	INFORME PERIÓDICO DEL SUPERVISOR (Para Contratos diferentes la prestación de servicios profesionales y de apoyo a la gestión)	**Código:** GC-FT-65 **Versión: 3** **Página:** 1 de 1 **Vigente Desde:** 23/11/2021

1. Datos generales

Número del Contrato o Convenio	IDIGER 295-2025							**Fecha suscripción contrato o convenio::**	17/12/2025		
Tipo de contrato	MINIMA CUANTIA							**Nombre o Razón Social del Contratista:**	GIGA SOURCE TECHNOLOGY DE COLOMBIA SAS		
Plazo de Ejecución (meses)	4 MESES							**Número de Cédula o NIT:**	900.702.873-0		
Periodo del Informe:	9	4	2026	al	18	4	2026	**Nombre del Representante Legal: (Quien en tenga la facultad en el periodo)**	WILMAR DÍAZ RODRÍGUEZ		
Interventor (si Aplica)	NO APLICA							**Número de Cédula o NIT: Nombre del Representante Legal: (Quien en tenga la facultad en el periodo)**	80.854.925 de Bogotá DC		
Cargo del Supervisor (1) del IDIGER (según cláusula de supervisión del contrato/convenio)	JEFE DE OFICINA TICS (SUPERVISION TEMPORAL DELEGADA)							**Nombre Supervisores de otras entidades (cooperantes) - (Si aplica)**	NO APLICA		
Cargo del Supervisor (2) del IDIGER (según cláusula del supervisor del contrato/convenio) Si Aplica	NO APLICA							**Cargos supervisores de otras entidades (Si Aplica)**	NO APLICA		
Cargo Apoyo a la Supervisión del IDIGER	NO APLICA										

Objeto Contractual:

ADQUIRIR SOPORTE, MANTENIMIENTO Y ASISTENCIA TÉCNICA PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL IDIGER, PARA GARANTIZAR LA FUNCIONALIDAD Y ACCESIBILIDAD DE LOS SISTEMAS QUE SOPORTAN LA INFORMACIÓN PROPIA DE LA ENTIDAD

2. Información presupuestal y plazo de ejecución

Valor Inicial del contrato/convenio	$ 20.408.500	**Aporte IDIGER**	Valor CDP	$ 22.759.275	Número CDP	468	Fecha CDP	20/10/2025	Fuente de Recursos	IDIGER
			Valor RP	$ 20.408.500	Número RP	688	Fecha RP	17/12/2025		
		Aporte FONDIGER	Valor CDP		Número CDP		Fecha CDP		Fuente de Recursos	
			Valor RP		Número RP		Fecha RP			
Plazo Inicial de Ejecución (meses)	4	**Valor Total**	$ 20.408.500							
		Aporte Cooperante/Parte Conviniente (Dinero/Especie) Según Aplique			**Descripción**					
		Valor Total	$ 20.408.500							

2.1 Adiciones y Prórrogas

Valor Adición No. 1 del contrato/convenio		**Aporte IDIGER**	Valor CDP		Número CDP		Fecha CDP		Fuente de Recursos	IDIGER
			Valor RP		Número RP		Fecha RP			
		Aporte FONDIGER	Valor CDP		Número CDP		Fecha CDP		Fuente de Recursos	
Cantidad de meses de prórroga 1			Valor RP		Número RP		Fecha RP			
		Subtotal	$ 0							
		Valor Total (Inicial + Adición 1)	$ 20.408.500							
Cantidad Total de meses (Total plazo de ejecución)		**Aporte Cooperante/Parte Conviniente (Dinero/Especie) Según Aplique**			**Descripción**					
		Valor Total	$ 20.408.500							

Si tiene mas de dos adiciones y prórrogas inserte las casillas necesarias

2.2 Disminuciones (Cuando Aplique)

Fecha Documento Disminución:		**Valor disminución :**	

Descripción del motivo de la disminución

NOVEDADES DE EJECUCIÓN PRESUPUESTAL

2.3 VALOR TOTAL Y PLAZO TOTAL MAS MODIFICACIONES

Cantidad de Adiciones (Sume la cantidad de adiciones realizadas)	0	**Valor Total de Contrato/Convenio (Valor inicial + Valor total de las Adiciones)**	$ 20.408.500	**Plazo Total de Ejecución (Cantidad de meses inicial + Cantidad de mese prórrogas)**	4 MESES

2.4. Anticipo (Si Aplica)

Valor Anticipo (Si Aplica)		**Porcentaje de Amortización (Si Aplica)**		**Fecha Pago del Anticipo**	dd	mm	aaa

	INFORME PERIÓDICO DEL SUPERVISOR (Para Contratos diferentes la prestación de servicios profesionales y de apoyo a la gestión)	**Código:** GC-FT-65 **Versión: 3** **Página:** 1 de 1 **Vigente Desde:** 23/11/2021

1. Datos generales

Número del Contrato o Convenio	IDIGER 295-2025							**Fecha suscripción contrato o convenio::**	17/12/2025	
Tipo de contrato	MINIMA CUANTIA							**Nombre o Razón Social del Contratista:**	GIGA SOURCE TECHNOLOGY DE COLOMBIA SAS	
Plazo de Ejecución (meses)	4 MESES							**Número de Cédula o NIT:**	900.702.873-0	
Periodo del Informe:	9	4	2026	al	18	4	2026	**Nombre del Representante Legal: (Quien en tenga la facultad en el periodo)**	WILMAR DÍAZ RODRÍGUEZ	
Interventor (si Aplica)	NO APLICA							**Número de Cédula o NIT: Nombre del Representante Legal: (Quien en tenga la facultad en el periodo)**	80.854.925 de Bogotá DC	
Cargo del Supervisor (1) del IDIGER (según cláusula de supervisión del contrato/convenio)	JEFE DE OFICINA TICS (SUPERVISION TEMPORAL DELEGADA)							**Nombre Supervisores de otras entidades (cooperantes) - (Si aplica)**	NO APLICA	
Cargo del Supervisor (2) del IDIGER (según cláusula del supervisor del contrato/convenio) Si Aplica	NO APLICA							**Cargos supervisores de otras entidades (Si Aplica)**	NO APLICA	
Cargo Apoyo a la Supervisión del IDIGER	NO APLICA									

Objeto Contractual:

ADQUIRIR SOPORTE, MANTENIMIENTO Y ASISTENCIA TÉCNICA PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL IDIGER, PARA GARANTIZAR LA FUNCIONALIDAD Y ACCESIBILIDAD DE LOS SISTEMAS QUE SOPORTAN LA INFORMACIÓN PROPIA DE LA ENTIDAD

3. Información relacionada con la contratación derivada

(Este aparte sólo debe diligenciarse en el evento de existir contratación derivada. Se debe allegar la relación de la misma y el estado que reporte la entidad que adelante la contratación derivada en caso que no sea directamente el IDIGER O

El supervisor certifica la existencia de contratación derivada del Contrato (Convenio) No. _____ de ____, consistente en _____ (cantidad) contratos, suscritos por _____ (contratante), con el fin de _____ (objeto). De igual manera allega relación de dicha contratación, en _____ folios, en la cual se identifica el número de contrato, la fecha de suscripción, el contratista, el objeto, la duración, el valor, observaciones generales y la certificación expresa del Contratante de que dicha contratación derivada se encuentra finalizada y/o liquidada, y de que todos sus contratistas se encuentran a paz y salvo por todo concepto.

4. Certificaciones para pagos suscritas por el supervisor

Periodo certificado	Fecha de certificación	Valor pagado	Observaciones
PAGO 01: 19 DE DICIEMBRE 2025 - 08 DE ABRIL 2026	14 DE ABRIL DE 2026	**$10.204.250**	FACTURA SGFE104
PAGO 02: 09 DE ABRIL 2026 - 18 DE ABRIL 2026	07 DE MAYO DE 2026	**$10.204.250**	

5. Pagos Efectuados

Número de pago/desembolso	Valor de desembolso (SEGÚN FORMA PACTADA)	Fecha y número de la orden de pago correspondiente	Observaciones (si el valor pagado fue diferente al pactado en la minuta, describir breve justificación, descuentos y concepto de los mismos)
PAGO 01	**$10.204.250**	OP 2501 DEL 22 DE ABRIL DE 2026	
TOTALES	**$ 10.204.250,00**		

6. Descuentos/Liberaciones/Reducciones al valor (si aplica)

Fecha Descuento/Liberación/Reducción	Valor Descuento/Liberación/Reducción	Concepto Descuento/Liberación/Reducción
TOTAL		

7. Reintegros efectuados (si aplica)

Fecha reintegro	Valor reintegro	Comprobante reintegro	Concepto reintegro

8. Garantías

Amparos	Compañía aseguradora	No. de póliza	Vigencia			
			Desde (Día/ mes/ año)	hasta (Día/ mes/ año)	Fecha aprobación (Día/ mes/ año	Valor del amparo
CUMPLIMIENTO DEL CONTRATO	SEGUROS DEL ESTADO SA	14-44-101251791	17/12/2025	17/10/2026	19/12/2025	4.081.700,00
PAGO DE SALARIOS,PRESTACIONES SOCIALES E INDEMNIZACIONES LABORALES			17/12/2025	17/04/2029	19/12/2025	2.040.850,00
CALIDAD DEL SERVICIO			17/12/2025	17/10/2026	19/12/2025	4.081.700,00

MODIFICACIÓN 1

Amparos	Compañía aseguradora	No. de póliza	Vigencia			
			Desde (Día/ mes/ año)	hasta (Día/ mes/ año)	Fecha aprobación (Día/ mes/ año	Valor del amparo

Si se presentan más prórrogas, incluir más filas para éstas.

9. Seguimiento a matriz de riesgos

Luego del seguimiento detectó alguno con alta probabilidad de ocurrencia?	Si		No	X

Registre cual(es) riesgo(s) detectó con alta probabilidad de ocurrencia:

Observaciones adicionales:

A

	INFORME PERIÓDICO DEL SUPERVISOR (Para Contratos diferentes la prestación de servicios profesionales y de apoyo a la gestión)	**Código:** GC-FT-65 **Versión: 3** **Página:** 1 de 1 **Vigente Desde:** 23/11/2021

1. Datos generales

Número del Contrato o Convenio	IDIGER 295-2025							**Fecha suscripción contrato o convenio::**	17/12/2025
Tipo de contrato	MINIMA CUANTIA							**Nombre o Razón Social del Contratista:**	GIGA SOURCE TECHNOLOGY DE COLOMBIA SAS
Plazo de Ejecución (meses)	4 MESES							**Número de Cédula o NIT:**	900.702.873-0
Periodo del Informe:	9	4	2026	al	18	4	2026	**Nombre del Representante Legal:** **(Quien en tenga la facultad en el periodo)**	WILMAR DÍAZ RODRÍGUEZ
Interventor (si Aplica)	NO APLICA							**Número de Cédula o NIT:** **Nombre del Representante Legal:** **(Quien en tenga la facultad en el periodo)**	80.854.925 de Bogotá DC
Cargo del Supervisor (1) del IDIGER (según cláusula de supervisión del contrato/convenio)	JEFE DE OFICINA TICS (SUPERVISION TEMPORAL DELEGADA)							**Nombre Supervisores de otras entidades (cooperantes) - (Si aplica)**	NO APLICA
Cargo del Supervisor (2) del IDIGER (según cláusula del supervisor del contrato/convenio) Si Aplica	NO APLICA							**Cargos supervisores de otras entidades (Si Aplica)**	NO APLICA
Cargo Apoyo a la Supervisión del IDIGER	NO APLICA								

Objeto Contractual:

ADQUIRIR SOPORTE, MANTENIMIENTO Y ASISTENCIA TÉCNICA PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL IDIGER, PARA GARANTIZAR LA FUNCIONALIDAD Y ACCESIBILIDAD DE LOS SISTEMAS QUE SOPORTAN LA INFORMACIÓN PROPIA DE LA ENTIDAD

10 REFERENTE AL SEGUIMIENTO TÉCNICO: Información de seguimiento técnico del contrato, así como análisis respecto del cronograma o avance inicialmente pactado (evidencia de posibles retrasos, vicisitudes, dificultades), (estado % de terminados, en ejecución, pendientes por ejecutar, pagos pendientes y/o en curso etc.).

CONTRATO DE MINIMA CUANTIA No. IDIGER 295 DE 2025

OBJETO: ADQUIRIR SOPORTE, MANTENIMIENTO Y ASISTENCIA TÉCNICA PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL IDIGER, PARA GARANTIZAR LA FUNCIONALIDAD Y ACCESIBILIDAD DE LOS SISTEMAS QUE SOPORTAN LA INFORMACIÓN PROPIA DE LA ENTIDAD

Fecha de inicio: 19/12/2025 **Fecha de terminación:** 18/04/2026

Valor del contrato: $20.408.500

PAGO 01: FACTURA SGFE104 POR $10.204.250 Correspondiente al periodo del 19 de diciembre 2025 al 08 de abril 2026 (PAGADA EN ABRIL 2026)

Durante el periodo certificado se recibio atención a las siguientes solicitudes:

1. Revisión y ajustes de configuracion para la estabilizacion de la red de alta velocidad SAN (Fibre channel)
2. Implementacion de una solucion syslog con el objetivo de centralizar los logs de la infraestructura

Así mismo se implemento el monitoreo en tiempo real de las aplicaciones criticas de la entidad, el cual permanecera activo durante la vigencia del contrato.

Saldo pendiente de pago: $10.204.250

PAGO 02: FACTURA SGFE106 POR $10.204.250 Correspondiente al periodo del 9 de abril 2026 al 18 de abril 2026 (A PAGARSE EN MAYO 2026)

Durante el periodo certificado se recibio atención a las siguientes solicitudes:

1. Migracion a la Red de gestion y cambio de credenciales del Switch SAN IBM 2498 que hace parte de la red de almacenamiento de alta velocidad (Fibre channel)
2. Implementacion del componente DELL CEE (como parte del sistema de auditoria de la NAS)
3. Diagnostico del Servidor Oracle Sun SPARC T4 luego de la falla presentada

11. Verificación Pago al Sistema de Seguridad Social Integral y Parafiscales.

La supervisión y/o interventoría verifico el cumplimiento del contratista de sus obligaciones con el Sistema de Seguridad Social Integral y parafiscales conforme a los documentos (planillas, pagos, certificaciones) allegados por el contratista en cumplimiento de lo establecido en el artículo 50 de la ley 789 de 2002: "(....) verificar y dejar constancia del cumplimiento de las obligaciones del contratista frente a los aportes mencionados durante toda su vigencia, estableciendo una correcta relación entre el monto cancelado y las sumas que debieron haber sido cotizadas. (...) Cuando la contratación se realice con personas jurídicas, se deberá acreditar el pago de los aportes de sus empleados, a los sistemas mencionados mediante certificación expedida por el revisor fiscal(...)" Nota: Esta verificación se hará cada vez que exista pago a favor del contratista, dependerá de la forma de pago pactada.

Fecha emisión de Informe

7	5	2026

Firma

CLAUDIA MARCELA LADINO HERRERA (SUPERVISION TEMPORAL DELEGADA)

JEFE DE OFICINA TICS

Firma

Nombre Apoyo a la Supervisión (Componente Técnico: en caso que haya sido designado) o el que aplique

Cargo o Contrato

Firma

Nombre Apoyo a la Supervisión (Componente Financiero: en caso que haya sido designado) o el que aplique

Cargo o Contrato

Firma

Nombre Apoyo a la Supervisión (Componente Jurídico: en caso que haya sido designado)) o el que aplique

Cargo o Contrato

Nota: Si se requiere la firma de más personas que intervinieron en el ejercicio de supervisión, se podrán incluir.

INFORME FALLA SERVIDOR ORACLE SVRFOPAEAPPN1

GSTCOL

NIT 900702873-0
Giga Source Technology de Colombia

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S. Empresa que provee e implementa soluciones de ingeniería Tecnológica, estamos comprometidos con la satisfacción del cliente, brindado el soporte ofreciendo un servicio ágil y eficiente. Contamos con un equipo de trabajo con experiencia profesional que implementa sistemas de Virtualización con HyperV Vmware Citrix, administración de plataformas tecnológicas: almacenamiento, redes, servidores, librerías, firewall, librerías, sistemas operativos, switch, redes de voz y datos, asistencia técnica, entre otras.

Entidad: IDIGER
Servidor: SVRFOPAEAPPN1 (Oracle Sun SPARC T4 — 2U, 8 discos)
Interfaz de gestión: Oracle ILOM v3.0.16.9.b r77667
Clasificación: Incidente Crítico de Infraestructura
Tiempo ejecutado: 15 Horas

Resumen Ejecutivo

El presente documento describe el análisis técnico, diagnóstico y acciones correctivas realizadas sobre el servidor Oracle SVRFOPAEAPPN1, equipo que aloja la aplicación SIRE del IDIGER. El servidor entró en estado de alarma crítica causando la indisponibilidad total del servicio. La causa raíz identificada corresponde a una falla en el suministro de voltaje del chasis (fault.chassis.voltage.fail), específicamente asociada a la tarjeta madre principal (Motherboard /SYS/MB), cuyo sensor de voltaje V_+3V3_VDD reportó lecturas fuera del rango operativo permitido.
Adicionalmente, el proceso de atención se vio dificultado por la ausencia de credenciales de acceso al sistema de gestión remota ILOM (Integrated Lights Out Manager), lo que obligó a realizar un procedimiento de recuperación de acceso mediante intervención física directa en el servidor. Una vez restaurado el acceso, se ejecutaron las acciones de diagnóstico y corrección pertinentes, logrando restablecer la operación del servidor.

Identificación del Equipo

Parámetro	Valor
Hostname	SVRFOPAEAPPN1-ilom
Tipo de servidor	Oracle Sun SPARC T4 — 2U, 8 disks, rev 5
Descripción FRU MB	PCA,MB,SPARC_T4-1
Part Number MB	7047134
Serial Number MB	465769T+1246BW0NR2
Firmware ILOM	Version 3.0.16.9.b r77667
System Firmware	Sun System Firmware 8.2.2.c 2012/12/11
OpenBoot	4.34.2.a 2012/11/02
POST	POST 4.34.2 2012/10/04
Hypervisor	1.11.2.b 2012/11/02
MAC Address SP	00:10:E0:23:06:F3
Procesador SP	AST2200 / ARM926EJ-S

Descripción Detallada de la Falla Principal

Falla Activa al Momento de la Atención
Al acceder al sistema de gestión ILOM y ejecutar el comando de diagnóstico fmadm faulty dentro del shell de gestión de fallos (/SP/faultmgmt/shell), se identificó la siguiente falla activa:

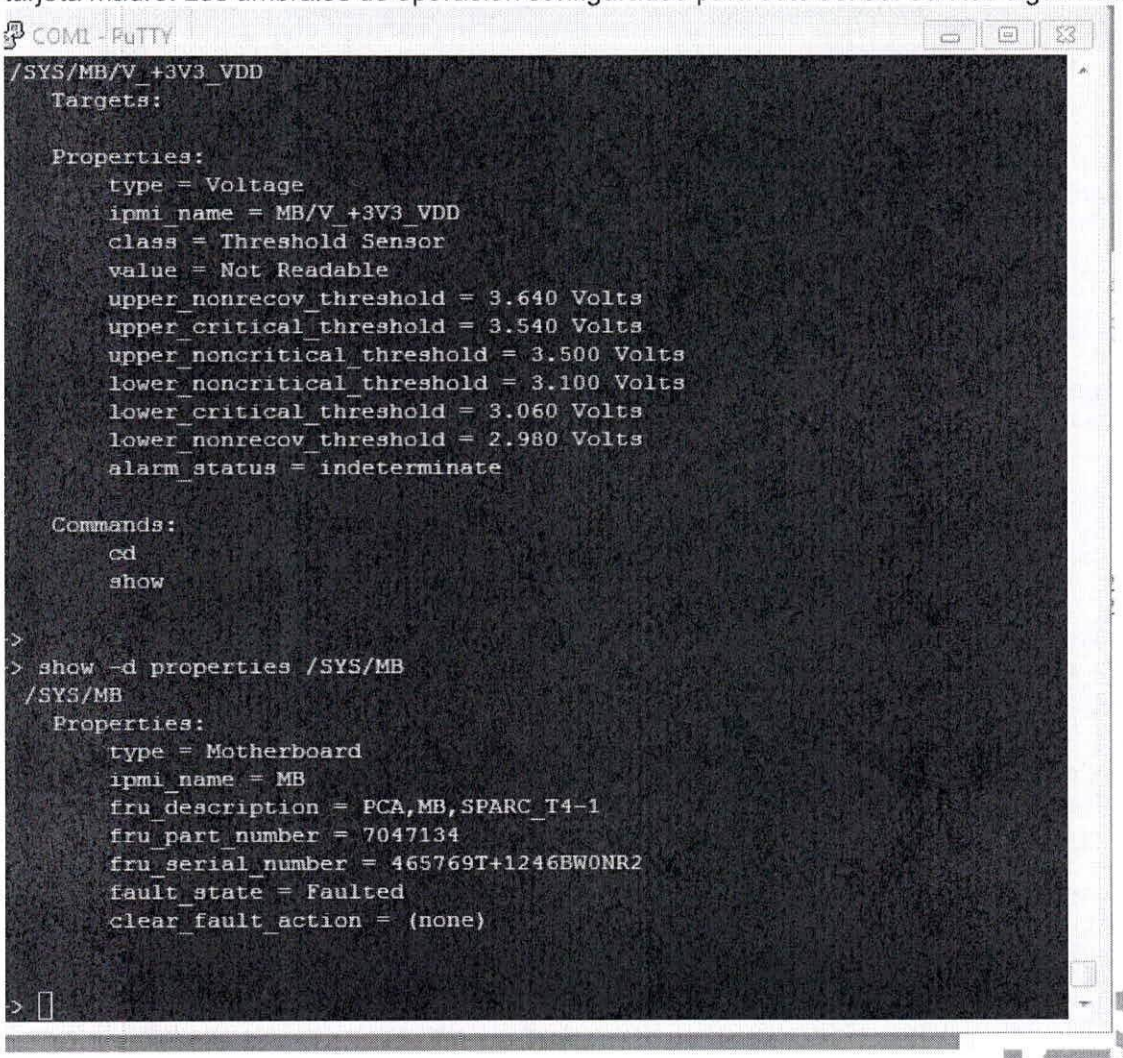
.

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

Campo	Detalle
Fecha / Hora registro	2026-04-09 / 14:08:11
UUID	e69b59bc-0833-e82b-aa00-a1d12a8ad540
Código de falla (msgid)	SPT-8000-DH
Clase de falla	fault.chassis.voltage.fail
FRU afectada	/SYS/MB — Tarjeta Madre Principal
Part Number	7047134
Serial Number	465769T+1246BW0NR2
Severidad	Crítica
Estado de falla MB	fault_state = Faulted
Acción de limpieza	clear_fault_action = (none)

Análisis Técnico de la Falla de Voltaje

La falla fault.chassis.voltage.fail (código SPT-8000-DH) indica que el suministro de voltaje del chasis operó fuera del rango permisible definido en el sensor MB/V_+3V3_VDD de la tarjeta madre. Los umbrales de operación configurados para este sensor son los siguientes:



GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

Umbral	Valor
Upper Non-Recoverable Threshold	3.640 Volts
Upper Critical Threshold	3.540 Volts
Upper Non-Critical Threshold	3.500 Volts
Lower Non-Critical Threshold	3.100 Volts
Lower Critical Threshold	3.060 Volts
Lower Non-Recoverable Threshold	2.980 Volts
Valor leído al momento de la falla	Not Readable (No legible)
alarm_status	indeterminate

El hecho de que el sensor reportara el valor como "Not Readable" con alarm_status = indeterminate es técnicamente significativo: no se trata simplemente de un voltaje fuera de rango, sino de una pérdida total de la capacidad de lectura del sensor, lo que indica una condición severa en los circuitos de medición o en los reguladores de voltaje integrados en la tarjeta madre /SYS/MB. Esta condición activó la respuesta automática del sistema ILOM, que procedió a apagar el servidor y bloquear su encendido, dado que el firmware considera que el sistema no es seguro para operar sin una confirmación explícita de que la falla ha sido resuelta.
La propiedad clear_fault_action = (none) registrada en /SYS/MB confirma que la falla no puede ser limpiada automáticamente por el sistema, sino que requiere intervención manual del administrador.

Impacto Operacional

Dado que la falla fue clasificada como crítica y el ILOM bloqueó el encendido del sistema, el impacto directo fue:

- Indisponibilidad total del servidor SVRFOPAEAPPN1
- Interrupción del servicio de la aplicación SIRE del IDIGER
- Imposibilidad de encendido remoto hasta resolver la falla
- El LED de servicio requerido del chasis fue activado, indicando visualmente la condición de alarma

Problema de Acceso — Ausencia de Credenciales ILOM

Situación Inicial
Al momento de recibir el reporte de alarma por parte del IDIGER, el equipo de infraestructura no contaba con las credenciales de acceso al ILOM del servidor SVRFOPAEAPPN1. Esto generó una demora adicional en el proceso de atención del incidente, ya que no fue posible iniciar el diagnóstico de manera inmediata mediante acceso remoto.

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

Intentos de Acceso Fallidos
Se realizaron múltiples intentos de autenticación con diferentes usuarios y credenciales estándar, todos sin éxito:

Usuario intentado	Resultado
root	Login incorrect
soporte	Login incorrect
oasfopae	Login incorrect
changeme	Login incorrect
roor	Login incorrect
port	Login incorrect
default	Requiere botón físico de presencia — no detectado inicialmente

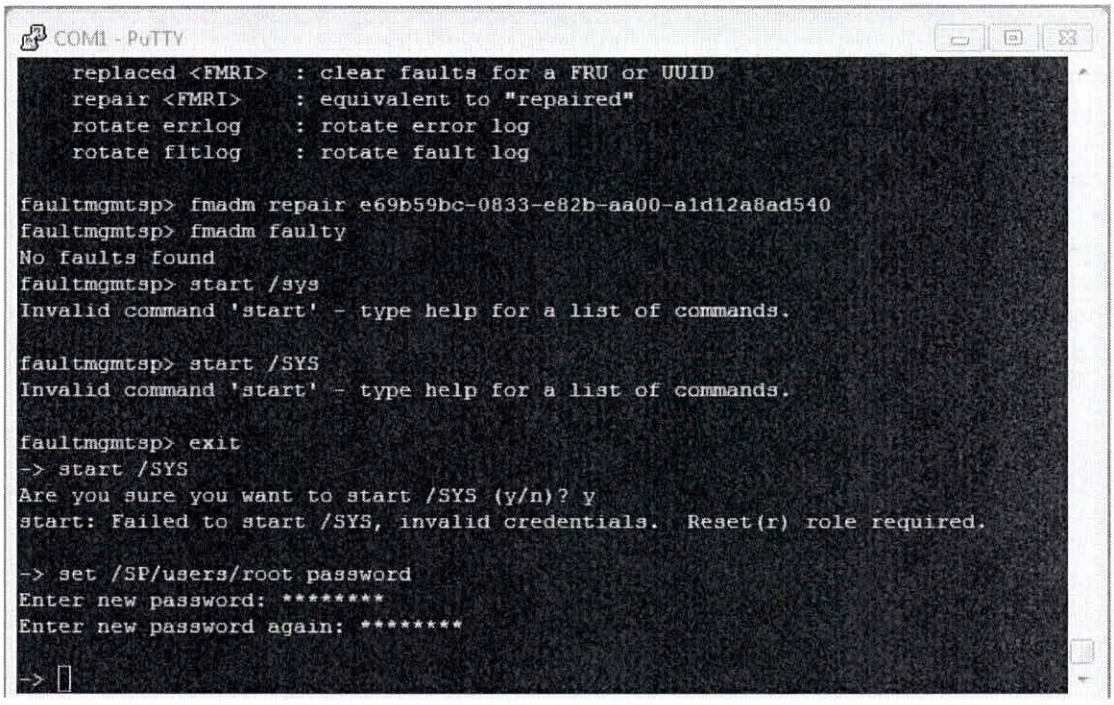
El usuario default en servidores Oracle ILOM es una cuenta especial de recuperación que requiere la pulsación del botón físico de presencia ubicado en el panel frontal o posterior del servidor como mecanismo de seguridad adicional para prevenir accesos no autorizados.

Procedimiento de Recuperación de Acceso
Ante la imposibilidad de acceder remotamente, se procedió a realizar la siguiente intervención física directa sobre el servidor:

1. Se realizó un reset físico del Service Processor (SP) desde la parte posterior del servidor.
2. Durante el proceso de reinicio del ILOM, se utilizó el usuario default y se presionó el botón físico de presencia del servidor, cumpliendo el requisito de seguridad del sistema.
3. Una vez dentro del ILOM con el usuario default, se procedió a restablecer la contraseña del usuario root mediante el siguiente comando ejecutado en la CLI del ILOM:

```
-> set /SP/users/root password
Enter new password: ********
Enter new password again: ********
```

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S



Se verificó el acceso exitoso con el usuario root y la nueva contraseña establecida, obteniendo acceso completo con el rol administrativo requerido (Reset(r) role).

Historial de Fallas del Servidor

El análisis de los logs del ILOM reveló un historial significativo de fallas de hardware en este servidor, que se remonta al año 2015. Este historial es relevante para comprender la naturaleza progresiva y recurrente de los problemas eléctricos del equipo:

Fecha	Código	Clase de Falla	FRU Afectada	Severidad
2015-11-12 12:23	SPT-8000-MJ	fault.chassis.power.fail	/SYS/PS0	Crítica
2017-04-26 12:41	SUN4V-8002-US	fault.sp.failed	/SYS/MB/SP	Crítica
2018-09-15 09:09	SPT-8000-5X	fault.chassis.env.power.loss	/SYS/PS1	Mayor
2018-09-15 09:11	SPT-8000-MJ	fault.chassis.power.fail	/SYS/PS1	Crítica
2020-06-17 17:17	SPT-8000-5X	fault.chassis.env.power.loss	/SYS/PS1	Mayor
2020-06-17 17:18	SPT-8000-MJ	fault.chassis.power.fail	/SYS/PS1	Crítica

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

2026-04-09 14:08	SPT-8000-DH	fault.chassis.voltage.fail	/SYS/MB	Crítica

Interpretación del Historial

El patrón de fallas observado es técnicamente preocupante. Las fallas iniciaron en la fuente de poder PS0 en 2015 y escalaron a fallas recurrentes en PS1 durante 2018 y 2020. La falla del año 2026, sin embargo, representa una escalada significativa: ya no se trata de las fuentes de poder como componentes aislados, sino que la condición de inestabilidad eléctrica alcanzó la tarjeta madre principal (/SYS/MB), afectando directamente los reguladores de voltaje integrados en la placa. Esto sugiere que el suministro eléctrico inestable y degradado a lo largo de los años ha generado daño acumulativo en los componentes de la tarjeta madre.

Acciones de Diagnóstico y Corrección Ejecutadas

Ingreso al Shell de Gestión de Fallos

```
-> start /SP/faultmgmt/shell
Are you sure you want to start /SP/faultmgmt/shell (y/n)? y
faultmgmtsp>
```

Diagnóstico de Fallas Activas

```
faultmgmtsp> fmadm faulty
```

Resultado: Se identificó la falla activa SPT-8000-DH en /SYS/MB.

Ejecución de Reparación

```
faultmgmtsp> fmadm repair e69b59bc-0833-e82b-aa00-a1d12a8ad540
faultmgmtsp> fmadm faulty
No faults found
```

La limpieza de la falla fue exitosa. El comando fmadm repair marca la falla como atendida en el registro del ILOM, permitiendo al sistema proceder con el encendido.

Encendido del Servidor

```
-> start /SYS
Are you sure you want to start /SYS (y/n)? y
Starting /SYS
```

El sistema inició correctamente.

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S.

Verificación de Consola del Host

```
-> start /HOST/console
Are you sure you want to start /HOST/console (y/n)? y
Serial console started.
```

Se verificó acceso exitoso a la consola serial del sistema operativo host.

Estado del Sistema Post-Intervención

Componente	Estado
ILOM	Operativo — acceso restaurado con credenciales restablecidas
Fallas activas ILOM	Ninguna (No faults found)
Sistema /SYS	Encendido y operando correctamente
Host /HOST	Iniciado
Consola serial /HOST/console	Accesible
Credenciales root ILOM	Restablecidas y documentadas
LED de servicio requerido	Apagado tras corrección de falla

Hallazgos Adicionales

Durante la intervención se identificaron las siguientes condiciones secundarias que requieren atención:

- **Pérdida de hora del RTC:** El reloj del Service Processor registró fecha 1999-12-31 al reiniciar, lo que indica que la batería CMOS del SP está agotada y no retiene la hora cuando el servidor pierde alimentación. Esto afecta la confiabilidad de los timestamps en los registros de eventos.
- **Falla de interfaz eth1 del SP:** Durante el arranque del ILOM se registró el error Failed to bring up eth1, lo que indica que la segunda interfaz de red de gestión del Service Processor no está operativa, eliminando la redundancia de conectividad de gestión remota.
- **Versión de firmware obsoleta:** El firmware del servidor data del año 2012 (Image revision: 77667), lo que representa una brecha de seguridad significativa y una limitación en cuanto a correcciones de bugs y soporte del fabricante.
- **Estado fault_state = Faulted en /SYS/MB:** Aunque la falla fue limpiada a nivel de registros ILOM, el componente físico (tarjeta madre) continúa siendo el mismo que presentó la falla. La limpieza con fmadm repair no implica que el hardware haya sido reparado, sino que el sistema fue habilitado para operar nuevamente.

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

Diagnóstico Definitivo

La causa raíz del incidente es una falla en el suministro de voltaje de la tarjeta madre principal (/SYS/MB) del servidor SVRFOPAEAPPN1, identificada bajo el código SPT-8000-DH (fault.chassis.voltage.fail). La tarjeta madre presentó una condición de voltaje fuera de rango en el riel V_+3V3_VDD, con pérdida total de lectura del sensor, lo que activó el mecanismo de protección del ILOM y causó el apagado forzado del servidor.
Esta falla es el resultado de una degradación progresiva del subsistema eléctrico del servidor, evidenciada por el historial de fallas acumuladas en las fuentes de poder PS0 y PS1 desde el año 2015. La tarjeta madre /SYS/MB debe ser considerada para reemplazo, dado que:

1. Es el componente que presentó la falla crítica activa
2. El sensor de voltaje integrado en la placa perdió capacidad de lectura
3. Su fault_state fue registrado como Faulted por el sistema de diagnóstico del fabricante
4. El historial de inestabilidad eléctrica sostenida en el tiempo puede haber causado daño acumulativo en los circuitos integrados de la placa

Recomendaciones

1. **Reemplazo de la tarjeta madre /SYS/MB** (Part Number: 7047134): Dado que la falla crítica activa fue diagnosticada directamente en este componente y el sensor de voltaje integrado perdió capacidad de lectura, se recomienda gestionar con Oracle Support el reemplazo de este componente como acción correctiva prioritaria.
2. **Reemplazo de la fuente de poder PS1** (Part Number: 300-2304, Serial: C40002): Este componente registra fallas críticas recurrentes desde septiembre de 2018, constituyendo un factor de riesgo permanente para la estabilidad del servidor.
3. **Revisión y reemplazo preventivo de la fuente PS0** (Part Number: 300-2304): Presenta falla registrada desde noviembre de 2015. Su condición actual es desconocida y representa un riesgo latente.
4. **Custodia segura de credenciales ILOM:** Las credenciales de acceso al ILOM de todos los servidores críticos deben ser almacenadas en una bóveda de contraseñas institucional (PAM/CyberArk o equivalente), con procedimiento documentado de recuperación de emergencia, para evitar demoras en futuros incidentes.
5. **Reemplazo de batería CMOS del Service Processor:** La pérdida de hora del RTC al reiniciar indica batería agotada, lo que afecta la integridad de los registros de eventos del ILOM.
6. **Revisión de conectividad eth1 del SP:** Diagnosticar y corregir la falla de la segunda interfaz de red del Service Processor para restaurar la redundancia de gestión remota.
7. **Actualización de firmware:** Evaluar la actualización del firmware del servidor desde la versión 2012 (r77667) a la versión más reciente disponible de Oracle para el modelo SPARC T4, con el fin de incorporar correcciones de seguridad y estabilidad.

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

8. **Implementar monitoreo proactivo:** Configurar alertas tempranas en el ILOM mediante el módulo /SP/alertmgmt para notificar al equipo de infraestructura ante cualquier condición de umbral de voltaje, temperatura o falla de componentes, antes de que escale a un incidente crítico.
9. **Evaluación de obsolescencia del servidor:** Dado que el hardware data del año 2012 y ha acumulado múltiples fallas críticas en sus componentes principales, se recomienda iniciar una evaluación formal de reemplazo del servidor por un equipo con soporte activo del fabricante.

WILMAR DIAZ RODRIGUEZ
Gerente Administrativa y Proyectos.
wilmar.diaz@gstcol.com , proyectos@gstcol.com

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

INFORME CONFIGURACIÓN DE ACCESO CEE (NAS)

GSTCOL
NIT 900702873-0
Giga Source Technology de Colombia

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S. Empresa que provee e implementa soluciones de ingeniería Tecnológica, estamos comprometidos con la satisfacción del cliente, brindado el soporte ofreciendo un servicio ágil y eficiente. Contamos con un equipo de trabajo con experiencia profesional que implementa sistemas de Virtualización con HyperV Vmware Citrix, administración de plataformas tecnológicas: almacenamiento, redes, servidores, librerías, firewall, librerías, sistemas operativos, switch, redes de voz y datos, asistencia técnica, entre otras.

Entidad contratante: Instituto Distrital de Gestión de Riesgos y Cambio Climático IDIGER NIT 800.154.275-1
Contrato IDIGER-295-2025
Infraestructura evaluada: Plataforma de almacenamiento NAS Dell PowerStore 1000
Componentes configurados: Dell CEE (Common Event Enabler) / Event Publisher PowerStore
Equipo de almacenamiento: Dell PowerStore 1000 DPE
Tiempo ejecutado: 20 Horas

Introducción

En el marco de los requerimientos institucionales del IDIGER orientados a garantizar la trazabilidad y auditoría de la actividad sobre los recursos de almacenamiento compartido, se llevó a cabo la configuración del componente Common Event Enabler (CEE) de Dell como parte del sistema de auditoría de actividad sobre la plataforma de almacenamiento NAS PowerStore 1000. Esta actividad representa la fase de integración entre el sistema de almacenamiento institucional y la plataforma de centralización de logs Graylog, previamente instalada y configurada en el servidor VLUBPSLOG01.

El Common Event Enabler (CEE) es un componente de software desarrollado por Dell Technologies que actúa como agente intermediario entre los sistemas de almacenamiento NAS de Dell y las plataformas externas de registro, auditoría y seguridad de la información. Su función principal consiste en recibir los eventos de actividad sobre archivos generados por el NAS Server del PowerStore tales como creación, modificación, eliminación, apertura y cierre de archivos compartidos mediante el protocolo SMB y retransmitirlos hacia los sistemas de destino configurados, en este caso el servidor Graylog. Esta capacidad de auditoría es fundamental para que la entidad pueda dar cumplimiento a los requerimientos de trazabilidad sobre el acceso y manipulación de información almacenada en la plataforma institucional, identificando en tiempo real quién accede a qué recursos, desde qué equipo y en qué momento.

La implementación del sistema de auditoría implica la correcta configuración y operación coordinada de tres componentes tecnológicos: el NAS Server del Dell PowerStore como generador de eventos, el servidor CEE (SRVSYSLOG02) como colector y procesador intermedio de dichos eventos, y el servidor Graylog (VLUBPSLOG01) como destino final de almacenamiento, indexación y visualización. Las actividades descritas en el presente informe corresponden a la instalación del componente CEE, su configuración técnica, la definición del publicador de eventos en el PowerStore y las pruebas de validación realizadas para verificar la correcta operación del flujo de auditoría.

Descripción del flujo de auditoria

El sistema de auditoría de actividad sobre la NAS PowerStore opera bajo un esquema de tres capas que garantiza la captura, transporte y almacenamiento de cada evento generado sobre los recursos de almacenamiento compartido. Comprender este flujo es fundamental para dimensionar el alcance de la configuración realizada y el estado actual de la implementación.

En la primera capa, el NAS Server del Dell PowerStore actúa como el origen de los eventos. Cuando un usuario o sistema accede a un archivo compartido mediante el protocolo SMB

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S.

ya sea para abrirlo, modificarlo, eliminarlo o crear uno nuevo el NAS Server genera internamente un evento de auditoría que describe la operación realizada, el recurso afectado, el usuario que ejecutó la acción y el momento en que ocurrió. Este mecanismo de generación de eventos es nativo del PowerStore y se activa a través de la funcionalidad denominada Event Publishing, la cual debe ser configurada para apuntar hacia el servidor CEE como destino de publicación.

En la segunda capa, el servidor SRVSYSLOG02 con el componente CEE instalado actúa como receptor y procesador intermedio de los eventos publicados por el PowerStore. El servicio EMC CAVA (Common Anti-Virus Agent), que forma parte del paquete CEE de Dell, escucha en el puerto TCP 12228 mediante el protocolo VCAPS (Value-Added Copy Architecture and Protocol Suite) y recibe los eventos enviados por el NAS Server. Una vez recibidos, el CEE los procesa y los retransmite en el formato adecuado hacia el servidor Graylog, cerrando así el ciclo de transporte del evento desde el origen hasta el sistema de registro.

En la tercera capa, el servidor Graylog (VLUBPSLOG01) recibe los eventos procesados por el CEE a través del puerto TCP 12201 mediante el protocolo GELF, los indexa en el motor OpenSearch y los pone a disposición del equipo de TI del IDIGER a través de la interfaz web de administración para su consulta, análisis y correlación en tiempo real.

Instalación del componente CEE en Windows Server 2025

La instalación del componente Common Event Enabler (CEE) de Dell se realizó sobre el servidor SRVSYSLOG02 con sistema operativo Windows Server 2025, utilizando el paquete oficial de instalación proporcionado por Dell Technologies para entornos Windows. Este servidor fue provisto por el IDIGER específicamente para alojar el componente colector CEE, con el usuario de acceso idiger\servicedell habilitado para las tareas de administración e instalación de software.

El proceso de instalación del CEE en entornos Windows implica la ejecución del instalador oficial de Dell, el cual despliega los servicios necesarios para la operación del agente CAVA y registra los componentes de comunicación requeridos para la interacción con el NAS Server del PowerStore. Durante la instalación se configuraron los parámetros de inicialización del servicio, estableciendo el tipo de inicio como automático para garantizar que el agente se encuentre disponible ante cualquier reinicio del servidor sin intervención manual.

Una vez completada la instalación, se procedió con la configuración del endpoint de destino de los eventos procesados por el CEE. Esta configuración se realiza directamente en el registro de Windows, en la ruta HKLM\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration, donde se define la dirección del servidor Graylog y el puerto de recepción de eventos GELF (TCP 12201) como destino hacia el cual el CEE debe retransmitir los eventos de auditoría recibidos desde el PowerStore. Esta entrada de registro establece el vínculo lógico entre el colector CEE y el servidor de centralización de logs, completando así la configuración del segundo eslabón de la cadena de auditoría.

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

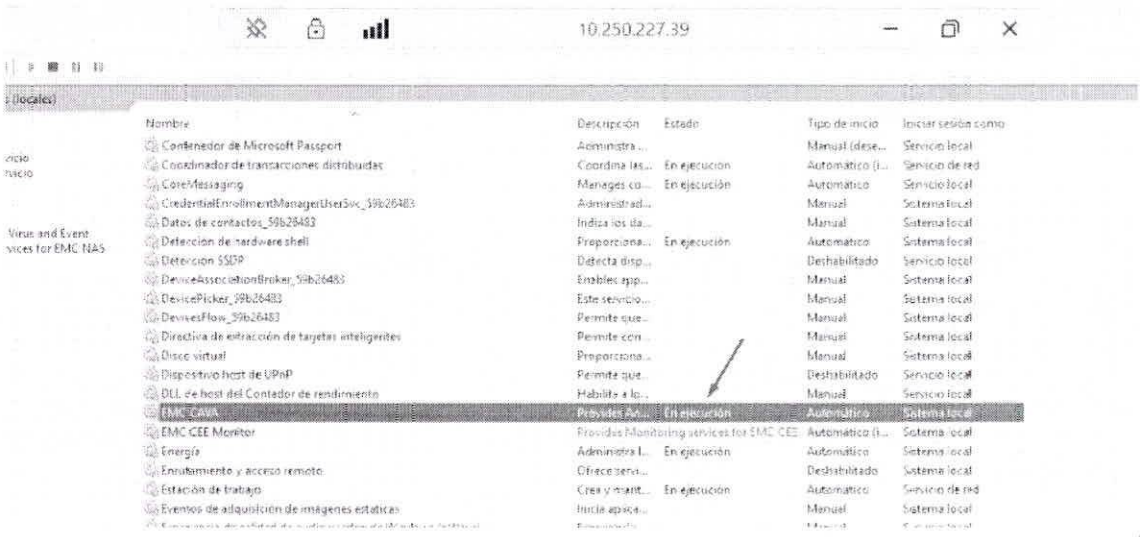


Imagen 1 Captura del Administrador de servicios de Windows (services.msc) en SRVSYSLOG02 mostrando el servicio "EMC CAVA" en estado "En ejecución" con tipo de inicio automático.

Posterior a la configuración del registro, se realizó la verificación del estado operativo del servicio EMC CAVA mediante el Administrador de servicios de Windows (services.msc), confirmando que el servicio se encontraba en estado "En ejecución". Adicionalmente, se validó la escucha activa en el puerto TCP 12228 mediante el comando netstat ejecutado desde la consola de administración del servidor, el cual confirmó que el proceso CAVA estaba correctamente enlazado al puerto de recepción de eventos del PowerStore.

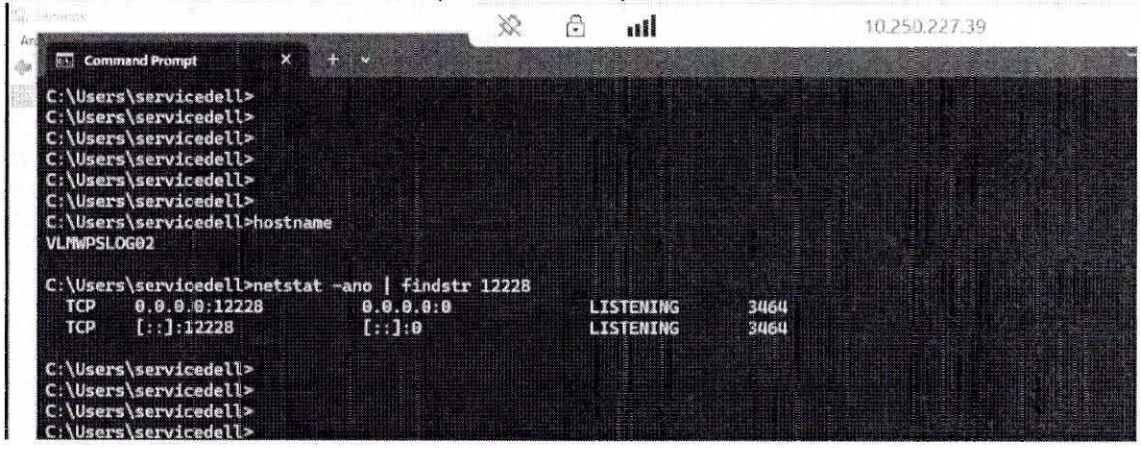


Imagen 2 Captura de CMD o PowerShell en SRVSYSLOG02 mostrando el resultado del comando `netstat -ano | findstr :12228` con el puerto TCP 12228 en estado LISTENING.

Configuración del Event Publisher en el PowerStore

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

La configuración del publicador de eventos en el Dell PowerStore constituye el eslabón inicial de la cadena de auditoría y es la responsable de activar el mecanismo de envío de eventos desde el NAS Server hacia el servidor CEE. Esta configuración se realiza desde la consola de administración web del PowerStore y comprende la definición de un Event Publishing Pool y la selección de los tipos de eventos que serán publicados.

El Event Publishing Pool es el objeto de configuración que agrupa las conexiones hacia los servidores CEE de destino y define los parámetros del protocolo de comunicación. Para la implementación del sistema de auditoría del IDIGER se creó el pool denominado "CEE-WINDOWS-Server-2025", en el cual se registró el servidor SRVSYSLOG02 como destino de publicación de eventos, especificando el protocolo HTTP sobre el puerto 12228 como canal de comunicación entre el PowerStore y el colector CEE. Esta configuración sigue las especificaciones del Capítulo 7 de la guía oficial Dell PowerStore Configuring SMB, que describe el procedimiento estándar para la integración con CEPA (Common Event Publishing Agent) en escenarios de auditoría de archivos.

En cuanto a la selección de eventos, se habilitaron tanto los pre-eventos como los post-eventos requeridos para la auditoría completa de las operaciones sobre archivos SMB. Los pre-eventos corresponden a las notificaciones que el NAS Server envía al CEE antes de ejecutar una operación sobre un archivo, mientras que los post-eventos corresponden a las notificaciones enviadas una vez que la operación ha sido completada exitosamente. La habilitación de ambos tipos de eventos garantiza una trazabilidad completa del ciclo de vida de cada operación sobre los recursos de almacenamiento compartido.

Adicionalmente, se realizaron pruebas con los dos métodos de autenticación disponibles en el PowerStore para la comunicación con el CEE: el método "Using SMB Server Account", que utiliza la cuenta de servicio del NAS Server para autenticarse ante el CEE, y el método "Using Custom User Account", que utiliza credenciales específicas definidas por el administrador. Ambos métodos fueron evaluados durante el proceso de validación con el objetivo de identificar cuál de ellos garantiza la comunicación estable entre el PowerStore y el servidor SRVSYSLOG02 en el entorno específico del IDIGER.

Pruebas de validación realizadas

Una vez completada la configuración de los componentes CEE en SRVSYSLOG02 y del Event Publisher en el PowerStore, se procedió con la ejecución de un conjunto de pruebas de validación orientadas a verificar la correcta operación del flujo de auditoría de extremo a extremo. Estas pruebas abarcaron la verificación del estado de cada componente de forma individual y la validación de la comunicación entre ellos.

En el servidor SRVSYSLOG02, las pruebas confirmaron que el servicio EMC CAVA se encontraba activo y escuchando en el puerto TCP 12228, y que la configuración del registro de Windows apuntaba correctamente al servidor Graylog como destino de los eventos procesados. En el PowerStore, se verificó desde la consola de administración que el Event Publishing Pool se encontraba en estado activo y que los parámetros de conexión hacia el

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S.

servidor CEE estaban correctamente definidos. Las pruebas de conectividad a nivel de red entre los segmentos de almacenamiento y los servidores de monitoreo fueron gestionadas con el equipo del IDIGER, confirmando la habilitación de los canales de comunicación requeridos en el dispositivo Fortinet, con NAT deshabilitado en la regla de firewall correspondiente para garantizar la correcta autenticación del protocolo VCAPS.

Durante las pruebas de validación del flujo completo de eventos desde el NAS Server del PowerStore hasta la consola de Graylog se identificó que la conexión no se establecía de forma estable. A pesar de que todos los componentes individuales mostraban estado operativo correcto (servicio CAVA activo, puerto 12228 en escucha, Event Publishing Pool configurado, reglas de firewall habilitadas), los eventos de auditoría del PowerStore no estaban llegando de manera consistente al servidor CEE. Ante esta situación, el equipo técnico de GSTCOL procedió con el análisis detallado de los logs de cada componente y con el escalamiento formal del caso al soporte técnico de Dell Technologies para descartar factores internos del equipo de almacenamiento como causa del comportamiento observado.

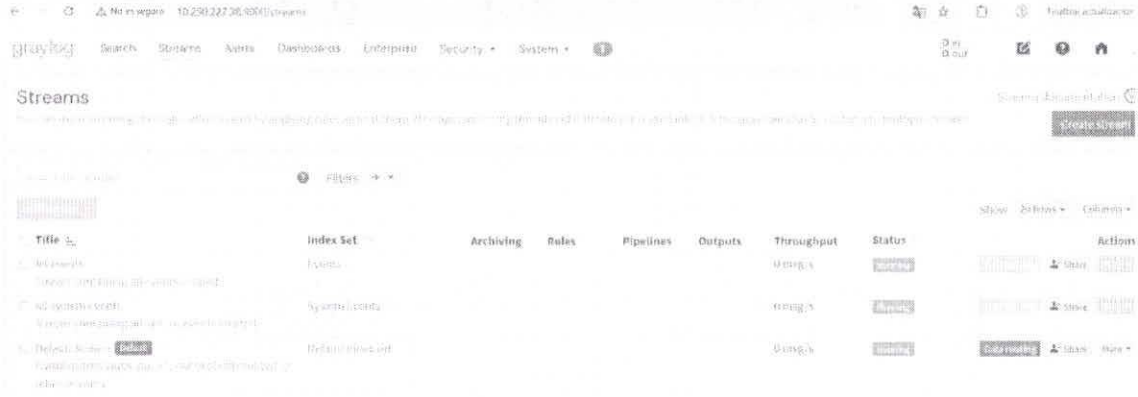


Imagen 3 Captura de la consola de Graylog (Search o Streams) mostrando el estado actual de recepción de eventos, evidenciando la situación identificada durante las pruebas de validación.

Escalamiento a soporte Dell Technologies Caso SR# 224421773

Dado que las pruebas de validación del flujo completo de auditoría no arrojaron los resultados esperados a pesar de la correcta configuración de todos los componentes, el caso fue escalado formalmente al soporte técnico de Dell Technologies, asignado al Ing. Gustavo Wong, bajo el número de caso SR# 224421773 para el equipo PowerStore 1000 DPE con Service Tag 4ZV0QM3. Como parte del proceso de escalamiento, el equipo técnico de GSTCOL envió al soporte de Dell la documentación técnica detallada del proceso de validación y configuración realizado, incluyendo evidencias del estado de cada componente, y cargó el archivo de logs del PowerStore mediante la opción "Send to Support" disponible en la consola de administración del equipo, conforme a las instrucciones del artículo de soporte referenciado por Dell (KB 133407).

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

Tras el análisis de la información suministrada, el soporte técnico de Dell Technologies confirmó que la configuración implementada dentro del PowerStore es técnicamente correcta y está alineada con las mejores prácticas del fabricante para la implementación del sistema de auditoría CEE. Dell identificó que los factores que condicionan la estabilización del flujo de eventos corresponden a condiciones del entorno de infraestructura que deben ser atendidas como parte de una fase de preparación previa a la puesta en marcha definitiva del sistema de auditoría.

Hallazgos técnicos identificados

El análisis técnico conjunto realizado por el equipo de GSTCOL y el soporte de Dell Technologies permitió identificar los siguientes hallazgos que inciden en la estabilización del sistema de auditoría:

El primero y más relevante corresponde a la versión de firmware del PowerStore actualmente instalada, la cual es una de las primeras versiones que soporta la funcionalidad de publicación de eventos NAS hacia el componente CEE. El soporte de Dell confirmó que versiones posteriores del firmware incorporan mejoras y correcciones específicas sobre esta funcionalidad que estabilizan significativamente el comportamiento del Event Publisher y la comunicación con el colector CEE. Esta condición explica el comportamiento intermitente observado durante las pruebas de validación, aun cuando la configuración de los componentes es correcta.

El segundo hallazgo corresponde a la compatibilidad de versiones entre el CEE instalado y el firmware del PowerStore. Dell recomendó verificar que la versión específica del paquete Common Event Enabler instalada en el servidor SRVSYSLOG02 sea plenamente compatible con la versión de firmware actual del PowerStore, ya que las matrices de compatibilidad entre estos dos componentes son estrictas y una incompatibilidad de versiones puede impedir el establecimiento estable de la comunicación.

El tercer hallazgo identificado por Dell corresponde al cableado de los puertos NAS del PowerStore, donde se detectó que se están utilizando cables de 1 Gb en lugar de los cables de 10 Gb recomendados por el fabricante para los puertos NAS. Esta condición, aunque no impide directamente la comunicación CEE, puede generar intermitencias y problemas de rendimiento en el flujo de eventos bajo condiciones de alta demanda sobre los recursos de almacenamiento compartido.

Hallazgo	Descripción	Impacto	Responsable de atención
Versión de firmware del PowerStore	Versión inicial con soporte limitado para Event Publisher CEE	Alto afecta estabilidad del flujo de eventos	Dell Technologies
Compatibilidad CEE vs. firmware	Requiere verificación de matriz de compatibilidad entre versiones	Alto puede impedir comunicación estable	Dell Technologies / GSTCOL

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

Cableado NAS 1 Gb	Se recomienda cableado 10 Gb para puertos NAS	Medio riesgo de intermitencias bajo alta demanda	IDIGER (infraestructura)

Estado actual de los componentes

Al cierre de las actividades correspondientes a las 20 horas ejecutadas en esta fase, el estado de cada componente del sistema de auditoría es el siguiente:

Componente	Servidor	Estado	Observación
Servicio EMC CAVA (CEE)	SRVSYSLOG02 Windows Server 2025	Instalado y operativo	Escuchando en puerto TCP 12228 con inicio automático
Configuración endpoint CEE → Graylog	SRVSYSLOG02 Registro de Windows	Configurado	Apunta a VLUBPSLOG01 puerto TCP 12201 (GELF)
Event Publishing Pool PowerStore	Dell PowerStore 1000 Consola web	Configurado	Pool "CEE-WINDOWS-Server-2025" activo, protocolo HTTP puerto 12228
Pre-eventos y post-eventos SMB	Dell PowerStore 1000	Habilitados	Cobertura completa de operaciones sobre archivos SMB
Reglas de firewall Fortinet	Infraestructura de red IDIGER	Habilitadas	NAT deshabilitado, puertos TCP/UDP 12201, 1514 y 12228 habilitados
Servidor Graylog	VLUBPSLOG01 Ubuntu Server	Operativo	Inputs GELF TCP 12201 y Syslog 1514 activos
Flujo completo PowerStore → CEE → Graylog	Integración de componentes	Pendiente de estabilización	Condicionado a actualización de firmware del PowerStore por parte de Dell

Conclusión y siguiente fase

Las actividades ejecutadas en el marco de esta fase permitieron completar la instalación y configuración de la totalidad de los componentes tecnológicos que conforman el sistema de auditoría de actividad sobre la NAS PowerStore del IDIGER. El servidor CEE (SRVSYSLOG02) se encuentra instalado y operativo con el servicio EMC CAVA activo y escuchando en el puerto de recepción de eventos. El servidor Graylog (VLUBPSLOG01) se

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

encuentra operativo con los inputs de recepción configurados y en condiciones de procesar y visualizar los eventos una vez que el flujo de auditoría quede completamente establecido. El Event Publishing Pool en el PowerStore se encuentra configurado con los parámetros correctos, la habilitación de pre-eventos y post-eventos SMB, y la referencia al servidor CEE como destino de publicación. Las reglas de conectividad en el firewall institucional fueron habilitadas y verificadas por el equipo del IDIGER, garantizando los canales de comunicación necesarios entre los segmentos de red involucrados.

Con base en el estado actual de los componentes y los hallazgos técnicos identificados durante el proceso de validación, se recomienda la ejecución de una siguiente fase de integración que permita completar la puesta en marcha del sistema de auditoría de actividad de la NAS PowerStore. Esta siguiente fase deberá contemplar, en primer lugar, la coordinación con Dell Technologies para la actualización del firmware del PowerStore a una versión estable que soporte de manera robusta la funcionalidad de publicación de eventos hacia el componente CEE, dado que esta actualización debe ser ejecutada por personal técnico autorizado del fabricante. Una vez actualizado el firmware, se deberá verificar la compatibilidad de versiones entre el nuevo firmware y el componente CEE instalado en SRVSYSLOG02, procediendo con la actualización del CEE en caso de ser necesario. Con los componentes en versiones compatibles y estables, se ejecutará la validación final del flujo completo de auditoría desde el NAS Server del PowerStore hasta la consola de visualización en Graylog, incluyendo la generación de eventos de prueba sobre recursos SMB, la verificación de su recepción en el servidor CEE y su correcta indexación y visualización en la plataforma Graylog, completando así la implementación integral del sistema de auditoría de actividad institucional.

WILMAR DIAZ RODRIGUEZ
Gerente Administrativa y Proyectos.
wilmar.diaz@gstcol.com , proyectos@gstcol.com

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

INFORME CAMBIO DE IP Y CREDENCIALES SWITCH SAN IBM 2498 B24

GSTCOL
NIT 900702873-0
Giga Source Technology de Colombia

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S. Empresa que provee e implementa soluciones de ingeniería Tecnológica, estamos comprometidos con la satisfacción del cliente, brindado el soporte ofreciendo un servicio ágil y eficiente. Contamos con un equipo de trabajo con experiencia profesional que implementa sistemas de Virtualización con HyperV Vmware Citrix, administración de plataformas tecnológicas: almacenamiento, redes, servidores, librerías, firewall, librerías, sistemas operativos, switch, redes de voz y datos, asistencia técnica, entre otras.

Entidad: IDIGER
Equipo intervenido: Switch SAN IBM 2498 B24
Clasificación: Confidencial — Infraestructura Crítica

Objetivos

Documentar el cambio controlado realizado sobre el Switch SAN IBM 2498 B24, consistente en la actualización de la dirección IP de administración y la modificación de credenciales de acceso, ejecutado por solicitud formal del Ing. John Fierro con el propósito de migrar el direccionamiento del segmento 172.16.24.x al segmento corporativo 10.250.200.x.

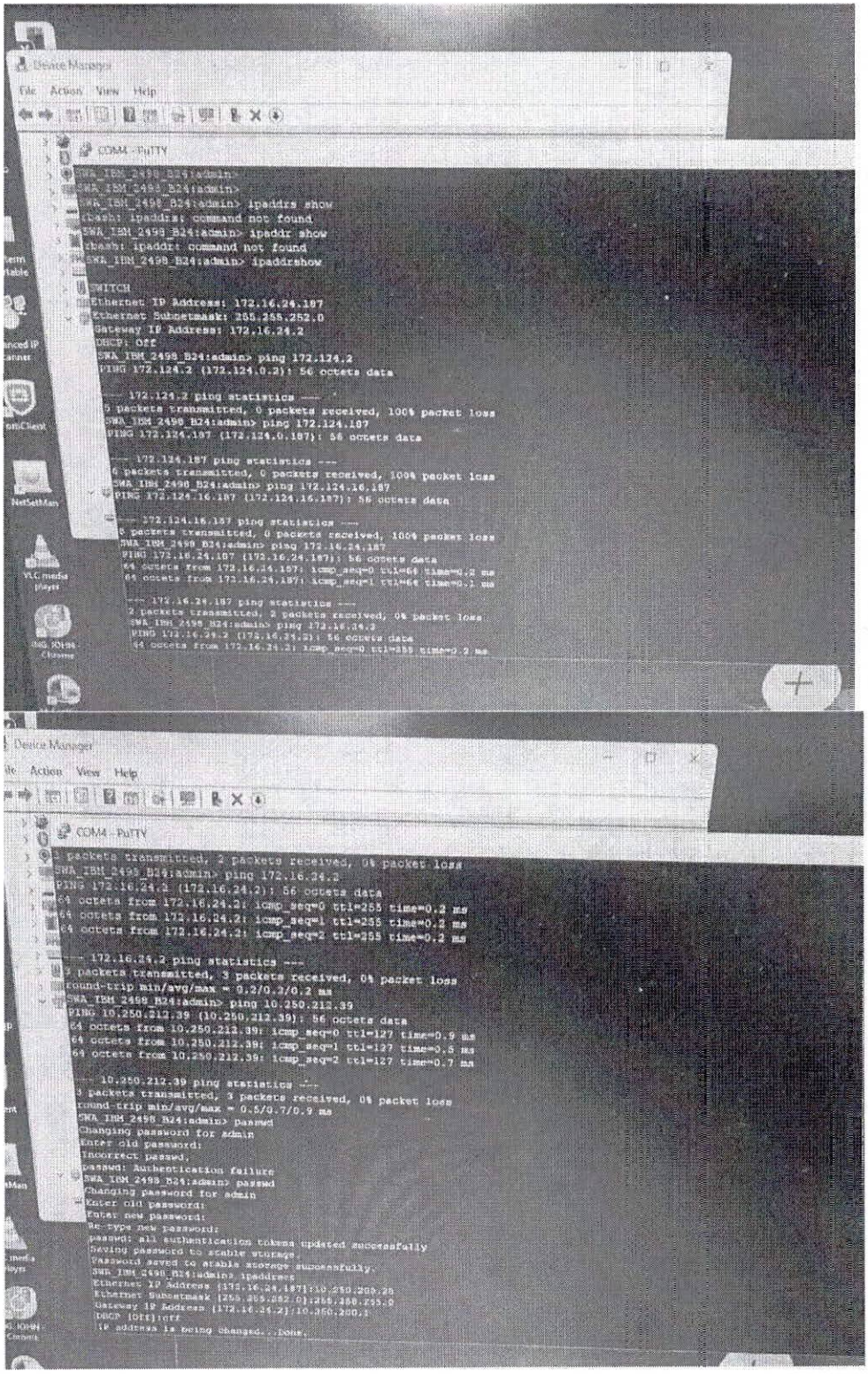
Identificación del Equipo

Parámetro	Valor
Equipo	Switch SAN IBM 2498 B24
Hostname	SWA_IBM_2498_B24
Usuario administrador	admin
Método de acceso	Consola serial — COM4 (PuTTY)

Cambios Ejecutados

Parámetro	Valor Anterior	Valor Nuevo
IP de administración	172.16.24.187	10.250.200.28
Máscara de subred	255.255.252.0	255.255.252.0
Gateway	172.16.24.2	10.250.200.1
DHCP	Off	Off
Contraseña usuario admin	Modificada	Modificada

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S



GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

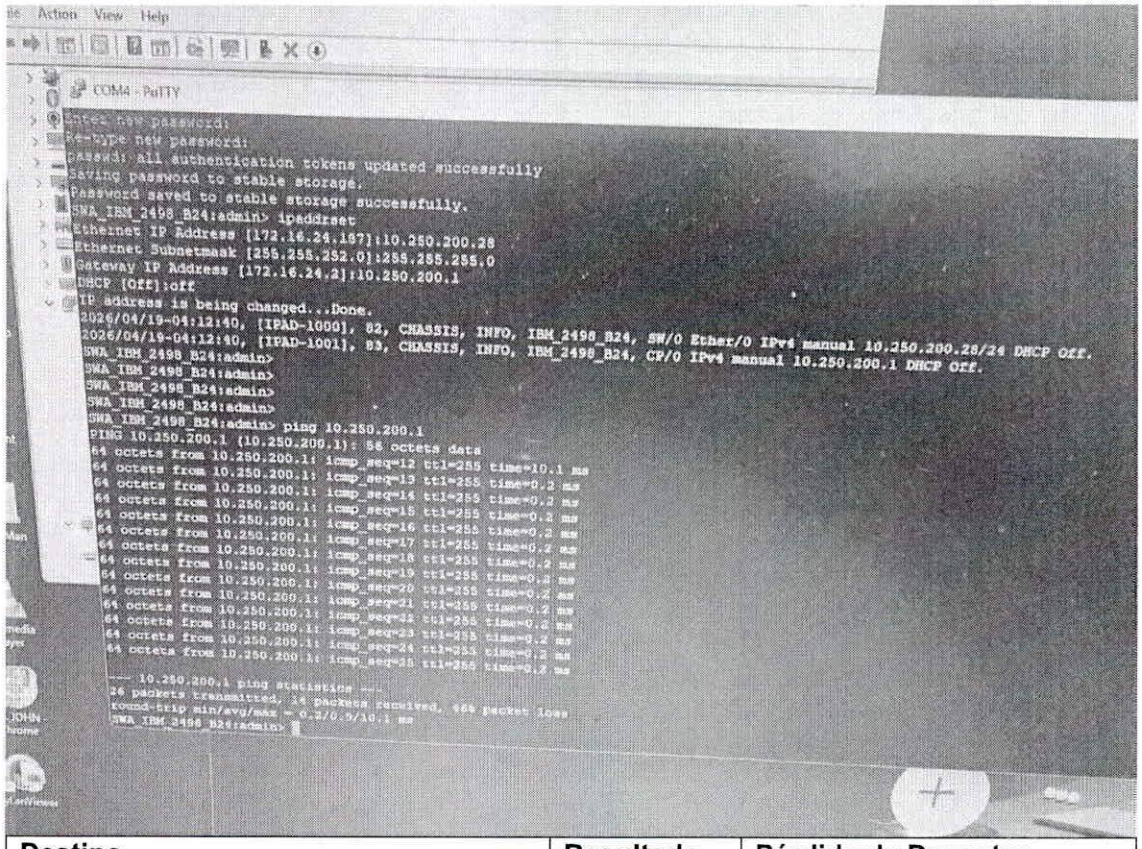
Cambio de Credenciales
Se ejecutó el comando passwd para actualizar la contraseña del usuario admin. El cambio fue confirmado por el sistema con el mensaje:

```
passwd: all authentication tokens updated successfully
Password saved to stable storage successfully.
```

Cambio de Dirección IP
Se ejecutó el comando ipaddrset con los nuevos parámetros de red. El sistema confirmó la aplicación del cambio con el mensaje IP address is being changed...Done. El evento quedó registrado automáticamente en el log del equipo bajo el código [IPAD-1001].

Verificación de Conectividad

Posterior al cambio se ejecutaron pruebas de conectividad ICMP con los siguientes resultados:



Destino	Resultado	Pérdida de Paquetes
10.250.200.1 (Gateway nueva red)	Exitoso	0% (prueba estabilizada)
10.250.212.39 (Equipo red nueva)	Exitoso	0%
172.16.24.2 (Gateway red anterior)	Exitoso	0%

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S

La conectividad del equipo en la nueva red fue confirmada satisfactoriamente.

Nota de Seguridad — Entrega de Credenciales

Las nuevas credenciales de acceso **no se incluyen en el presente informe ni deben ser transmitidas por correo electrónico**, dado que estos medios no garantizan la confidencialidad requerida para información de infraestructura crítica. La contraseña debe ser entregada exclusivamente mediante uno de los siguientes canales seguros:

- **Bóveda de contraseñas institucional** (CyberArk, Bitwarden Business o equivalente)
- **Comunicación verbal presencial** o llamada a número corporativo verificado
- **Canal cifrado de extremo a extremo** (Microsoft Teams canal privado, Signal corporativo)

Práctica	Seguridad
Correo electrónico sin cifrar	No permitido
Incluir en informes o tickets	No permitido
WhatsApp / chat no corporativo	No permitido
Bóveda institucional de contraseñas	Recomendado
Entrega verbal presencial	Recomendado

Resultado y Acciones Pendientes

El cambio fue ejecutado y verificado exitosamente. Como acciones pendientes se requiere:

- Actualizar el inventario de IPs corporativo con la nueva dirección 10.250.200.28
- Registrar las nuevas credenciales en la bóveda institucional de contraseñas
- Actualizar las herramientas de monitoreo con la nueva IP de administración
- Retirar la referencia a la IP anterior 172.16.24.187 de la documentación de red

WILMAR DIAZ RODRIGUEZ
Gerente Administrativa y Proyectos.
wilmar.diaz@gstcol.com , proyectos@gstcol.com

GIGA SOURCE TECHNOLOGY DE COLOMBIA S.A.S