día 11 de octubre de 2024. La actividad inició a las 20:00 horas y finalizó a las 20:36 horas.

4.2 Participantes internos

Para el desarrollo de la prueba participaron los siguientes funcionarios:

Nombre	Cargo	Contacto
Jair Antonio Villanueva Ricardo	Gerente de TI y Operaciones	JairVR@idea.gov.co
Alexander Restrepo Zuluaga	Director de TI	AlexanderRZ@idea.gov.co
Carlos Eduardo Ochoa	Profesional Universitario - Dirección de TI	carlosoa@idea.gov.co
Diego Londoño	Profesional Universitario - Dirección de TI	diegolv@idea.gov.co
Diana Sirley Ortiz Velásquez	Gerente de Riesgos	DianaOV@idea.gov.co
William René Alvarado Ordóñez	Director de Ciberseguridad y Seguridad de la Información	WilliamAO@idea.gov.co
Yaritza Shirley Montoya Bolívar	Contratista - Dirección de Ciberseguridad y Seguridad de la Información	YaritzaMB@idea.gov.co
Leydy Carolina Barrios Urrego	Contratista - Gerencia de Riesgos	LeydyBU@idea.gov.co

4.3 Participantes externos: Proveedores

Para el desarrollo de la prueba participaron los siguientes proveedores:

Proveedor	Rol	Contacto
Tigo UNE - Canales	No se requiere en la prueba	
Core IP – Ciberseguridad – Administración del Firewall	No se requiere en la prueba	
Proveedor SOC - Olimpia	Juan Camilo Carrillo Néstor Fabian Cuellar José Miguel Ortiz Pimentel	Dirección de Ciberseguridad y Seguridad de la Información
Valor Mas – VPNs Línea 800 Mesa de Servicio	Requerido	Dirección de TI
SIIF G&G	Requerido	Dirección de TI
Conectividad Bancos	Pruebas de autenticación en portales	Gerencia de TI y Operaciones
Iseguras (Observadores)	Ramiro Merchán – Consultor BCP Juan Manuel Santoyo – Consultor BCP Joaquin Afanador – Consultor BCP	ramiro.merchan@iseguras.com.co juan.santoyo@iseguras.com.co joaquin.afanador@iseguras.com.co

4.4 Procedimientos de continuidad a probar

Durante la prueba se verificó la idoneidad de los siguientes procedimientos:

- No Aplica

4.5 Indicadores de gestión

Durante la prueba se verificaron los siguientes indicadores de continuidad:

Indicadores Generales	RTO del proceso más critico	Resultado
RTO (horas)	1 hora	22 min
RPO (horas)	24 horas	No incluido en el alcance de la prueba

4.6 Recursos

Previo a la ejecución de la prueba se tiene acceso a los siguientes recursos:

- **Explorador web (Microsoft Edge, Firefox, Chrome)**
- **Consola de administración Fortigate**
- **Acceso a servicios de Azure**

5 DESARROLLO DE LA PRUEBA

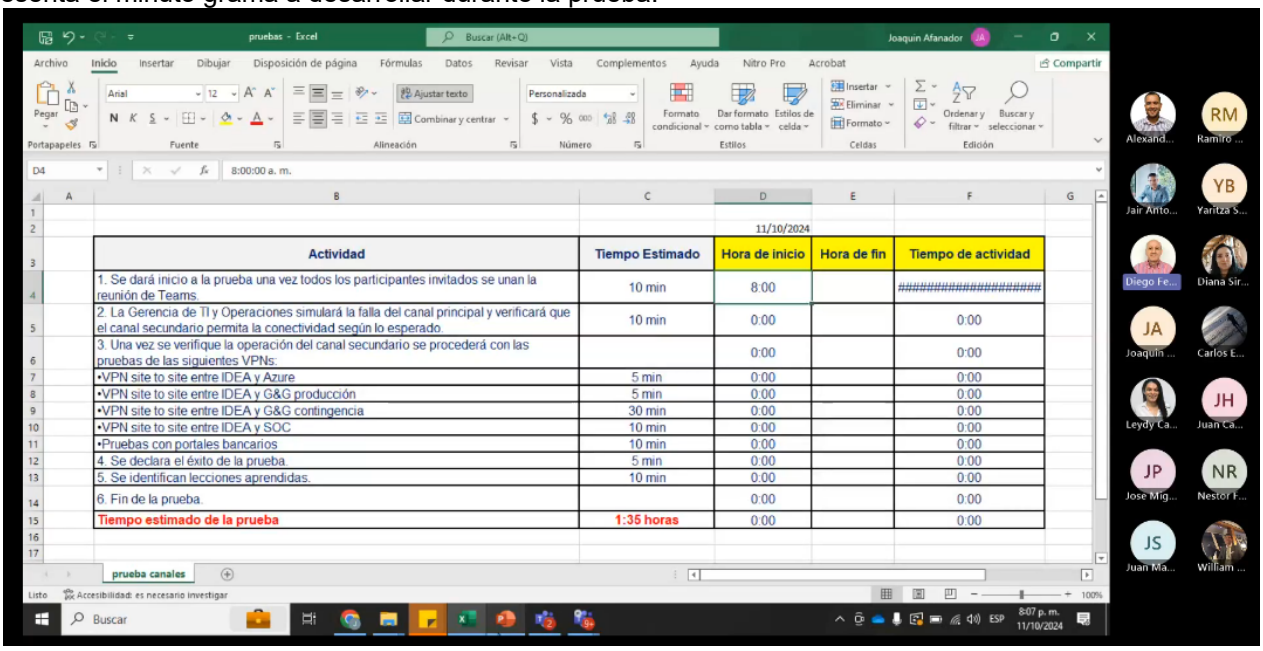
A continuación, se presenta el minuto grama ejecutado durante la prueba:

Actividad	Tiempo Estimado	Hora de inicio Real	Hora de fin real	Tiempo de actividad	Observaciones
1. Se dará inicio a la prueba una vez todos los participantes invitados se unan la reunión de Teams.	10 min	20:00	20:10	0:10	
2. La Gerencia de TI y Operaciones simulará la falla del canal principal y verificará que el canal secundario permita la conectividad según lo esperado.	10 min	20:10	20:11	0:01	El cambio al canal secundario fue del orden de segundos.
3. Una vez se verifique la operación del canal secundario se procederá con las pruebas de las siguientes VPNs:					El SOC se demora en verificar que el canal secundario se encuentra caído.
3.1. VPN site to site entre IDEA y G&G producción	5 min	20:20	20:22	0:02	
3.2. VPN site to site entre IDEA y G&G contingencia	30 min	20:22	20:23	0:01	
3.3. VPN site to site entre IDEA y Azure	5 min	20:24	20:27	0:03	
3.4. VPN site to site entre IDEA y SOC	10 min	20:24	20:29	0:05	
3.5. Pruebas con portales bancarios	10 min	20:30	20:36	0:06	
4. Se declara el éxito de la prueba.	5 min	20:36	20:40	0:04	
5. Se identifican lecciones aprendidas.	10 min	20:40	20:40	0:00	
6. Rollback	10 min	20:40	20:44	0:04	
7. Fin de la prueba.		20:44			
Tiempo estimado de la prueba	**1:45 horas**			**36 minutos**	

6 EVIDENCIAS ACTIVIDADES DEL MINUTOGRAMA

1. Se dará inicio a la prueba una vez todos los participantes invitados se unan la reunión de Teams.

A continuación, se evidencia momento en el que los participantes hacen su presentación, luego de lo cual se presenta el minuto grama a desarrollar durante la prueba.



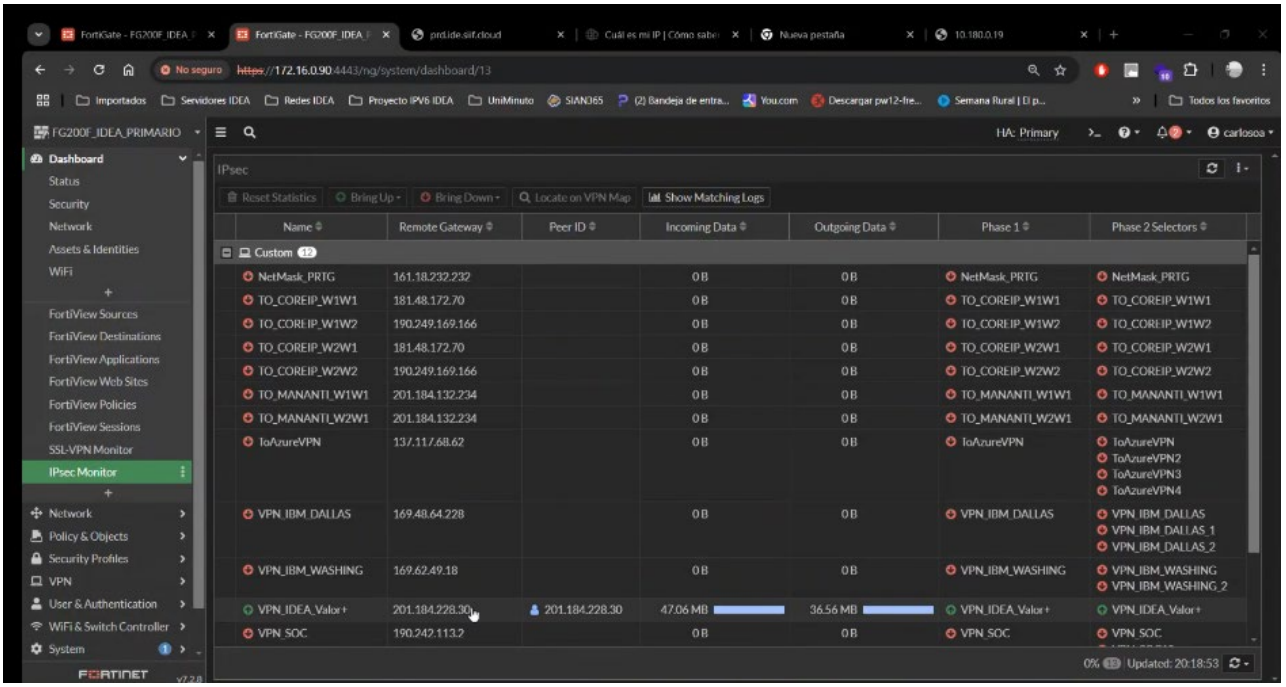
11/10/2024

Actividad	Tiempo Estimado	Hora de inicio	Hora de fin	Tiempo de actividad
1. Se dará inicio a la prueba una vez todos los participantes invitados se unan la reunión de Teams.	10 min	8:00		##########
2. La Gerencia de TI y Operaciones simulará la falla del canal principal y verificará que el canal secundario permita la conectividad según lo esperado.	10 min	0:00		0:00
3. Una vez se verifique la operación del canal secundario se procederá con las pruebas de las siguientes VPNs:		0:00		0:00
•VPN site to site entre IDEA y Azure	5 min	0:00		0:00
•VPN site to site entre IDEA y G&G producción	5 min	0:00		0:00
•VPN site to site entre IDEA y G&G contingencia	30 min	0:00		0:00
•VPN site to site entre IDEA y SOC	10 min	0:00		0:00
•Pruebas con portales bancarios	10 min	0:00		0:00
4. Se declara el éxito de la prueba.	5 min	0:00		0:00
5. Se identifican lecciones aprendidas.	10 min	0:00		0:00
6. Fin de la prueba.		0:00		0:00
Tiempo estimado de la prueba	1:35 horas	0:00		0:00

2. La Gerencia de TI y Operaciones simulará la falla del canal principal y verificará que el canal secundario permita la conectividad según lo esperado.
Momento en el que inicia la prueba. Se presenta la IP pública del canal principal.



A continuación, se muestra la evidencia de la caída del canal principal



Momento en el que el canal secundario se encuentra operativo y se evidencia cambio en la IP pública



3. Una vez se verifique la operación del canal secundario se procederá con las pruebas de las siguientes VPNs:

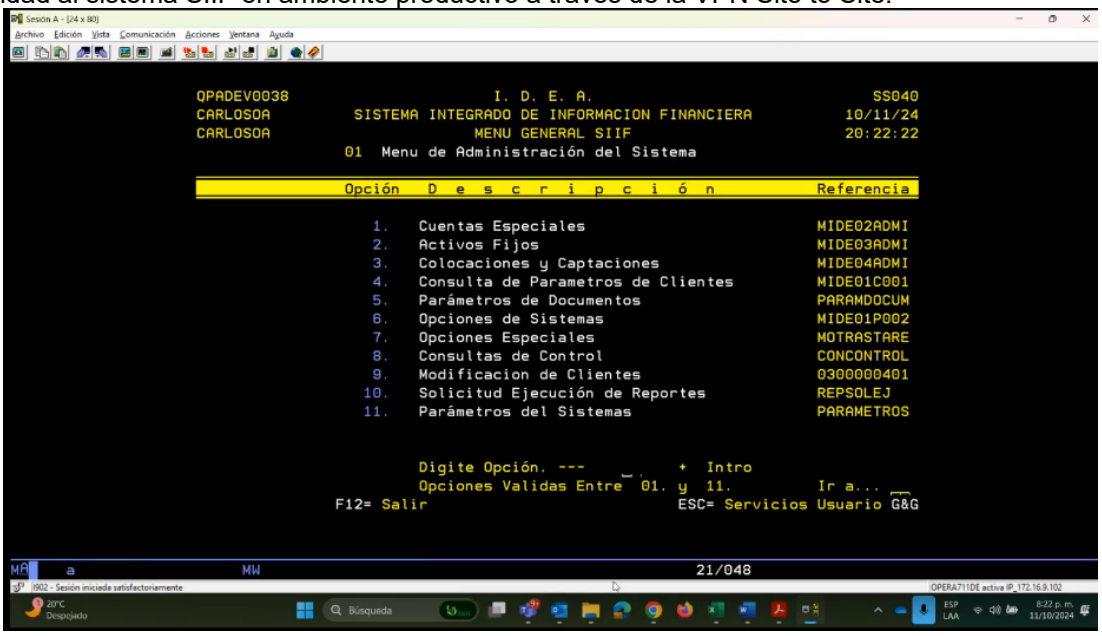
El SOC se demora en verificar que el canal secundario se encuentra caído. Sobre las 8:20 se hacen las verificaciones correspondientes y se inician las pruebas con las VPNs Site to Site.

3.1. VPN site to site entre IDEA y G&G producción

A continuación, se evidencia el momento en el que la VPN Site to Site se encuentra arriba y permite conectividad, con el ambiente SIIF de producción.



Conectividad al sistema SIIF en ambiente productivo a través de la VPN Site to Site.

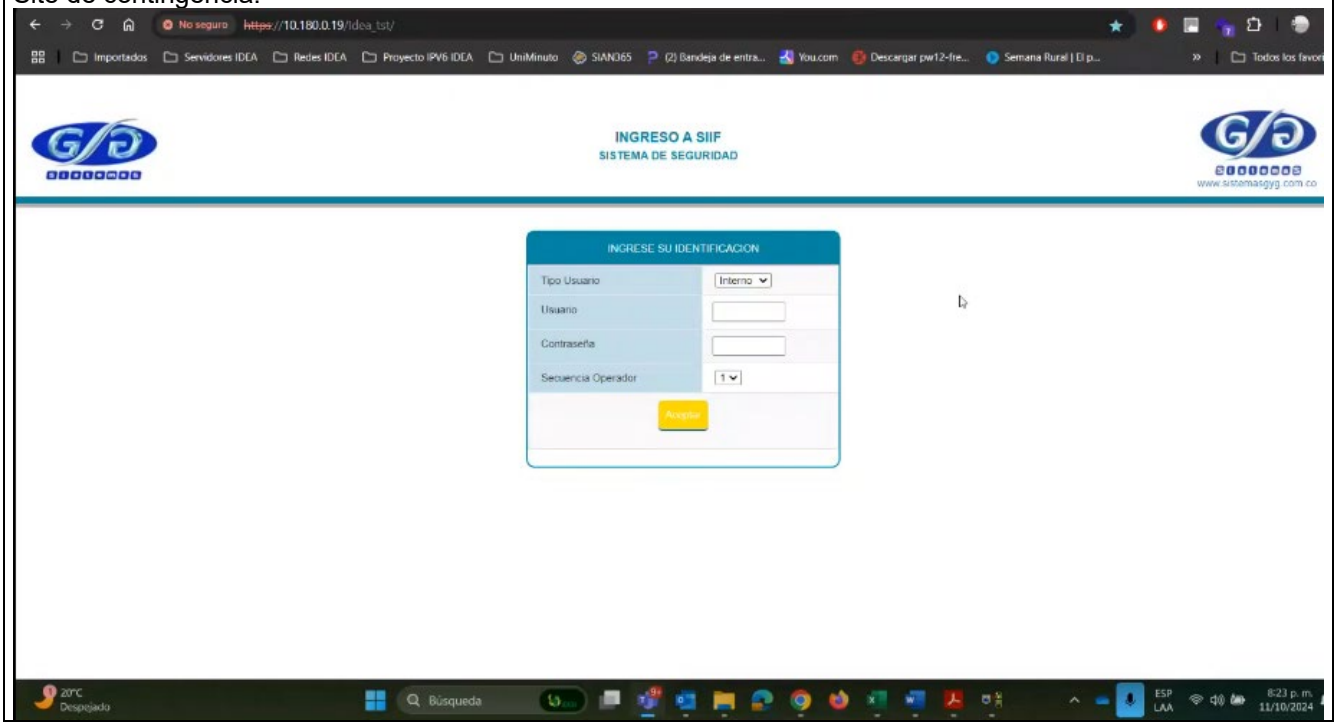


Evidencia del funcionamiento de la VPN site to site al ambiente de producción de G&G

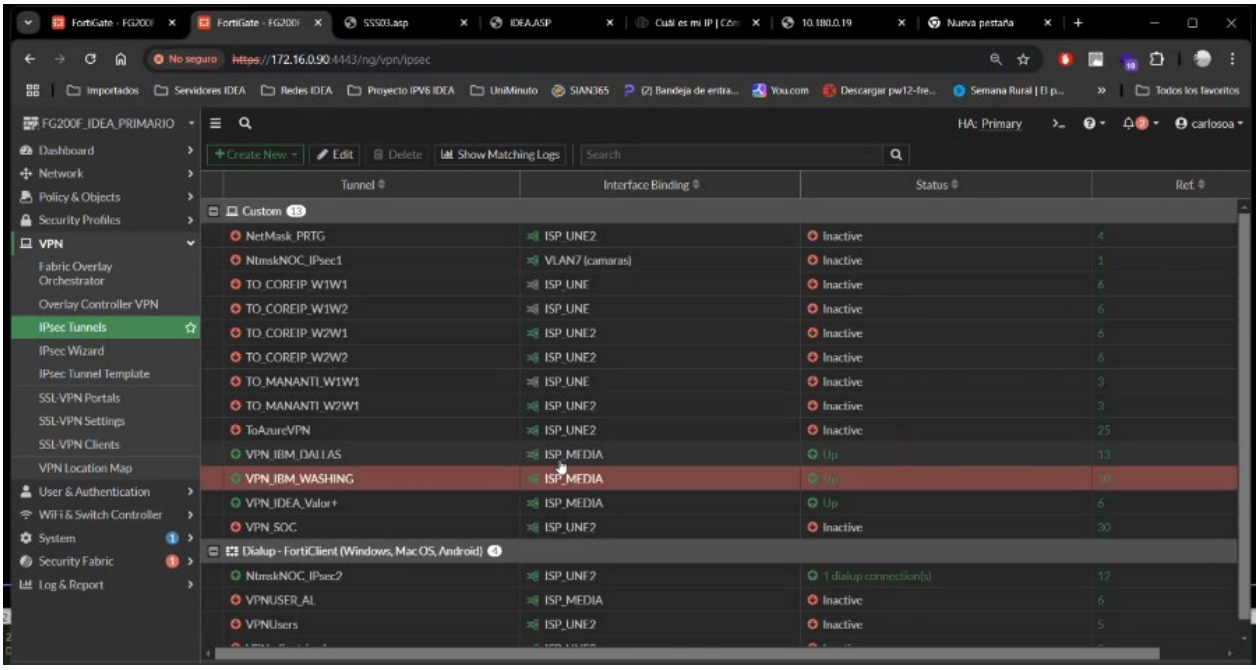


3.2. VPN site to site entre IDEA y G&G contingencia

Momento en el que se tiene conectividad al ambiente de pruebas del sistema SIIF a través de la VPN Site to Site de contingencia.

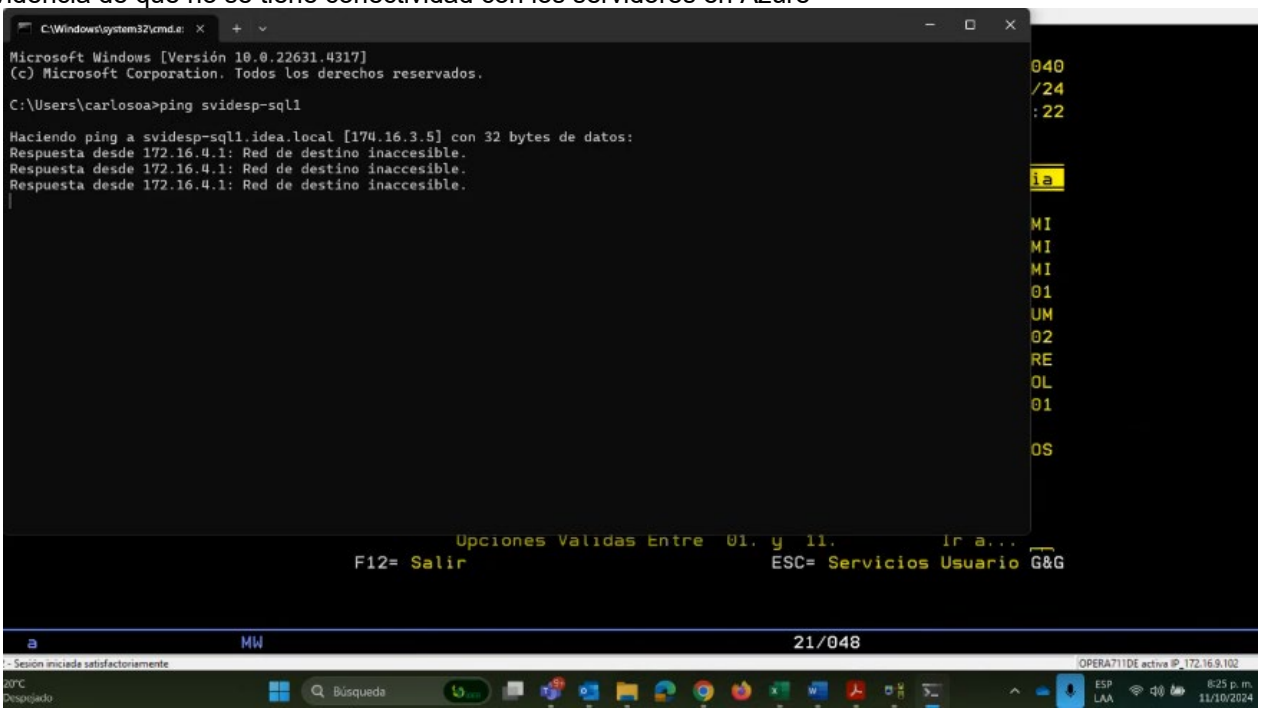


Evidencia del funcionamiento de la VPN site to site al ambiente de pruebas de G&G

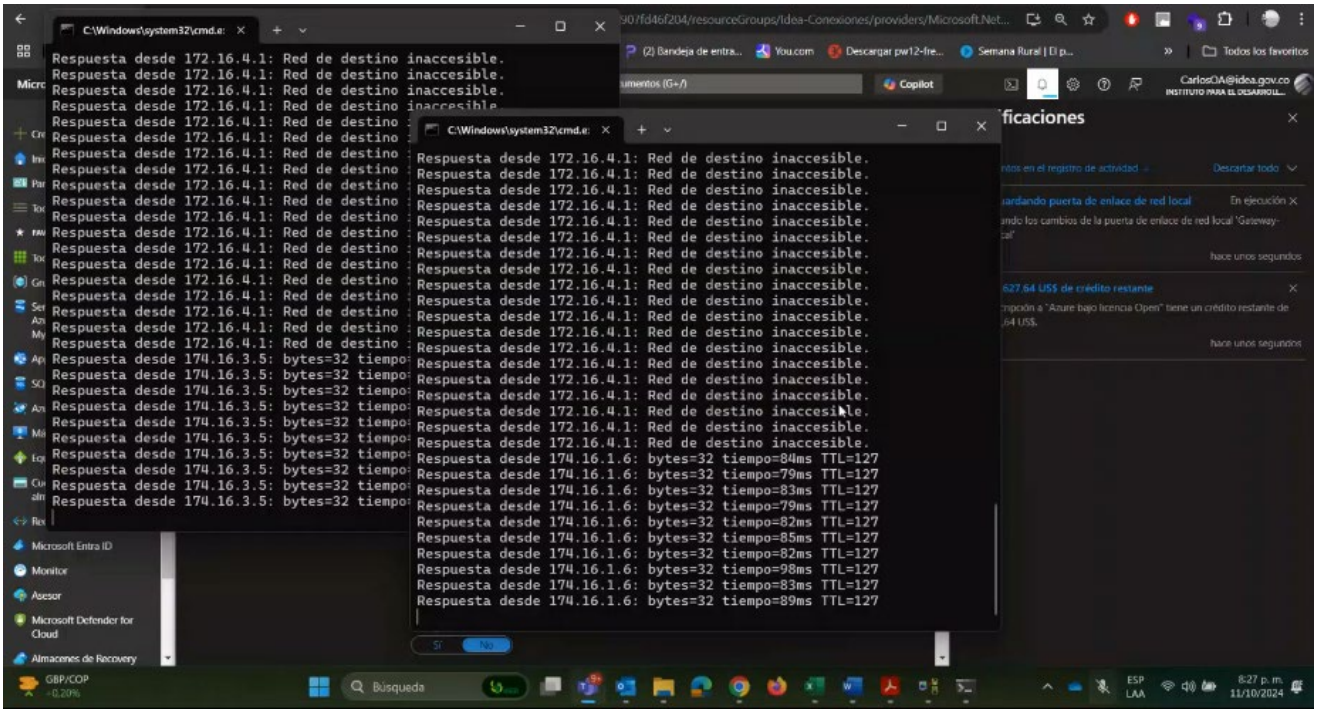


3.3. VPN site to site entre IDEA y Azure

Evidencia de que no se tiene conectividad con los servidores en Azure



Momento en el que la VPN site to site con los servicios de Azure, entra en funcionamiento

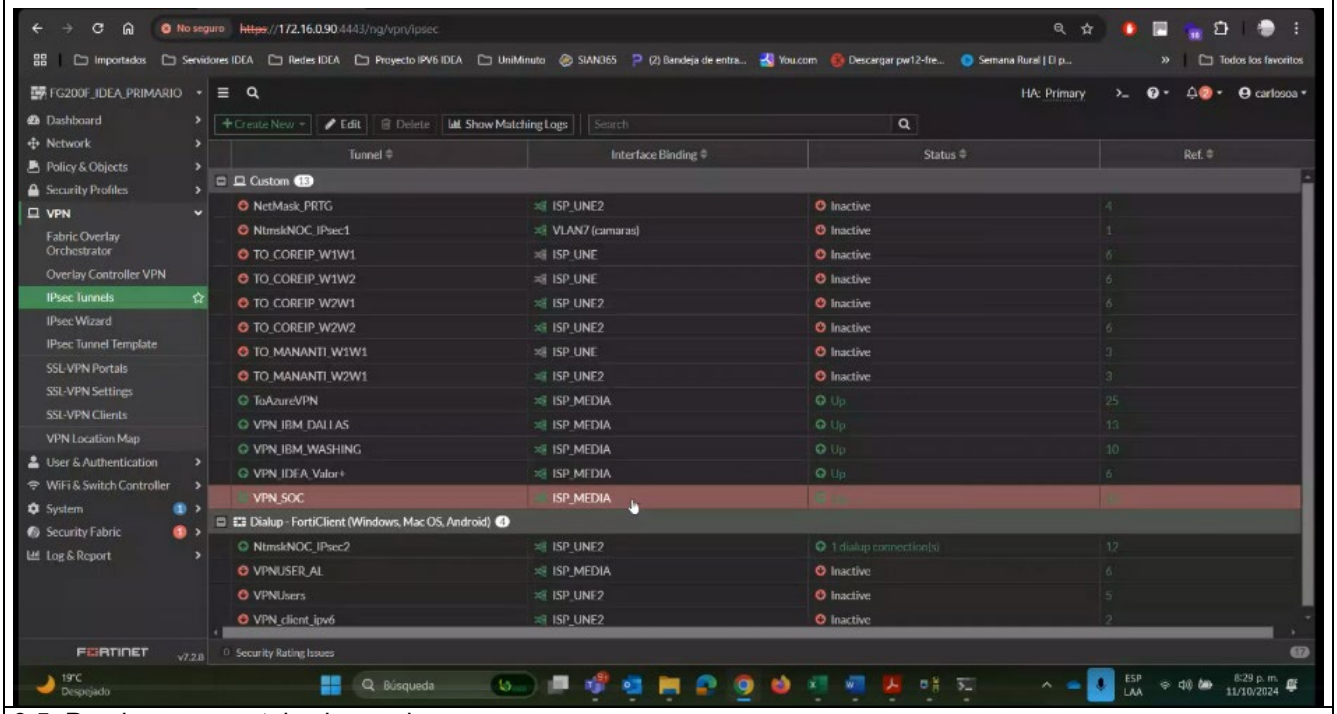


Evidencia de la VPN Site to Site con Azure en funcionamiento



3.4. VPN site to site entre IDEA y SOC

Momento en el que la VPN Site to Site con el SOC queda en funcionamiento



3.5. Pruebas con portales bancarios.

Las pruebas a los portales bancarios se ejecutan de manera confidencial. El Gerente de TI y Operaciones - Jair Antonio Villanueva Ricardo es quien las realiza.

Estas pruebas se inician sobre las 20:30 horas y finalizan sobre las 20:36 horas.

4. Se declara el éxito de la prueba.

Se declara el éxito de la prueba sobre las 20:40 horas. Se concluye que se tienen claros los pasos por parte de la Dirección de TI para poner en funcionamiento el canal secundario de acceso a internet, así como las VPNs con:

- VPN site to site entre IDEA y G&G producción
- VPN site to site entre IDEA y G&G contingencia
- VPN site to site entre IDEA y Azure
- VPN site to site entre IDEA y SOC

Se identifica que el SOC se demora en verificar que el canal secundario se encuentra caído, se indica que se debe a la marca de firewall que se tiene en el SOC (CheckPoint).

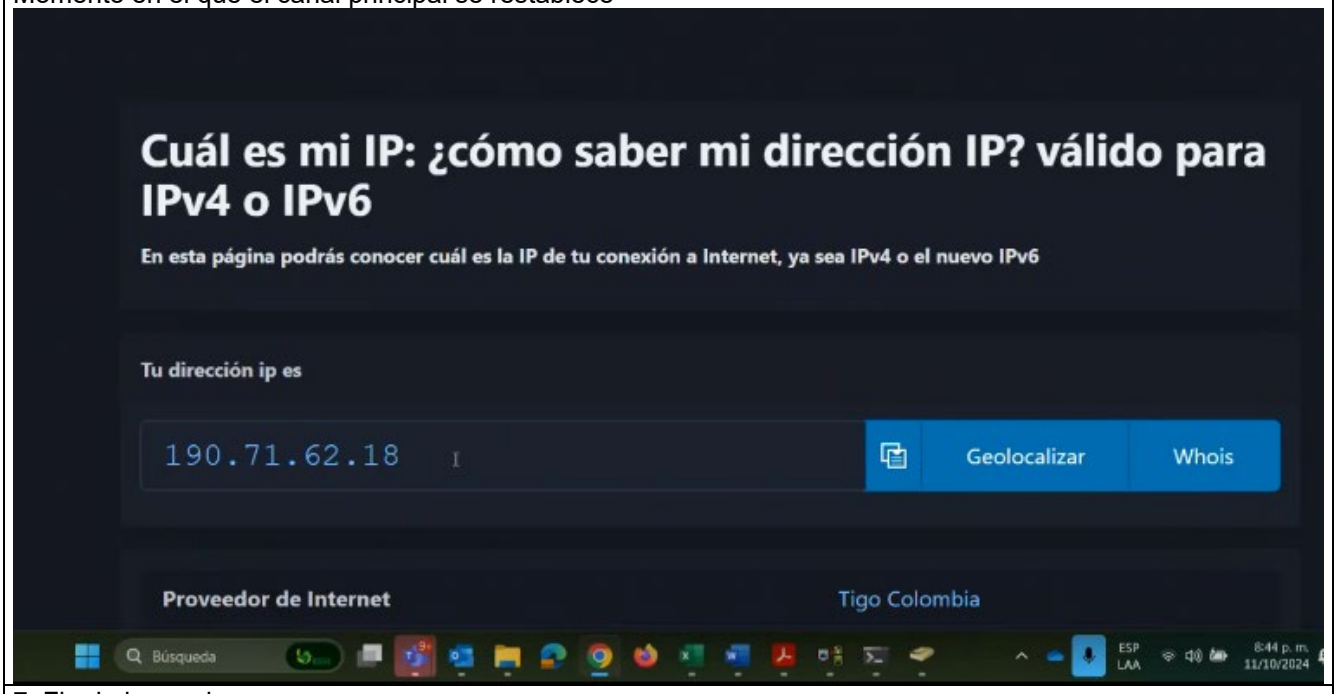
El Director de Ciberseguridad y Seguridad de la Información el ing. William René Alvarado Ordóñez pregunta si, además del Profesional Universitario - Dirección de TI el ing. Carlos Eduardo Ochoa, alguien más tiene el conocimiento del procedimiento, y la Dirección de TI responde que el Profesional Universitario - Dirección de TI el ing. Diego Londoño también posee la competencia.

5. Se identifican lecciones aprendidas.

No se identifican lecciones aprendidas.

6. Rollback

Momento en el que el canal principal se restablece



7. Fin de la prueba.

7 CONCLUSIONES

- La prueba inicio sobre las 20:10 horas. La prueba finaliza sobre las 20:40 horas de manera exitosa. Se concluye que, por parte de la Dirección de TI, se tienen claros los pasos para poner en funcionamiento el canal secundario de acceso a internet, asi como las VPNs con:
  - VPN site to site entre IDEA y G&G producción
  - VPN site to site entre IDEA y G&G contingencia
  - VPN site to site entre IDEA y Azure
  - VPN site to site entre IDEA y SOC

- El Director de Ciberseguridad y Seguridad de la Información el ing. William René Alvarado Ordóñez pregunta si además del Profesional Universitario - Dirección de TI el ing. Carlos Eduardo Ochoa, alguien más tiene el conocimiento, y la Dirección de TI responde que el Profesional Universitario - Dirección de TI el ing. Diego Londoño también posee la competencia.

- No se identifican lecciones aprendidas.

- El ing. José Miguel Ortiz Pimentel del Proveedor SOC informa, sobre las 20:50, que aún no se reciben eventos con normalidad, razón por la cual el ing. Ramiro Merchan – Consultor BCP, al ver que el correlacionador de eventos se demora en recibir eventos, pregunta si hubo perdida de eventos. Por lo anterior se une a la ing. Andrea Alejandra Cortes Angarita a quien se le pregunta sobre el funcionamiento de la solución Qradar, donde se explica que se tiene un Collector on Premise, el cual almacena los Logs y los reenvía a la Nube para su gestión.

- El ing. Ramiro Merchan – Consultor BCP pide validar si se tienen eventos de la ejecución de la prueba, y la ing. Andrea Alejandra Cortes Angarita indica que se tienen Logs de todas las fuentes configuradas y presenta evidencia. Se concluye que no se presenta perdida en la recolección de eventos de seguridad.