Nº Radicado 0124000412202/ MDN-COGFM- JEMC-SEMPE-CGDJ6-DITIN– 29-10

Bogotá D.C., 23 de Julio de 2024

Señora Teniente Coronel
Maritza Molina Carrillo
Directora Administrativa y Financiera COGFM
Comando General Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá D.C.

Asunto: Informe de Supervisión y Seguimiento No 02 de la Orden de Compra No. 150 de 2024
Mensual X ó Final _

Respetuosamente, me dirijo a la señora Teniente Coronel, Directora Administrativa y Financiera, con el fin de presentar el informe de supervisión y seguimiento del contrato del asunto, de acuerdo con la siguiente información:

1. Datos del supervisor

Nombre del supervisor	TE. IVAN NICOLAS RAMIREZ VERGARA
Dependencia	Dirección Tecnologías de la Información
Cargo	Jefe de Área de Infraestructura Tecnológica
Apoyo a la supervisión	N/A

2. Datos del contrato

Número y fecha de suscripción del Contrato		No. 150 del 26/04/2024	
Contratista		IDENTIAN SAS	
Cedula de Ciudadanía o Nit.		900.678.711-3	
Objeto		"Contratar la renovación, actualización, ampliación, y soporte de la herramienta de monitoreo para la infraestructura de TI del Comando General de las Fuerzas M l tar s, de acuerdo con las esp c f cac ones técn cas"	
Valor del Contrato		$ 99.000.000,00	
Plazo de ejecución		Desde 03/05/2023 hasta 25/10/2024	
		Modificatorio	
Adición	Prorroga	Suspensión	Otros

3. Descripción del desarrollo de las actividades contractuales

Número	Obligación especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	Cumple	No cumple	Evidencia del cumplimiento de las obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato
1	Cumplir con el objeto del contrato, de conformidad con las especificaciones Técnicas contratadas y dentro del plazo establecido para la ejecución	X		El contratista está realizando su labor sin ninguna novedad y ya cumplió con el primer mantenimiento solicitado por el señor supervisor
2	Obtener con la oportunidad debida, las licencias, autorizaciones y permisos a que hubiere lugar para el cumplimiento de todas las obligaciones que le corresponden en los términos del contrato	X		El contratista está realizando su labor actualizo la plataforma sin ninguna novedad y ya cumplió con el primer mantenimiento solicitado por el señor supervisor
3	Mantener durante el plazo de ejecución del contrato los precios ofertados	X		El contratista se compromete a no aumentar los precios del presenta contrato y a cumplir con lo estableció en el contrato
4	Elaborar y suscribir, dentro de los cinco (05) días siguientes a la comunicación del inicio del plazo de ejecución, conjuntamente con el supervisor, el cronograma de actividades del contrato	X		El contratista cumple y envía el cronograma realizado en conjunto con el supervisor
	SOPORTE Y MANTENIMIENTO DE LA HERRAMIENTA			
5	Se debe realizar dos (02) mantenimientos preventivos a todo nivel, durante el tiempo de ejecución del contrato asi: a) Un anexo que describa la clasificación de acuerdo con el nivel de criticidad establecidos en la herramienta de la siguiente manera: - Prioridad Crítica/ Alta: Es requerido la acción inmediata sobre la continuidad total del negocio que afectan su disponibilidad eventos cuyo umbral superan el nivel crítico según las definiciones. - Prioridad Media: Cuando hay alertamiento de nivel warning sobre infraestructura de criticidad media para el negocio - Prioridad Baja: Cuando hay alertamiento sobre entornos menores como calidad, desarrollo o catalogados como de criticidad baja b) Atención de casos ilimitados. c) Atención de consultas técnicas ilimitadas. d) Acceso a Portal de Soporte del proveedor. e) Soporte técnico remoto Ilimitado. f) Recepción de casos en horario 5x8 (horario local - Colombia). g) Soporte técnico telefónico ilimitado. h) Update de versiones menores (Instalación de parches) i) Soporte del Fabricante j) Upgrade de software aplicación k) Reportes de desempeño del servicio l) Todo el soporte debe ser en español, así como la documentación que se genere. m) El contratista debe ofrecer soporte local a través de ingenieros certificados en la herramienta ofrecida. n) El contratista debe certificar que los servicios ofrecidos, por lo que requiere presentar la certificación donde demuestra que cuenta con el respaldo del fabricante del producto.	X		El contratista se compromete a realizar los dos mantenimientos los cuales el primero se realizaría iniciando el proyecto y el segundo a finalizar. (junio - agosto), El proveedor de servicio anexa el documento del primer mantenimiento se anexa documento con 48 páginas. Faltaría el segundo mantenimiento

	ñ) Soporte Local a través de un Ingeniero de sistemas con experiencia comprobada de la solución ofrecida en desarrollo, customización, soporte y gestión de infraestructura de la solución ofrecida.			
6	El oferente debe estar en la capacidad de gestionar y/o realizar: a) Cualquier evento que se presente en la operación de la entidad y que sea detectado por el sistema de monitoreo debe ser registrado por la herramienta. b) Un anexo que describa el estado de los eventos y/o incidentes y/o problemas de monitoreo que hayan afectado cualquiera de los componentes que conforman el alcance del servicio. c) Un conjunto de informes predeterminado en la herramienta de monitoreo que describa el estado de monitoreo de los servicios a nivel de negocio donde el cliente pueda consultar cuando desee. d) Un reporte generado por la herramienta de inventario donde se pueda conocer el estado actual de monitoreo y los activos en monitoreo. e) Un anexo que describa la clasificación de acuerdo con el nivel de criticidad establecidos en la herramienta de la siguiente manera: - Prioridad Crítica/ Alta: Es requerido la acción inmediata sobre la continuidad total del negocio que afectan su disponibilidad eventos cuyo umbral superan el nivel crítico según las definiciones. - Prioridad Media: Cuando hay alertamiento de nivel warning sobre infraestructura de criticidad media para el negocio - Prioridad Baja: Cuando hay alertamiento sobre entornos menores como calidad, desarrollo o catalogados como de criticidad baja	X		El contratista se compromete a garantizar, gestionar cualquier evento que se presente
	GARANTÍA TÉCNICA Y SERVICIO			
7	Se deberá prestar un acompañamiento con un Horario 7x24 por el proveedor, por el término de doce (12 meses)	X		El proveedor anexa la documentación de servicio técnico
8	Se debe brindar acompañamiento técnico telefónico o remoto de forma inmediata en el momento de presentar alguna novedad con el servicio adquirido. Si en el lapso de cuatro (04) horas después de haber reportado el incidente no se ha dado una solución definitiva al incidente, se deberá enviar personal técnico especializado a sitio en un tiempo máximo de una (02) horas. (tiempos de respuesta)	X		El proveedor anexa la documentación de servicio técnico
9	El servicio de acompañamiento se podrá prestar a través de herramientas de servicio remoto, o también en sitio en la ciudad de Bogotá	X		El proveedor anexa la documentación de servicio técnico
10	El servicio prestado deberá indicar procedimiento de escalamiento si es necesario	X		El proveedor anexa la documentación de servicio técnico
	ALCANCE GARANTÍA TÉCNICA			
11	El término de la garantía técnica o garantía legal de conformidad con los artículos No. 7, 8, 9 y 11 de la Ley 1480 de 2011, será de (12) meses contados a partir de la activación de las licencias. Estos acompañamientos deben incluir como mínimo las siguientes actividades: - Actualizaciones (Upgrade, Update, criticas de Seguridad). - Revisión y solución de errores. - Realización y programación de copias de seguridad.	X		El proveedor anexa alcance de la garantía

	- Revisión logs. - Desinstalación de funcionalidades inoperativas. - Procedimientos de hardening. Los acompañamientos deben ser programados en horarios no hábiles de acuerdo con las coordinaciones y necesidades del COGFM. - Configuraciones, puesta en producción y funcionamiento. El servicio será prestado en sitio en la ciudad de Bogotá de acuerdo con los tiempos de respuesta establecidos			
	ACTUALIZACIONES			
12	Durante el tiempo de la garantía se debe brindar e instalar actualizaciones a la herramienta descrita en el presente anexo, cada vez que se libere en el mercado una nueva versión de software, upgrade, o parche. Lo anterior previa solicitud y aprobación del supervisor del contrato y una vez haya sido probada en laboratorio, asegurando la continuidad del servicio y funcionamiento de los sistemas	X		El contratista se compromete a garantizar, la actualización de la herramienta en donde se ve reflejado los trabajos en el primer mantenimiento y todas las reuniones que también se anexan en el informe de supervisión
13	Se debe realizar entrega al COGFM, de los medios magnéticos y/o manuales si existen cambios de versión			El proveedor entregara los manuales de las versiones apenas este actualizado
	REPORTES E INFORMES TÉCNICOS			
14	Una vez realizados los acompañamientos (remotos o en sitio), se deberá hacer entrega o enviar dentro de los cinco (05) días siguientes de cada mantenimiento, un reporte técnico donde se indique las actividades realizadas, observaciones y pendientes, el informe técnico como mínimo debe indicar: - Actividades realizadas. - Actualizaciones aplicadas. - Procedimientos preventivos y/o correctivos aplicados. - Recomendaciones. - Pendientes	X		El proveedor de servicio anexa el documento del primer mantenimiento se anexa documento con 48 páginas. Faltaría el segundo mantenimiento.
	SEGURIDAD			
15	ACUERDO DE CONFIDENCIALIDAD: El contratista y todos los colaboradores de la ejecución del contrato se comprometen a firmar acuerdos de confidencialidad y no divulgación de equipos, elementos, configuraciones, cantidad y características de activos en hardware, software e información previos instalados y por adquirir, así como los resultados de los posibles análisis de Malware que serán usados para las pruebas, durante la ejecución del contrato, este se reserva el derecho de admisión del personal que hará del desarrollo del proyecto por parte de la empresa contratista seleccionada, lo cual será verificado por el supervisor del contrato	X		El contratista envío el documento de confidencialidad en el informe de supervisión N°1
16	Políticas de seguridad informática: El contratista debe comprometerse a conocer, aceptar y ajustarse a las políticas de seguridad de la directiva de seguridad informática de las Fuerzas Militares	X		El contratista envío el documento de confidencialidad en el informe de supervisión N°1
17	El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que	X		El contratista envío el documento de confidencialidad en el informe de supervisión N°1

	brindará			
	PERFIL DEL PERSONAL REQUERIDO EN LA EJECUCIÓN DEL CONTRATO			
18	- Consultor Seguridad de la Información II: 1 (uno), con dedicación de tiempo parcial, presencial o virtual, quien realizara las actividades de liderar cada una de las actividades del presente proceso según el anexo de especificaciones técnicas - Consultor Pen Testing: 1 (uno), con dedicación de tiempo parcial, presencial o virtual, Quien realizara las actividades de implementación de la herramienta de monitoreo del presente proceso según el anexo de especificaciones técnicas	X		El contratista envía hojas de vida de los ingenieros que van a cumplir esta labor que son los ingenieros Arthuz Diaz y Robin Salcedo en el informe de supervisión N°1

4. Cumplimiento de Obligaciones al Sistema de Seguridad Social y Parafiscales

Que la Planilla Integrada de Liquidación de Aportes N° 78396946 con fecha de pago 03 de julio de 2024, evidencian el cumplimiento de las obligaciones al Sistema de Seguridad Social Integral, la cual es anexada al presente informe.

Que mediante certificación de fecha 17 de julio de 2024, suscrito por el señor JAVIER STIVEN MUÑOZ URIBE, revisor fiscal con TP. No 258022-T, de la empresa IDENTIAN SAS, estipula encontrarse al día en el pago al Sistema de Seguridad Social en Pensiones y en Salud, riesgos profesionales, aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje (SENA). Se anexa certificado del cumplimiento por parte del contratista.

NOTA: El certificado de aportes parafiscales lo puede firmar el representante legal cuando en cámara de comercio no reporta revisor fiscal, cuando el contratista tiene revisor fiscal este es el único competente para firmar las certificaciones de paz y salvo de seguridad social y parafiscal.

5. Aspectos Financieros

Valor Inicial del Contrato Incluido IVA:	$ 99.000.000,00
Valor total del Contrato es de:	$ 99.000.000,00

Que se tramitaron las siguientes facturas con cargo al contrato supervisado:

No Factura	Fecha	Valor de la Factura
FAID1001	11/07/2024	$49.500.000,01
Oficio de Centavo	11/07/2024	- $0,01
Valor Facturado		$0
Saldo por Facturar		$49.500.000,00
Valor de Reintegro		$0
Valor Total del Contrato		$ 99.000.000,00

Nota: En el anterior cuadro se deberán relacionar todas las facturas que se hayan tramitado para pago durante la ejecución del contrato.

6. Observaciones relevantes del supervisor:

Anotación: el señor representante legal de la empresa identian envía documento envía oficio del día 11 de julio del 2024 en donde por fallas técnicas en su servicio de facturación la factura FAID 1001 es

expedida con un centavo adicional ($0.01) y el señor representante expone que desiste de este centavo y que el COGFM cancele el valor de la factura sin este centavo adicional con esto el valor a pagar por el COGFM es ($49.500.000,00).

7. Documentos anexos:

Anexo	Descripción del anexo	No. paginas
Certificado de aportes parafiscales	X	01
Planilla de pagos al sistema de seguridad social	X	03
Informe primer mantenimiento	X	48

Atentamente,



TENIENTE RAMIREZ VERGARA IVAN NICOLAS
Supervisor Contrato No. 150/2024
Correo electrónico ivanram@cgfm.mil.co
Teléfono 3150111 - Ext. 21221

Espacio para ser diligenciado en la Dirección Administrativa y Financiera

CONTROL DE APROBACIONES Y DE TIEMPOS PARA PUBLICAR				
CONTRATOS	FECHA DE RECEPCIÓN DEL INFORME	FECHA DE APROBACIÓN Y CARGUE DEL INFORME.	NOMBRE DE FUNCIONARIO REVISOR	FIRMA DEL FUNCIONARIO AVALANDO INFORME
	24 JUL/24	24 JUL/24	PS. LOURDES FONSECA 24 JUL/24 9:18 AM	

IDENTIAN®

NIT : 900,678,711 - 3
AV CLLE 26 No 59 41 OFC 1002
BOGOTA D.C.-BOGOTA - COLOMBIA
6017042400
info@identian.co
Responsables de iva - No somos autorretenedores
Actividad Económica 6202 Tarifa 6,90

Cliente	MINISTERIO DEFENSA NACIONAL COMANDO GENERAL DE LAS FUIERZAS MILITARES.		
NIT	800,230,729 - 9 /Id. Extranjero:	**Teléfono**	6013150111
Dirección	AV DORADO CAN CARRERA 54 26 25	**Vendedor**	IDENTIAN SAS
Ciudad	BOGOTA D.C.-BOGOTA - COLOMBIA	**Centro Costo**	1.270
Correo	facturacionDIADF@cgfm.mil.co		
Order Reference Prefijo		**Numero**	150COGFM DIADF2024

FACTURA ELECTRÓNICA DE VENTA
FAID 1001

Fecha y Hora de Factura

Generación	2024-07-11	15:39:11
Expedición	2024-07-11	15:41:15
Vencimiento	2024-08-11	

Código	Descripción	Unid	Cant	V. Unit	Valor Total
0100006000001	SERVICIO DE MANTENIMIENTO PARA LA HERRAMIENTA DE MONITOREO, DETECCION Y ALERTAMIENTO DE EVENTOS SOBRE LA INFRAESTRUCTURA DE TI DE COGFM 150COGFM DIADF2024	UND	1	41,596,638.66	41,596,638.66

Total Bruto	41,596,638.66
IVA	7,903,361.35
Total a Pagar	**$ 49.500.000,01**

CONDICION DE PAGO

Credito	Credito Clientes Nacionales	Efectivo	49.500.000,01	Cuota 1 Vence el 2024-08-11

VALOR EN LETRAS

Cuarenta Y Nueve Millones Quinientos Mil Pesos M/Cte Con 01/100

OBSERVACIONES

#$15-01-02-000;contrato150;facturacionDIADF@cgfm.mil.co#$

Esto con el fin de recepcionar la factura de la manera adecuada en SIIF nación.

Elaborado, impreso y enviado electrónicamente por S.A.S. NIT

Firma Elaborado por : Fernanda Castro

Firma Recibido

REALIZAR PAGO A LA CUENTA DE AHORROS BANCOLOMBIA No. 58216984933. A NOMBRE DE IDENTIAN SAS NIT. 900.678.711-3

A esta factura de venta aplican las normas relativas a la letra de cambio (artículo 5 Ley 1231 de 2008). Con esta el Comprador declara haber recibido real y materialmente las mercancías o prestación de servicios descritos en este título - Valor. **Resolución y/o Autorización de facturación No**18764074219907 **aprobado en** 2024-07-03 **vigente** 1 Años, **prefijo** FAID **desde el número** 993 **al** 2000

CUFE :4e36ed22c04c182eae4764da7309e19fd0faf830c0dc5de6700775d6f62b4c087fabe87589a22a56daa16bed97ee2b67

ORIGINAL

Bogotá, julio 23 de 2024

Señores:
COGFM
Bogotá D.C.

Asunto: Alcance Garantía Técnica del Contrato

Estimados Señores:

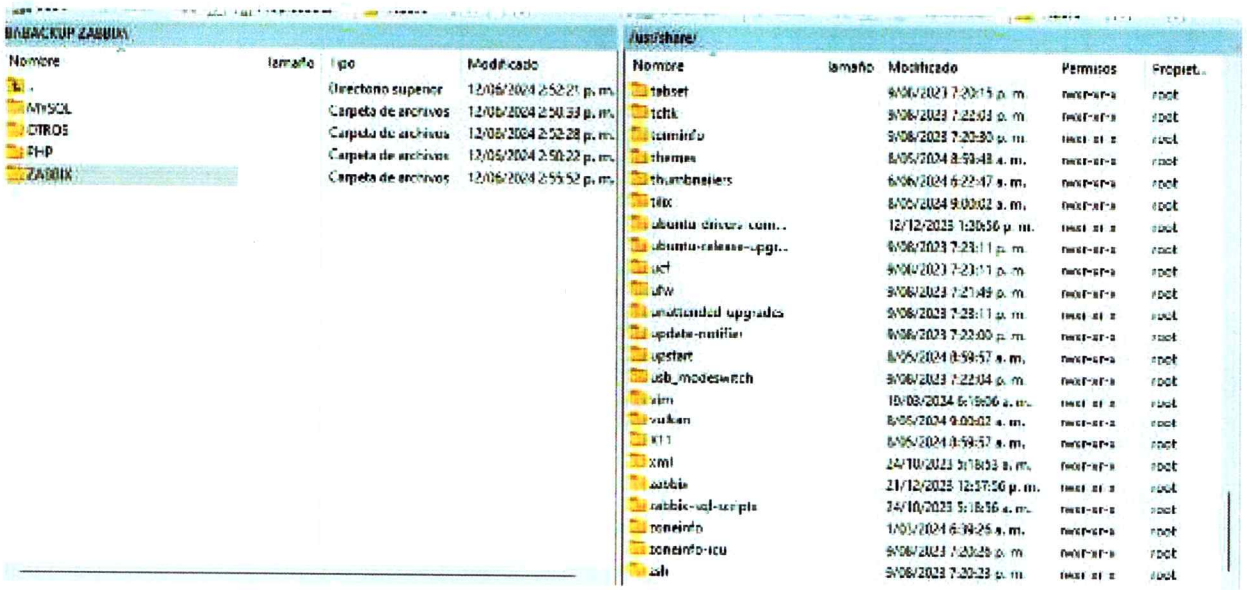
De acuerdo con el contrato **150COGFMDIADF2024**, y su garantía que comprende un período entre el 01 de julio de 2024 al 01 de julio de 2025, se realizan las siguientes actividades:

- Actualizaciones (Update, Upgrade y críticas de seguridad)
- Revisión y solución de errores.
- Realización y programación de copias de seguridad.
- Revisión de logs.

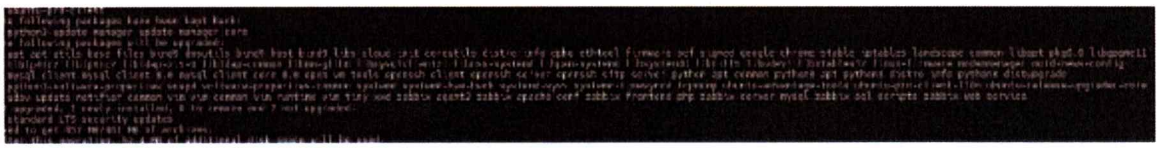
Las actividades anteriormente expuestas se ejecutaron sin generar ningún tipo de indisponibilidad.

Como evidencia de la gestión realizada, se relaciona la siguiente información:

- Se muestra la ruta de los backups y la configuración para la herramienta.



- Se ejecuto la actualización del servidor de Zabbix a la última versión disponible.



- Se remedio la falla del export de reportes.



Saludos,

Robin Josè Salcedo Buelvas
Representante Legal
CC. 77.090.560 de Valledupar
rsalcedo@identian.co
www.identian.co
PBX. 601-7042400 - 3014873962

Bogotá, Julio 11 de 2024

Señores:
CGFM
Ciudad

Asunto: Facturación de contrato150COGFM DIADF2024

Estimados Señores:

Teni ndo n cu nta l contrato 150COG M DIAD 2024, cuyo obj to s "Servicio de Mantenimiento para la Herramienta de Monitoreo, Detección y Alertamiento de Eventos sobre la Infraestructura de TI de COGFM", y que el Supervisor del Contrato el Sr. Teniente Nicolas Ramirez, realiza la solicitud de generación de factura por el cincuenta porciento (50%)
Hemos emitido la Factura FAID 1001 por valor de $49.500.00.01 y encontramos que se presenta una diferencia de mayor valor frente a lo estipulado en la liquidación por un centavo ($0.01) en el valor del IVA, esta diferencia se presenta porque al subir el valor de la base de la factura a nuestra plataforma contable (SIIGO), el valor del IVA se aproxima al siguiente decimal, ocasionando en el valor total de la factura haya un centavo ($0.01) de diferencia, elevamos esta consulta a asesoría en la DIAN y nos dicen que no es posible hacer una NC por un centavo ($0.01) ya que se afectaría el valor base de la factura.
Teniendo esto en cuenta certificamos y confirmamos con este documento que Identian no cobrará esta diferencia y asume ese centavo ($0.01) en la diferencia del IVA y no hará cobro de él, esta situación también está en conocimiento del Supervisor del contrato el Teniente Nicolas Ramirez.
Por lo tanto el valor a cancelar por parte del Comando General de las Fuerzas Militares será de $49.500.000.00= Cuarenta y nueve millones quinientos mil pesos.

Agradecemos de antemano su amable atención y gestión.

Saludos,

Robin José Salcedo Buelvas
Representante Legal
CC. 77.090.560 de Valledupar
rsalcedo@identian.co
www.identian.co
PBX. 601-7042400 - 3014873962

IDENTIAN®

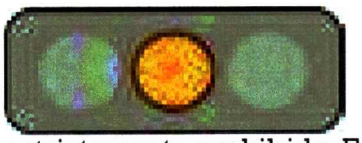
Informe de monitoreo y correlación NOC

Presentado a:

COMANDO GENERAL
FUERZAS MILITARES DE COLOMBIA
UNIÓN - INTEGRIDAD - VICTORIA

Julio 2024

RESTRICCIONES DE USO Y DECLARACIONES



Este documento contiene información privilegiada. Su uso es sólo para destinatarios autorizados. Cualquier propagación, distribución o duplicado de esta información, total o parcial, sin previa autorización escrita por parte de **IDENTIAN**, está estrictamente prohibida. Estas restricciones no limitan el derecho otorgado a los destinatarios autorizados del documento a utilizar las estadísticas o información disponible en este documento, las cuales fueron obtenidas a través de fuentes tales como organizaciones públicas, privadas o reportes noticiosos. Si usted no es un destinatario autorizado, por favor contacte a quien se lo envió, y destruya toda copia del mensaje original.

TABLA DE CONTENIDO

Capítulo	Página
1.INTRODUCCIÓN	4
2.OBJETIVO	8
3.ALCANCE	8
4.CUMPLIMIENTO	8
5.METODOLOGIA	11
6.RIESGO	15
7.DIAGRAMA	20
8.ACTIVOS	21
8.1 ESTADO POR AGENTE	24
8.2 ESTADO DE LOS SERVICIOS	24
9.CONCLUSIONES	44

1.INTRODUCCIÓN

El presente informe ejecutivo tiene como objetivo documentar el desarrollo del documento de ingeniería llevado a cabo durante el proyecto de Implementación de plataforma de monitoreo basada en Zabbix y Grafana para comando General de las Fuerzas Militares (CGFM). En este informe, se proporcionará una descripción detallada de cada una de las pestañas que componen el documento, desde una perspectiva a nivel gerencial. El enfoque principal será evaluar el grado de cumplimiento de los requisitos iniciales establecidos, así como analizar la información presentada en dichas pestañas con respecto a las disposiciones de información planteadas inicialmente.

Zabbix es una solución de monitoreo distribuido de código abierto de clase empresarial, es un software que monitorea numerosos parámetros de una red y la salud e integridad de servidores, máquinas virtuales, aplicaciones, servicios, bases de datos, sitios web, la nube, etc. Esto lo vuelve escalable e implementable en grandes infraestructuras.

Esta herramienta es una solución de monitoreo de red altamente integrada que ofrece una multiplicidad de características en un solo paquete.

Beneficios potenciales

Mejora en la detección temprana de problemas de rendimiento y disponibilidad.
- Reducción del tiempo de inactividad y aumento de la disponibilidad de servicios.

Mejora en la eficiencia operativa y optimización de recursos.
Facilita la toma de decisiones informadas basadas en datos.

A continuación, se nombrarán muchas de las funciones que son de interés en Zabbix por miles de compañías:

Recopilación de datos

- Verificaciones de disponibilidad y rendimiento.

soporte para SNMP (tanto captura como sondeo), IPMI, JMX, monitoreo de VMware
Verificaciones personalizadas
Recopilación de los datos deseados a intervalos personalizados
Realizado por servidor/proxy y por agentes

Definiciones de umbral flexibles

- Puede definir umbrales de problemas muy flexibles, llamados iniciadores, logrando generar alertas cuando se superen estos umbrales personalizados.

Alertas altamente configurables

El envío de notificaciones se puede personalizar para el cronograma de escalamiento, destinatario, tipo de medio
Las notificaciones pueden hacerse significativas y útiles mediante macro. variables
Las acciones automáticas incluyen comandos remotos

Gráficos en tiempo real

las métricas monitoreadas se grafican inmediatamente usando la funcionalidad de gráficos integrados

Capacidades de monitoreo web

Zabbix puede seguir una ruta de clics de ratón simulados en un sitio web y comprobar la funcionalidad y el tiempo de respuesta.

Extensas opciones de visualización

Capacidad de crear gráficos personalizados que pueden combinar varios elementos en una sola vista
Mapas de red
Presentaciones de diapositivas en una descripción general estilo panel de control
Informes
Vista de alto nivel (comercial) de los recursos monitoreados

Información histórica de almacenamiento

Datos almacenados en base de datos
Historial configurable
Procedimiento de limpieza incorporado

Configuración fácil

Agregar dispositivos monitoreados como equipos
Los equipos se seleccionan para el monitoreo, una vez en la base de datos
Aplicar plantillas a dispositivos monitoreados

Uso de plantillas

Agrupar verificaciones en plantillas
Las plantillas pueden heredar otras plantillas
Descubrimiento de red
Descubrimiento automático de dispositivos de red
Registro automático de agentes
Descubrimiento de sistemas de archivos, interfaces de red y OIDs de SNMP

Interfaz web

Una interfaz web en PHP
Accesible desde cualquier lugar
Puede hacer clic en su camino a través
Registro de auditoría

API de Zabbix

La API de Zabbix proporciona una interfaz programable a Zabbix para manipulaciones masivas, integración de software de terceros y otros fines.

Requisitos del Sistema

Sistema Operativo

Debido a los requisitos de seguridad y la naturaleza de misión crítica del servidor de monitoreo, UNIX es el único sistema operativo que puede ofrecer constantemente el rendimiento necesario, la tolerancia a fallos y la resiliencia sin embargo Zabbix opera en versiones líderes del mercado.

Los componentes de Zabbix están disponibles y probados para las siguientes plataformas[1]:

Plataforma	Servidor	Agente
Linux	Si	Si
IBM AIX	Si	Si
FreeBSD	Si	Si
NetBSD	Si	Si
OpenBSD	Si	Si
HP-UX	Si	Si
Mac OS X	Si	Si
Solaris	Si	Si
Windows	-	Si

Hardware Necesario

Windows:

Sistema operativo: Windows XP o superior (64 bits recomendado desde Zabbix)
Procesador: Cualquier procesador compatible con la arquitectura del sistema operativo
Memoria RAM: 128 MB
Espacio en disco: 256 MB

Linux:

Sistema operativo: Cualquier distribución compatible con la arquitectura del sistema operativo
Procesador: Cualquier procesador compatible con la arquitectura del sistema operativo
Memoria RAM: 128 MB
Espacio en disco: 256 MB

Software necesario

Requisito	Estado obligatorio	Descripción
libpcre/libpcre2	Uno de	Se requiere una de las bibliotecas PCRE/PCRE2 para admitir Expresión regular compatible con Perl (PCRE). El nombre puede diferir dependiendo de la distribución GNU/Linux, por ejemplo 'libpcre3' o 'libpcre1'. Se admiten PCRE v8.x y PCRE2 v10.x (desde Zabbix 6.0.0). Requerido para el monitoreo de registros. También requerido en Windows.
libpthread	Sí	Requerido para soporte de muteSi y bloqueo de lectura-escritura (podría ser parte de libc). No es necesario en Windows.
libresolv		Requerido para la resolución DNS (podría ser parte de libc). No es necesario en Windows.
libiconv		Requerido para la codificación de texto/conversión de formato a UTF-8 en elementos de registro, contenido de archivos, expresiones regulares de archivos y elementos de coincidencia (podría ser parte de libc). No es necesario en Windows.
libgnutls o *libopenssl*	No	Obligatorio si se usa encryption. Versiones mínimas: *libgnutls* - 3.1.18, *libopenssl* - 1.0.1 En Microsoft Windows se requiere OpenSSL 1.1.1 o posterior.
libldap		Obligatorio si se utiliza LDAP. No compatible con Windows.
libcurl		Requerido para las métricas del agente Zabbix web.page.*. No es compatible con Windows. Se recomienda la versión 7.28.0 o superior.
libmodbus		Solo es necesario si se utiliza la monitorización Modbus. Versión 3.0 o superior.

2.OBJETIVO

Ofrecer el resumen de los riesgos cibernéticos a través de un análisis de eventos y alarmas de seguridad generadas por los diferentes sistemas de información de misión crítica, mediante casos de uso específicos que permitan observar los escenarios con sus diferentes vectores para proteger la disponibilidad, confidencialidad e integridad de la información de **CGFM**.

3.ALCANCE

El objetivo del servicio es validar y definir claramente los niveles de exposición en que se encuentra la plataforma tecnológica de **CGFM** frente a posibles ataques e incursiones no autorizadas por parte de delincuentes informáticos, con el fin de lograr que la configuración de la infraestructura tecnológica implementada actualmente, cumpla con los más altos estándares de seguridad, de manera que se minimice el riesgo en cuanto a la integridad, disponibilidad y confidencialidad de la información de la red de datos de **CGFM.**

(Monitoring as a Service).

Escalabilidad: La infraestructura permite escalar el sistema según las necesidades del cliente, ya sea en términos de número de dispositivos monitoreados o volumen de datos procesados.

Mantenimiento y Actualizaciones: Gestionar el mantenimiento y las actualizaciones del sistema, asegurando que la infraestructura esté siempre al día con las últimas mejoras y parches de seguridad.

Reducción de Costos: reducir costos operativos al no tener que invertir en hardware, licencias de software y personal especializado para gestionar el sistema de monitoreo.

Alta Disponibilidad: Las solucione MaaS garantizan alta disponibilidad y redundancia, minimizando el riesgo de tiempo de inactividad.

Seguridad: implementar medidas de seguridad robustas para proteger los datos monitoreados, lo que incluye cifrado, controles de acceso y auditorías de seguridad.

4.CUMPLIMIENTO

CONPES 3854: Se destaca el rol crucial del gobierno en la sociedad, resaltando su capacidad para mantener la seguridad integral y establecer directrices. Se enfatiza la necesidad de la participación y constante del gobierno en la transformación digital, haciendo hincapié en aspectos como la formación de abogados con conocimientos tecnológicos, programas de actualización en universidades para expertos en seguridad, leyes que respalden a los usuarios frente a delitos cibernéticos y la inversión en infraestructura tecnológica para protegerse contra ataques cibernéticos. También se subraya la importancia de realizar

revisiones constantes, incluyendo auto evaluaciones para descubrir nuevas vulnerabilidades que puedan poner en riesgo activos críticos.

1. **Creación de un marco institucional**: Definir claramente las responsabilidades y roles en la gestión de la seguridad digital.

2. **Gestión de riesgos:** Establecer condiciones para que las partes interesadas gestionen los riesgos de seguridad digital en sus actividades.

3. **Fortalecimiento de la seguridad digital:** Mejorar la seguridad de individuos y del Estado en el entorno digital tanto a nivel nacional como transnacional.

4. **Defensa y soberanía digital:** Impulsar acciones para proteger la integridad y seguridad nacional en el ámbito digital.

5. **Cooperación internacional:** Promover la colaboración y asistencia en materia de seguridad digital a nivel nacional e internacional

MIPG: Modelo Integrado de Planeación y Gestión (MIPG) es un marco de gestión adoptado en Colombia que integra varios sistemas de gestión para mejorar la eficiencia y eficacia de las entidades públicas.

El estándar **ISO 27001:2022** ayuda a las organizaciones a administrar la seguridad de los activos confidenciales, como datos financieros, propiedad intelectual, registros de empleados, datos de clientes y otra información confidencial. Exige que **CGFM** hagan cumplirla seguridad de la información, reduciendo así el posible riesgo de robos e infracciones de datos.

CONTROLES ISO 27002:2022

El siguiente es el cumplimiento que cumple el monitoreo SOC a la norma *ISO 27001:2022*

A.5.6 Contacto con grupos de interés especial

Proporciona contactos apropiados con grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales

A.8.1 Política de dispositivos móviles

Se adoptará una política y medidas de seguridad de apoyo para gestionar los riesgos introducidos por el uso de dispositivos móviles.

A.5.9 Inventario de activos

Se identificarán los activos de control asociados con la información y las instalaciones de procesamiento de la información y se elaborará y mantendrá un inventario de estos activos.

A.5.10 Propiedad de los activos

Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos asociados con la información y las instalaciones de procesamiento de la información. Uso aceptable de los activos.

A.8.7 Controles contra el malware

Está relacionado con los controles de detección, prevención y recuperación para proteger contra el malware que se implementarán, combinado con la conciencia adecuada del usuario.

A.8.5 Registro de eventos

Está relacionado con los registros de eventos que registran las actividades de los usuarios, las excepciones, las fallas y los eventos de seguridad de la información que deben producirse, conservarse y revisarse periódicamente.

A.8.19 Instalación de software en Sistemas operativos

Se implementarán procedimientos para controlar la instalación de software en los sistemas operativos.

A.8.8 Restricciones en la instalación de software

Se establecerán e implementarán reglas que rijan la instalación de software por parte de los usuarios.

A.8.34 Controles de auditoría de sistemas de información

Está relacionado con los requisitos y actividades de auditoría que involucran la verificación de sistemas operativos que deben planificarse y acordarse cuidadosamente para minimizar las interrupciones en los procesos comerciales.

A.8.8 Informe de eventos de seguridad de la información

Está relacionado con los eventos de seguridad de la información que se deben informar a través de los canales de gestión apropiados lo más rápido posible.

A.5.36 Cumplimiento de las Políticas y Estándares de Seguridad

Está relacionado con los gerentes TI que deben revisar periódicamente el cumplimiento de los procedimientos y procesamiento de información dentro de su área de responsabilidad con las políticas, estándares y cualquier otro requisito de seguridad apropiado.

A.5.7 Inteligencia de amenazas

El objetivo de la inteligencia de amenazas es proporcionar a las organizaciones una comprensión más profunda de las amenazas cibernéticas mediante la recopilación, el análisis y la contextualización de datos sobre ataques cibernéticos actuales y futuros. Un ejemplo de inteligencia de amenazas sería identificar las tácticas, técnicas y procedimientos (TTP) que usan los atacantes para ingresar a las redes o comprometer a sus objetivos. Como resultado, la defensa contra esos ataques específicos se vuelve más manejable.

A 8.12 fuga de datos

La fuga de datos se puede definir como el acceso, la transmisión o la extracción no autorizados de información por parte de personal y sistemas internos y externos, o entidades maliciosas que tienen como objetivo los sistemas de información de una organización. La fuga de datos es un problema frecuente para las organizaciones que gestionan grandes cantidades de datos, que van desde diferentes clasificaciones, en múltiples sistemas de TI, aplicaciones y SWITCHes de archivos distintos e interconectados.

A.8.16 monitoreo de la red

El monitoreo de la red es esencial para cualquier operación exitosa de soporte de TI y seguridad de la información. Las organizaciones deben implementar una estrategia de resolución de incidentes y seguridad de la información de extremo a extremo que marque hasta el último casillero al promover un enfoque proactivo para el monitoreo que tiene como objetivo prevenir incidentes antes de que ocurran y coordinar esfuerzos reactivos.

A.8.28 Codificación segura

Ayuda a las organizaciones a prevenir riesgos de seguridad y vulnerabilidades que pueden surgir debido a prácticas de codificación de software deficientes mediante el desarrollo, la implementación y la revisión de prácticas de codificación de software seguro adecuadas.

Circular Externa 33 del 2020 de la Superintendencia Financiera por medio de la cual se imparten Instrucciones relacionadas con la Taxonomía Única de Incidentes Cibernéticos TUIC, el formato para el reporte de métricas de seguridad de la información y ciberseguridad y el protocolo de etiquetado para el intercambio de información **TrafficLight Protocol (TLP)**

5.METODOLOGIA

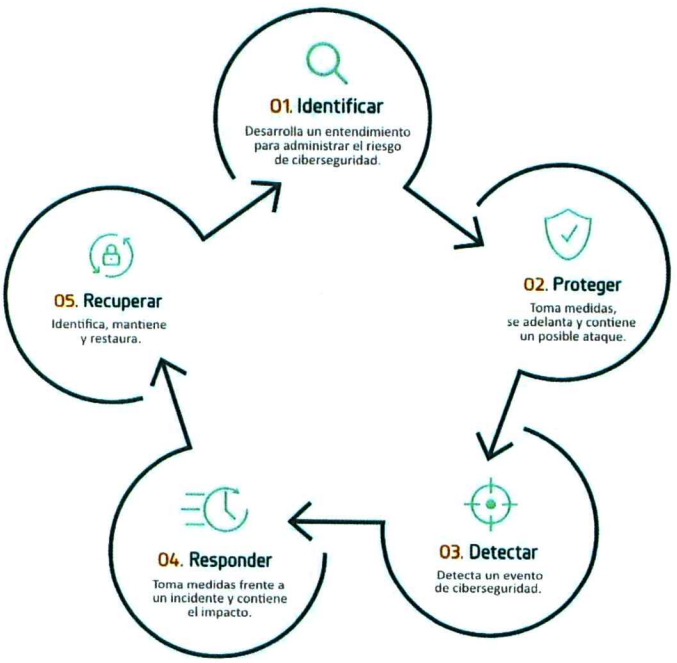


Ilustración 1.Metodología NIST.

Tomando como base el marco de ciberseguridad del **NIST**, y aportando todo el conocimiento en la definición e implantación de arquitecturas TEST-GRAVITY, desde IDENTIAN se proporcionan las mejores soluciones que ofrecen los niveles más altos de seguridad para todas las funciones identificadas en dicho marco:

Identificar: Posibilita determinar sistemas, activos, datos y competencia del negocio, su contexto, los recursos que soportan las funciones críticas y los riesgos que afectan al entorno.

Proteger: Permite diseñar y llevar a cabo contramedidas necesarias para contener el impacto del ciberataque.

Detectar: Facilita el diseño y la puesta en marcha de acciones necesarias para reaccionar frente a un ciberataque mediante la monitorización continua.

Responder: Incluye acciones necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contender el impacto que ocasiona.

Recuperar: Identifica las actividades necesarias para mantener planes de resiliencia y restaurar cualquier activo dañado debido a un incidente de ciberseguridad.

1. Planificación y Definición de Requisitos

1.1. Identificación de Objetivos

Definir objetivos de monitoreo: Disponibilidad, rendimiento, seguridad, capacidad, etc.

Determinar, definir y mantener los KPI (Key Performance Indicators): Métricas clave que se quieren monitorizar.

1.2. Análisis de Infraestructura

Inventario de recursos: Identificar, agregar, mantener y soportar todos los dispositivos y sistemas que serán monitoreados (SWITCHes, aplicaciones, dispositivos de red, etc.).

Requisitos de red y conectividad: Verificar, diagnosticar y mantener la conectividad entre los agentes, proxies y el SWITCH Zabbix.

1.3. Evaluación de Recursos

Requerimientos de hardware y software: Recomendar, validar y mantener los recursos necesarios para el SWITCH Zabbix, base de datos y almacenamiento.

Asignación de personal: Asignación del equipo que estará a cargo del mantenimiento y soporte Zabbix.

2. Diseño de la Arquitectura

2.1. Arquitectura del Sistema

SWITCH Zabbix: mantenimiento SWITCH principal el cual tiene ubicación on-premise.

Base de Datos: Seleccionar el tipo de base de datos y su configuración.

Agentes Zabbix: Mantenimiento y soporte de agentes en los dispositivos a monitorear.

2.2. Seguridad

Acceso y Autenticación: Definir políticas de acceso, autenticación y permisos para usuarios.

Seguridad de Datos: Implementar medidas de cifrado y asegurar la integridad de los datos de monitoreo.

3. Implementación

3.1. Instalación de nuevas características de Zabbix

Interfaz Web: Configurar la GUI de Zabbix y asegurar su accesibilidad segura.

3.2. Configuración de Proxies y Agentes

Proxies Zabbix: Instalar y configurar proxies si se necesitan.

Agentes Zabbix: Desplegar agentes en todos los dispositivos relevantes, configurar el monitoreo básico.

3.3. Plantillas de Monitoreo

Desarrollar Plantillas: Crear y soportar plantillas de monitoreo personalizadas para diferentes tipos de dispositivos y aplicaciones.

Aplicar Plantillas: Asociar las plantillas con los hosts correspondientes.

4. Pruebas y Validación

4.1. Pruebas de Funcionamiento

Verificar Conectividad: Asegurarse de que todos los agentes y proxies se comuniquen correctamente con el SWITCH Zabbix.

Pruebas de Monitoreo: Validar que las métricas y datos recogidos sean precisos y útiles.

4.2. Pruebas de Rendimiento

Carga del Sistema: Evaluar el rendimiento del sistema bajo carga esperada y ajustar configuraciones según sea necesario.

Optimización: Realizar ajustes para optimizar el rendimiento del SWITCH Zabbix y la base de datos.

5. Implementación en Producción

5.1. Despliegue

Desplegar en Producción: Mantener y soporta el despliegue de nuevas características en el entorno de producción.

5.2. Monitorización Continua

Monitoreo y Ajustes: Continuar monitoreando el rendimiento del sistema y realizar ajustes según sea necesario.

Actualizaciones y Mantenimiento: Planificar y ejecutar actualizaciones y mantenimiento regular del sistema Zabbix.

6. Capacitación y Documentación

6.1. Formación de Personal

Manuales y Documentación: Proporcionar documentación detallada sobre la configuración y operación del sistema.

6.2. Mejora Continua

Retroalimentación: Recoger retroalimentación de los usuarios y hacer mejoras continuas en la configuración de monitoreo.

Revisión Periódica: Realizar revisiones periódicas de la configuración y rendimiento del sistema para asegurarse de que sigue cumpliendo con los objetivos de monitoreo.

6.RIESGO

El personal **CGFM** debe identificar al personal que será contactado para las alertas críticas. Además, determinar quién se contactará primero, y sucesivamente bajo estos escenarios. Se define la siguiente matriz para las escalas de notificación de acuerdo con la clasificación de los eventos de la herramienta que permite clasificar los eventos de acuerdo con la criticidad del mismo clasificado de acuerdo con la matriz de impacto. Podemos interpretar mediante un parámetro de julior o menor probabilidad a que la alerta o vulnerabilidad pueda ser aprovechada, materializada y así generar una amenaza por parte de un adversario (interno o externo), hasta el momento en que sea mitigada o remediada totalmente.

FRECUENCIA /PROBABILIDAD/OCURRENCIA		
Frecuencia	**Descripción**	**Valor**
Muy probable	Es muy alta la probabilidad de ocurrencia del riesgo, normalmente la materialización del riesgo ocurre con frecuencia o recurrente.	5
Probable	La materialización del riesgo es posible que suceda varias veces en la vida laboral.	4
Moderado	Es posible que se materialice el riesgo alguna vez en la vida laboral, el riesgo puede materializarse en cualquier momento.	3
Improbable	No es esperable que se materialice el riesgo, aunque puede ser concebible, la probabilidad de que ocurra es baja, aunque puede presentarse.	2
Muy Improbable	No es esperable que se materialice el riesgo, la probabilidad de que ocurra un riesgo, es decir, que se materialice, es demasiado baja, casi nula.	1

Tabla.Criterios para determinar la probabilidad de ocurrencia.

IMPACTO		
Impacto	**Criterio** (Impacto del riesgo para el negocio)	**Valor**
Insignificante	**Impacto en el negocio Insignificante.** Se puede remediar rápidamente. (incluye el impacto ambiental) Nada reportable a la alta dirección. No hay productos o servicios no conformes. Mínima insatisfacción de personal o el cliente. 0,5% del total de los ingresos operacionales El riesgo está controlado.	2
Menor	**Impacto leve en el negocio.** Daños localizados. (incluye el impacto ambiental) Incidente reportable a la alta dirección. Afectación menor a la conformidad de productos y servicios. Algunos problemas de insatisfacción del personal o el cliente. Monto equivalente del 0,5% al 2,5% del total de los ingresos operacionales Bajo impacto en las medidas preventivas tomadas.	4
Moderado	**Impacto limitado en el negocio**. Impacto moderado en ciertos recursos. Incidente reportable a la alta dirección con seguimiento. Correcciones en productos o servicios no conformes. Problemas generalizados de insatisfacción del personal o el cliente. Monto equivalente del 2,6% al 5,0% del total de los ingresos operacionales La eficacia de los controles es moderada.	6
Julior	**Impacto serio en el negocio.** Impacto serio en los recursos. Significativa pérdida de mercado. Reportable a la alta dirección con seguimiento de su parte y acción correctiva. Correcciones a grupos de productos y servicios no conformes. Reportable a organismos legales con corrección. Alta rotación de personal. Monto equivalente del 5,1% al 7,4% del total de los ingresos operacionales Cuenta con medidas preventivas o correctivas con una eficacia baja.	8
Catastrófico	**Impacto desastroso en el negocio.** Daños juliores en gran cantidad de recursos. Dramática pérdida de mercado. Serios problemas legales (litigaciones, multas, cierre) Daños irreparables en la satisfacción de clientes y empleados. Cierre potencial del negocio, Monto equivalente del 7,5% en adelante del total de los ingresos operacionales. Las acciones preventivas o correctivas son nulas o no existen.	10

Tabla. Criterios para determinar el impacto.

PROBABILIDAD		IMPACTO				
		Insignificante	Menor	Moderado	Julior	Catastrófico
		2	4	6	8	10
Muy probable	5	10	20	30	40	50
Probable	4	8	16	24	32	40
Moderado	3	6	12	18	24	30
Improbable	2	4	8	12	16	20
Muy improbable	1	2	4	6	8	10

Tabla.Criterios para determinar el riesgo.

Sin clasificar (Not classified)

o Estas alertas se notificarán únicamente a través de la interfaz Web y no llevan asociada ninguna acción. No se ha definido ninguna alerta de este tipo para la plataforma de monitorización actual.

Información (Information)

Se notificarán a través de la interfaz Web y, dependiendo del tipo de alerta concreta, también se ejecutará una acción de envío de e-mail.Las alertas de este tipo que se han diseñado son:

- □ Aviso de reinicio en el SWITCH de Zabbix.
- □ Cambios en la configuración del host en el SWITCH de Zabbix.
- □ Cambio del nombre del SWITCH de Zabbix.

Advertencia (Warning)

Los criterios son los mismos que para el caso de las alertas de nivel Información.

Las alertas diseñadas para este nivel son:

- Enlace caído en un puerto de los conmutadores de la electrónica de red.
- Equipo sin conexión (electrónica de red).

  Carga de CPU excesiva durante los últimos 3 minutos en el SWITCH central Zabbix.

  Alta carga de procesador en el SWITCH central Zabbix.
- Excedido el 90% de uso de CPU en los equipos.
- Eventos de advertencia registrados en los Logs de Seguridad,Sistema y Aplicación correspondientes a los equipos de los
- Cambio de versión del agente Zabbix instalado en los equipos

Medio (Average)

La forma de actuar es la misma que para las alertas con nivel Información y Advertencia. Las alertas diseñadas para este nivel son:

Los demonios syslogd, sshd, inetd y mysqld no están ejecutándose en el SWITCH central Zabbix.

Demasiados usuarios conectados al SWITCH central Zabbix.

Falta de memoria libre en el SWITCH central Zabbix.

Cambios en la configuración de los ficheros /usr/sbin/sshd,/usr/bin/ssh, /etc/services, /etc/passwd, /etc/inetd.conf

Demasiados procesos ejecutándose en el SWITCH central Zabbix.

El SWITCH SSH no está ejecutándose en el SWITCH central Zabbix.

Falta de memoria libre en los equipos de los centros de control o en los SWITCHes

Reinicio de un SWITCH de grabación o de un equipo

Cambios en a configuración de fichero "au oexec.ba ".

Cambios en la información de los equipos

Alta carga de procesador en los equipos

Uso elevado de CPU en los equipos

Alto (High)

En este caso, la alerta se notificará a través de la interfaz Web y, en todos los casos, se enviará un correo electrónico informando del evento una vez se ha producido y otro correo electrónico una vez se haya solucionado el problema. Las alertas diseñadas para el nivel alto son:

Equipo sin conexión.

Bajo nivel de espacio en disco en el SWITCH central Zabbix.

El proceso zabbix_server no se está ejecutando en el SWITCH central Zabbix.

El proceso zabbix_agentd no se está ejecutando en el SWITCH central Zabbix.

El SWITCH de Apache no se está ejecutando en el SWITCH central.

El SWITCH HTTP no se está ejecutando en el SWITCH central.

El SWITCH central Zabbix está caído (no responde a conexión).

Demasiados procesos ejecutándose en el SWITCH central.

- Demasiados procesos ejecutándose en los equipos

Fallo en uno de los discos del RAID de almacenamiento



Temperatura de la CPU por encima de los 60°C

Bajo nivel de espacio disponible (<10 MB) en disco en los equipos

Espacio libre en disco por debajo del 5% de la capacidad total en los SWITCHes □

Eventos de error registrados en los Logs de Seguridad, Sistema y Aplicación correspondientes a los equipos

Crítico (Disaster)

Las consideraciones son las mismas que para el caso del nivel Alto.

Daño total de los equipos

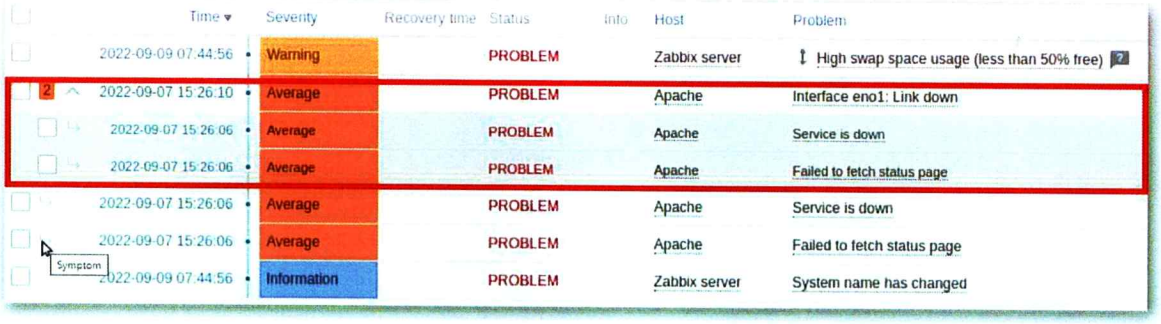


Tabla.Niveles de riesgo.

7.DIAGRAMA

Diagrama de red actual que identifica todas las conexiones entre el entorno de datos de la correlación. En esta pestaña podemos evidenciar un diagrama de la arquitectura de la plataforma de monitoreo, así como el detalle de recursos utilizados para la implementación en cada máquina. Dentro del diagrama se pueden apreciar los puertos a habilitar dentro de los diferentes servidores para que el sistema de monitoreo funcione de manera correcta.

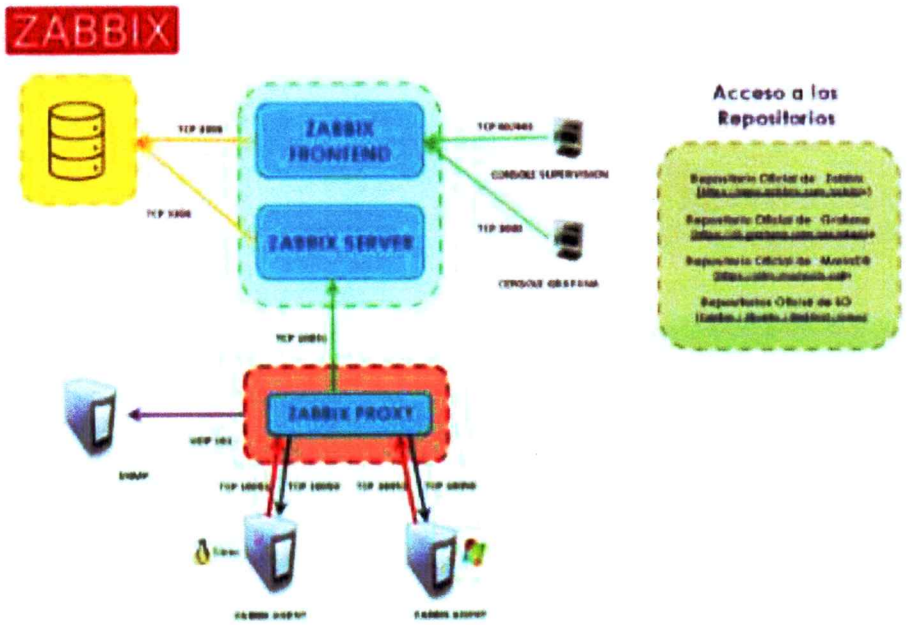


Ilustración 2.Diagrama de la correlación de eventos CGFM.

8.ACTIVOS

El análisis de la recolección de evidencias de este documento tiene como fin, poner al tanto a **COMANDO GENERAL DE LAS FUERZA MILITARES**

Este tipo de registros son aplicados a los siguientes activos:

NOMBRE	HOST	DESCRIPCION	IP	TIPO DE MONITOREO
AGREGACION	AGREGACION	SW DE AGREGACION	172.18.30.253	SNMP
AGRUPACION DE SEGURIDAD	AGRUPACION DE SEGURIDAD		172.18.30.28	SNMP
ALMACEN-COM-RIC	ALMACEN-COM-RIC		172.18.30.17	SNMP
BYPASS	BYPASS		172.18.30.60	SNMP
CAMPUS	CAMPUS		192.168.18.17	SNMP
CANCILLERIA-COGFM	CANCILLERIA-COGFM		172.18.30.37	SNMP
CCTV-INDUMIL	CCTV-INDUMIL		172.18.30.42	SNMP
CENTRO DE MONITOREO CCTV	CENTRO DE MONITOREO CCTV		172.18.30.29	SNMP
CGADCHRONOS	CGADCHRONOS	SWITCH AD	172.18.1.12	AGENTE ZABBIX
CGADPIJAO01	CGADPIJAO01	SWITCH AD	172.18.1.13	AGENTE ZABBIX
CGALFA	CGALFA		172.18.42.120	AGENTE ZABBIX
CGBETA	CGBETA		172.18.42.121	AGENTE ZABBIX
CGDUJO	CGDUJO	NODO CGDUJO	172.18.42.92	AGENTE ZABBIX
CGKOGI	CGKOGI	NODO CGKOGI	172.18.42.93	AGENTE ZABBIX
CGMATAPI	CGMATAPI	NODO MATAPI	172.18.42.94	AGENTE ZABBIX
CGNUKAK	CGNUKAK	BACKUP NUKAK	172.18.42.95	AGENTE ZABBIX
CGPIJAO	CGPIJAO	SERVER FILE CGPIJAO	172.18.42.171	AGENTE ZABBIX
CGPISAMIRA	CGPISAMIRA	NODO CGPISAMIRA	172.18.42.91	AGENTE ZABBIX

CGYAGUA	CGYAGUA	NODO CGYAGUA	172.18.42.90	AGENTE ZABBIX
CONTROL-ACCESO-VEHICULAR	CONTROL-ACCESO-VEHICULAR		172.18.30.254	SNMP
DCCA CALL CENTER	DCCA CALL CENTER		172.18.30.49	SNMP
DCCAE	DCCAE		172.18.30.50	SNMP
GESTION_ORACLE	GESTION_ORACLE		172.18.30.10	SNMP
GPON1	GPON1	SWITCH REDES	172.18.42.206	AGENTE ZABBIX
GRUPO-SEGURIDAD	GRUPO-SEGURIDAD		172.18.30.28	SNMP
GUARDIA-MODULOS	GUARDIA-MODULOS		172.18.30.65	SNMP
GUARDIA ANTIGUA	GUARDIA ANTIGUA		172.18.30.27	SNMP
GUARDIA GENERALES	GUARDIA GENERALES		172.18.30.40	SNMP
RED_MOVIL_DIGITAL	RED_MOVIL_DIGITAL		172.18.30.19	SNMP
SISTEMAS-RIC	SISTEMAS-RIC		172.18.30.16	SNMP
SUPERVISION-RIC	SUPERVISION-RIC		172.18.30.15	SNMP
SW CORE 7500	SW CORE 7500	CORE	172.18.30.254	SNMP
TRANSPORTES	TRANSPORTES		172.18.30.32	SNMP
Zabbix server	Zabbix server		172.16.42.86	SWITCH ZABBIX
Zabbix_DB	Zabbix_DB		172.16.42.87	SWITCH ZABBIX
Zabbix_Proxy_01	Zabbix_Proxy_01		172.16.42.88	SWITCH ZABBIX

Tabla. Activos CGFM.

La siguiente es la tabla de registros solicitados por **CGFM** muestra el cumplimiento de cada uno de los activos monitoreado durante el mes de julio:

SEVERIDAD	FECHA	STATUS	HOST	INCIDENTE	DURACION	TIPO
High	2024-03-22 15:21:01	PROBLEM	Zabbix server	Sitios Web	2M 1d 23h	
High	2024-02-29 13:15:12	PROBLEM	CGNUKAK	High disk space utilization	2M 24d 2h	Application: ChatBot, Application: Filesystem C:,

				(over 95%) on volumen C:		Application: Filesystems
High	2023-11-09 8:40:38	PROBLEM	Zabbix_DB	Unavailable by ICMP ping	6M 16d 6h	Application: Status, Availability: Yes
High	3/22/2024 15:21	PROBLEM	Zabbix server	Sitios Web	2M 1d 23h	
High	2/29/2024 13:15	PROBLEM	CGNUKAK	High disk space utilization (over 95%) on volumen C:	2M 24d 2h	Application: ChatBot, Application: Filesystem C:, Application: Filesystems
High	11/9/2023 8:40	PROBLEM	Zabbix_DB	Unavailable by ICMP ping	6M 16d 6h	Application: Status, Availability: Yes
High	3/22/2024 15:21	PROBLEM	Zabbix server	Sitios Web	2M 1d 23h	
High	2/29/2024 13:15	PROBLEM	CGNUKAK	High disk space utilization (over 95%) on volumen C:	2M 24d 2h	Application: ChatBot, Application: Filesystem C:, Application: Filesystems
High	11/9/2023 8:40	PROBLEM	Zabbix_DB	Unavailable by ICMP ping	6M 16d 6h	Application: Status, Availability: Yes

Tabla.Eventos críticos

Activos desconectados

Guardia-modulos 172.18.30.66

Campus 192.168.18.17

NOTA: Se adjunta anexo1 de incidentes CGFM para su consulta.

8.1 ESTADO POR AGENTE

Items

Los ítems son las métricas de datos que se recogen. Un host necesita tener ítems para todos los aspectos que se quieran monitorizar. Estos valores se pueden obtener mediante snmp, agente instalado, comprobaciones externas u otros protocolos. Por ejemplo, se puede utilizar snmp para comprobar el estado de las interfaces de un dispositivo para revisar que se encuentra levantada. Zabbix cada X tiempo realizará consultas para recoger el estado y tener valores actualizados del estado de las interfaces.

Triggers

Los Triggers son expresiones que sirven para generar alertas ante ciertas condiciones. Utilizando los ítems se genera una expresión lógica para comparar el valor recogido con un umbral. De la misma forma que una interfaz caída genera una alerta, se puede configurar que cuando la interfaz vuelva a estar operativa se solucione la alerta y no aparezca en el dashboard.

Templates

Los templates permiten crear, como su nombre indica, plantillas para definir una estructura de métricas y alertas que aplicar a un host.

En nuestro caso el objetivo es agrupar todas las métricas necesarias para cumplir con la baseline en una template.

Las templates se pueden anidar e incluir otras templates en su interior. Zabbix dispone de un conjunto bastante extenso de templates.

Para nuestro caso se ha creado una template nueva y anidado varias templates sencillas para comprobar el estado superficial del estado de la máquina; como el acceso por ICMP ping, estado y accesibilidad de SNMP, o estado del servicio del agente de Zabbix

8.2 ESTADO DE LOS SERVICIOS

Servicio URL

Zabbix http://monitoreo.cgfm.mil.co/zabbix/

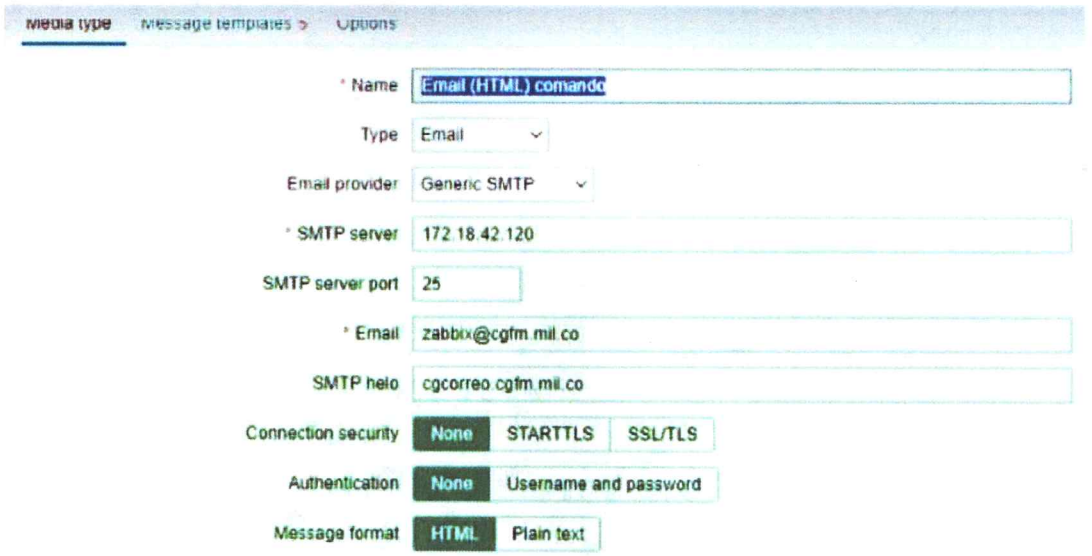
Grafana http://monitoreo.cgfm.mil.co:3000

El Zabbix Proxy es considerado una extensión o brazo del Zabbix Server, ya que tiene la posibilidad de ejecutar las mismas funciones de monitoreo que la cabeza de la operación. Su utilización trae muchas ventajas, como la de delegar cargas de procesamiento de nuestros servidores y la posibilidad de gestionar los accesos de monitoreo más fácilmente, esto en caso de que existan firewalls o reglas de seguridad de por medio.

Alias	Nombre	Apellido	e-mail	Group	User type
alex.balaguera	Alex	Balaguera Gutierrez	alex.balaguera@unisimon.edu.co	Todo	Administrador
brenner.pinilla	Brenner	Pinilla Padilla	brenner.pinilla@unisimon.edu.co	Todo	Administrador
nelson.cardozo	Nelson	Cardozo Salas	nelson.cardozo@unisimon.edu.co	Todo	Administrador
francisco.pautt	Francisco Jose	Pautt Lopez	francisco.pautt@unisimon.edu.co	Todo	Administrador

Como se evidencia se tiene el cerebro de la operación etiquetado como Zabbix Server que comprende un servidor mencionado en la sección anterior. El Zabbix Server se enlaza a nodo de base de datos MariaDB a donde almacenará toda la información.

Finalmente, el sistema se vincula con un Zabbix Proxy, con el fin de mejorar el performance de la herramienta.

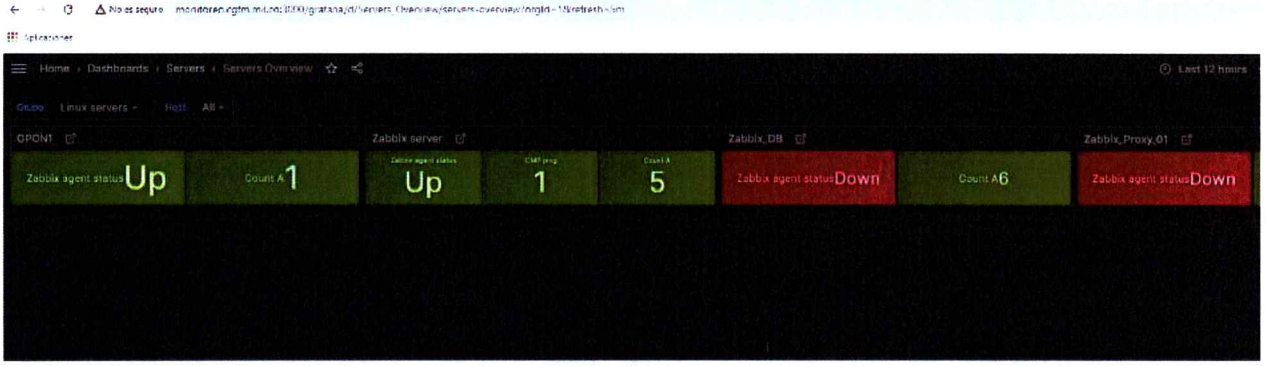


En estos dashboards se podrá encontrar el resumen de todos los sistemas integrados y su respectiva redirección a los dashboards específicos.

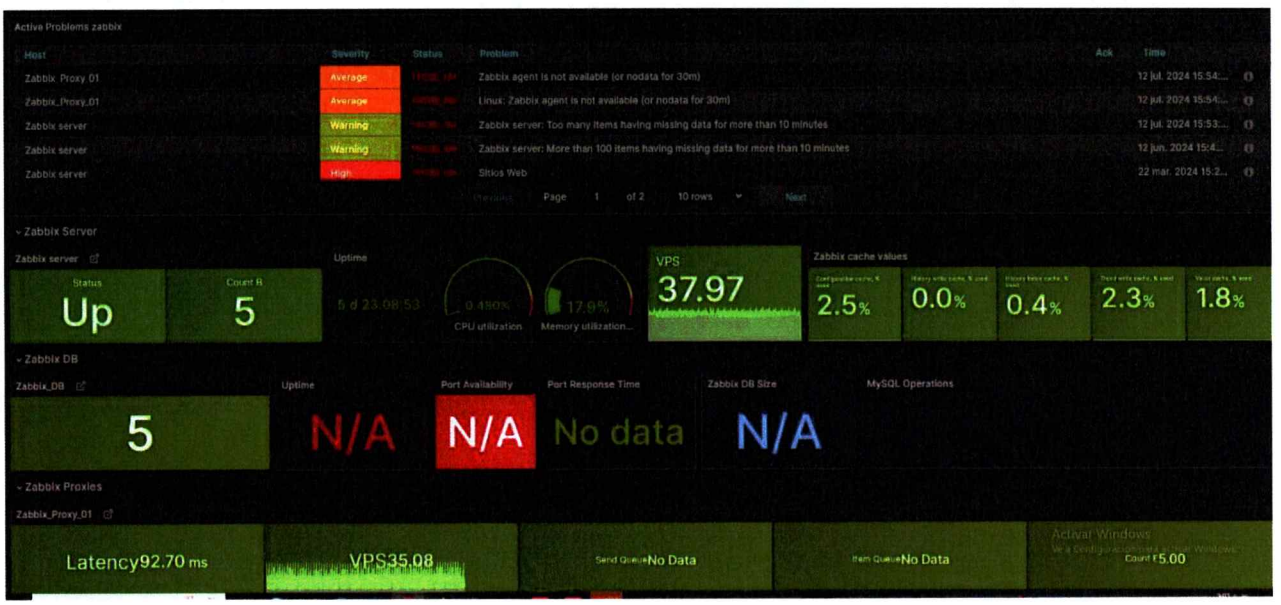
Se evidencia que hay 5 switch por fuera .Es necesario el enrolamiento de estos activos al monitoreo nuevamente.

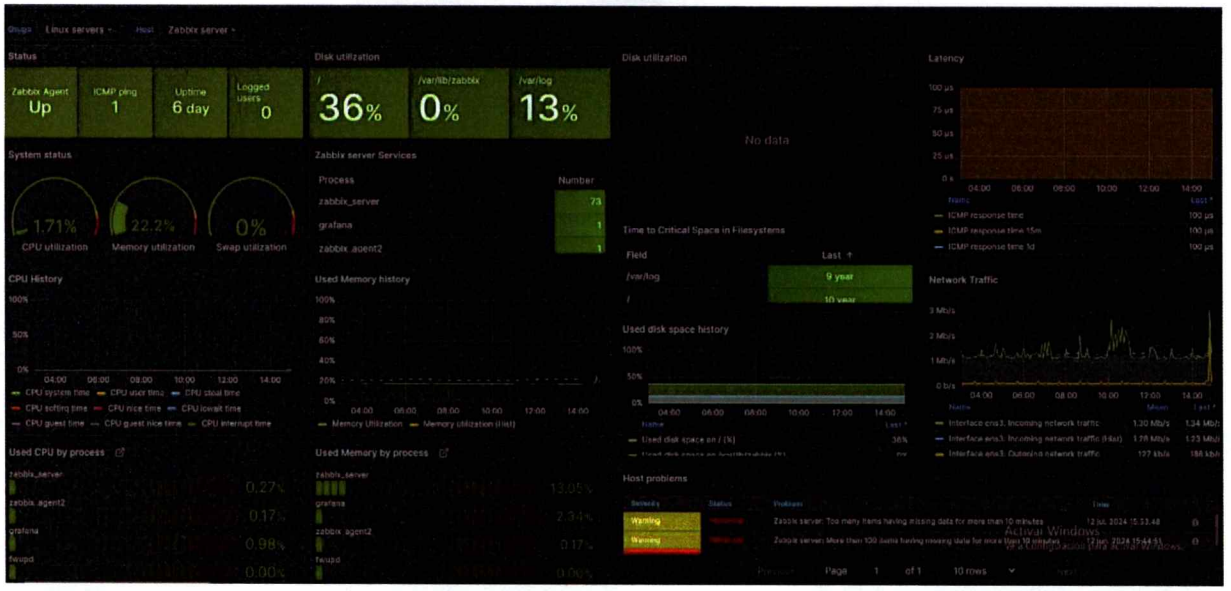


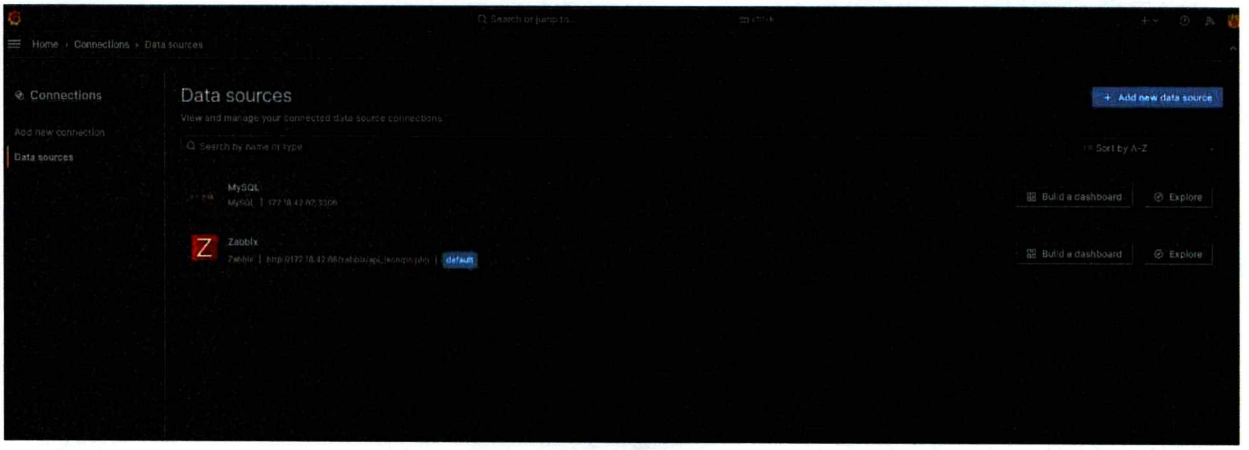
Los servidores están operacionales y en correcto funcionamiento:

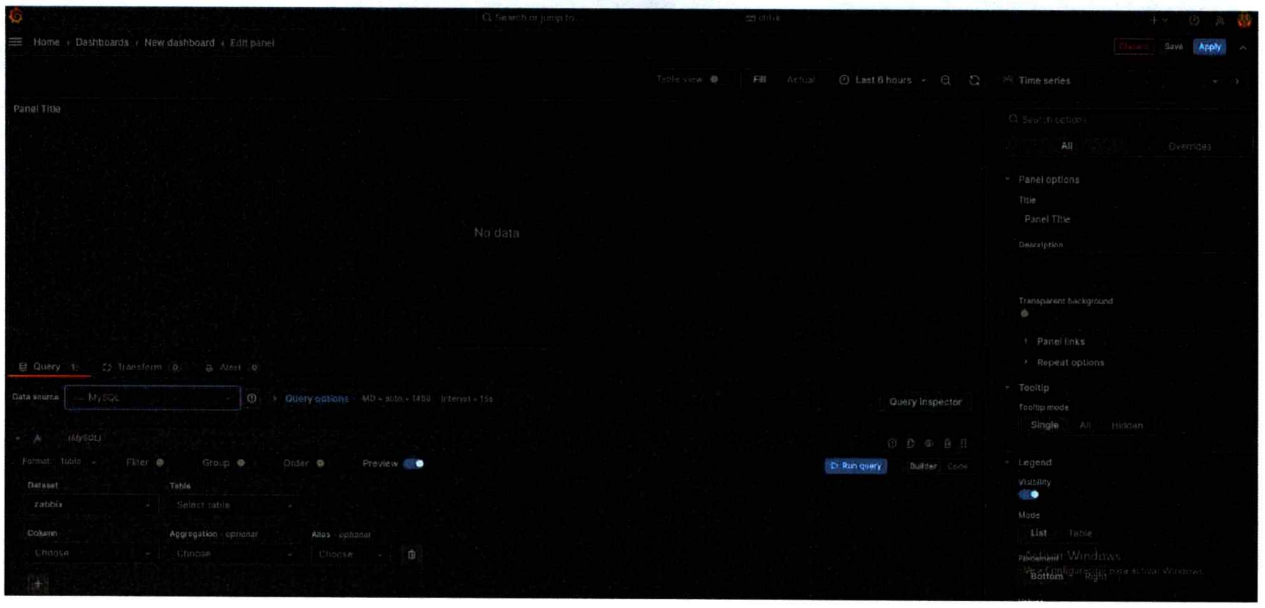




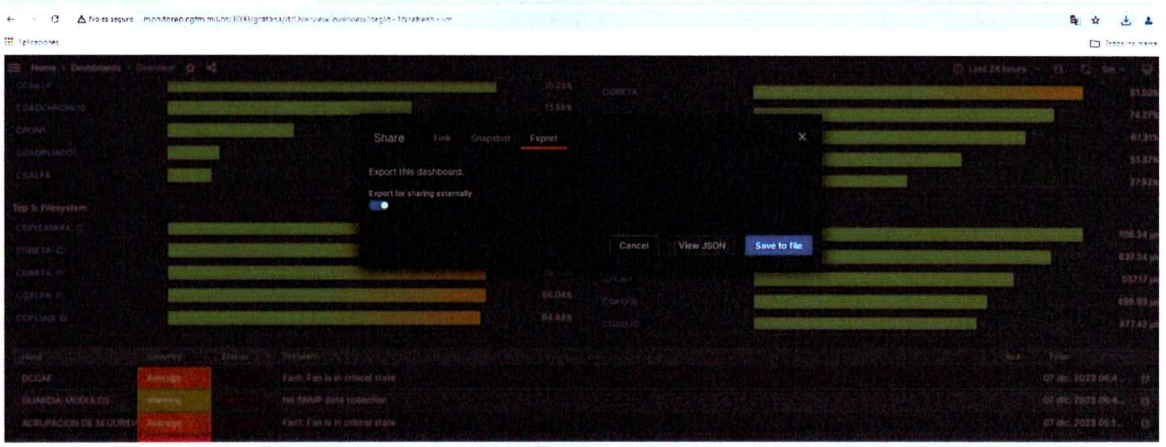



Linux servers
Zabbix server
Status
Zabbix Agent
Up
ICMP ping
1
Uptime
6 day
Logged users
0
Disk utilization
/
36%
/var/lib/zabbix
0%
/var/log
13%
Disk utilization
No data
Latency
System status
1.71%
CPU utilization
22.2%
Memory utilization
0%
Swap utilization
Zabbix server Services
Process
Number
zabbix_server
grafana
zabbix_agent2
Time to Critical Space in Filesystems
Field
Last
/var/log
9 year
/
10 year
Network Traffic
CPU History
Used Memory history
Used disk space history
Used CPU by process
Used Memory by process
Host problems
Warning
Warning
Page 1 of 1
10 rows


Home › Connections › Data sources
Connections
Add new connection
Data sources
Data sources
View and manage your connected data source connections
Add new data source
Search by name or type
Sort by A-Z
MySQL
Build a dashboard
Explore
Zabbix
default
Build a dashboard
Explore


Home › Dashboards › New dashboard › Edit panel
Discard
Save
Apply
Panel Title
Table view
Fill
Actual
Last 6 hours
Time series
No data
Query
Transform
Alert
Data source
MySQL
Query options
Query inspector
Run query
Builder
Code
Panel options
Title
Panel Title
Description
Transparent background
Panel links
Repeat options
Tooltip
Tooltip mode
Single
All
Hidden
Legend
Visibility
Mode
List
Table
Placement
Bottom
Right

Recomendamos crear nuevos dashboard a partir de la herramienta Grafana, que se ajusten a las necesidades de la operación.

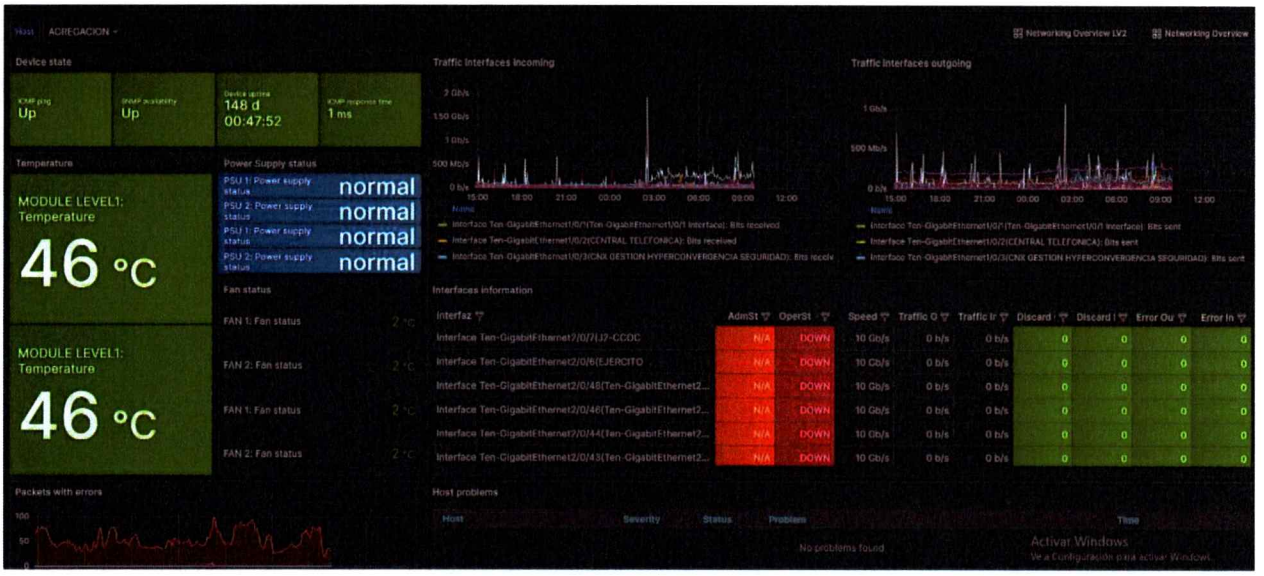




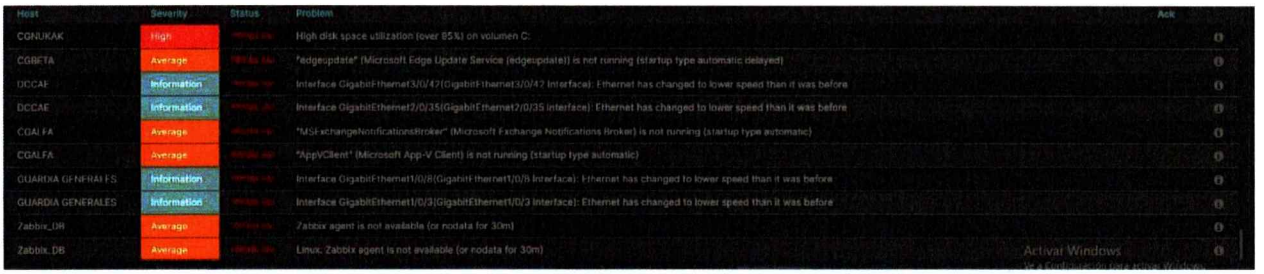


Severity	Time	Status	Host	Problem	Duration	Ack	Actions	Tags
High	7/12/2024 15:54	PROBLEM	CGADCHRONOS	System time is out of sync (diff with Zabbix server > 600s)	5d 22h 56m	No	Actions (3)	Component : General
High	7/12/2024 15:52	PROBLEM	CGADPIJAO01	System time is out of sync (diff with Zabbix server > 600s)	5d 22h 58m	No	Actions (3)	Component : General
High	7/12/2024 15:49	PROBLEM	CGALFA	System time is out of sync (diff with Zabbix server > 600s)	5d 23h	No	Actions (3)	Component : General
High	7/12/2024 15:49	PROBLEM	CGMATAPI	System time is out of sync (diff with Zabbix server > 600s)	5d 23h 1m	No	Actions (3)	Component : General
High	7/12/2024 15:49	PROBLEM	CGBETA	System time is out of sync (diff with Zabbix server > 600s)	5d 23h 1m	No	Actions (3)	Component : General
High	7/12/2024 15:48	PROBLEM	CGYAGUA	System time is out of sync (diff with Zabbix server > 600s)	5d 23h 1m	No	Actions (3)	Component : General
High	7/12/2024 15:48	PROBLEM	CGDUJO	System time is out of sync (diff with Zabbix server > 600s)	5d 23h 2m	No	Actions (3)	Component : General
High	7/12/2024 15:46	PROBLEM	CGPIJAO	System time is out of sync (diff with Zabbix server > 600s)	5d 23h 3m	No	Actions (3)	Component : General
High	7/12/2024 15:46	PROBLEM	CGPISAMIRA	System time is out of sync (diff with Zabbix server > 600s)	5d 23h 4m	No	Actions (3)	Component : General
High	7/12/2024 15:45	PROBLEM	CGKOGI	System time is out of sync (diff with Zabbix server > 600s)	5d 23h 4m	No	Actions (3)	Component : General
High	7/12/2024 15:45	PROBLEM	GPON1	System time is out of sync (diff with Zabbix server > 600s)	5d 23h 4m	No	Actions (3)	Application : General
High	3/22/2024 15:21	PROBLEM	Zabbix server	Sitios Web	3M 27d 23h	No	Actions (3)	
High	2/29/2024 13:15	PROBLEM	CGNUKAK	High disk space utilization (over 95%) on volumen C:	4M 20d 1h	No	Actions (3)	Application : ChatBot, Application : Filesystem C:, Application : Filesystems
High	11/9/2023 8:40	PROBLEM	Zabbix_DB	Unavailable by ICMP ping	8M 12d 6h	No		Application : Status, Availability: Yes

Tabla. Aletas CGFM.



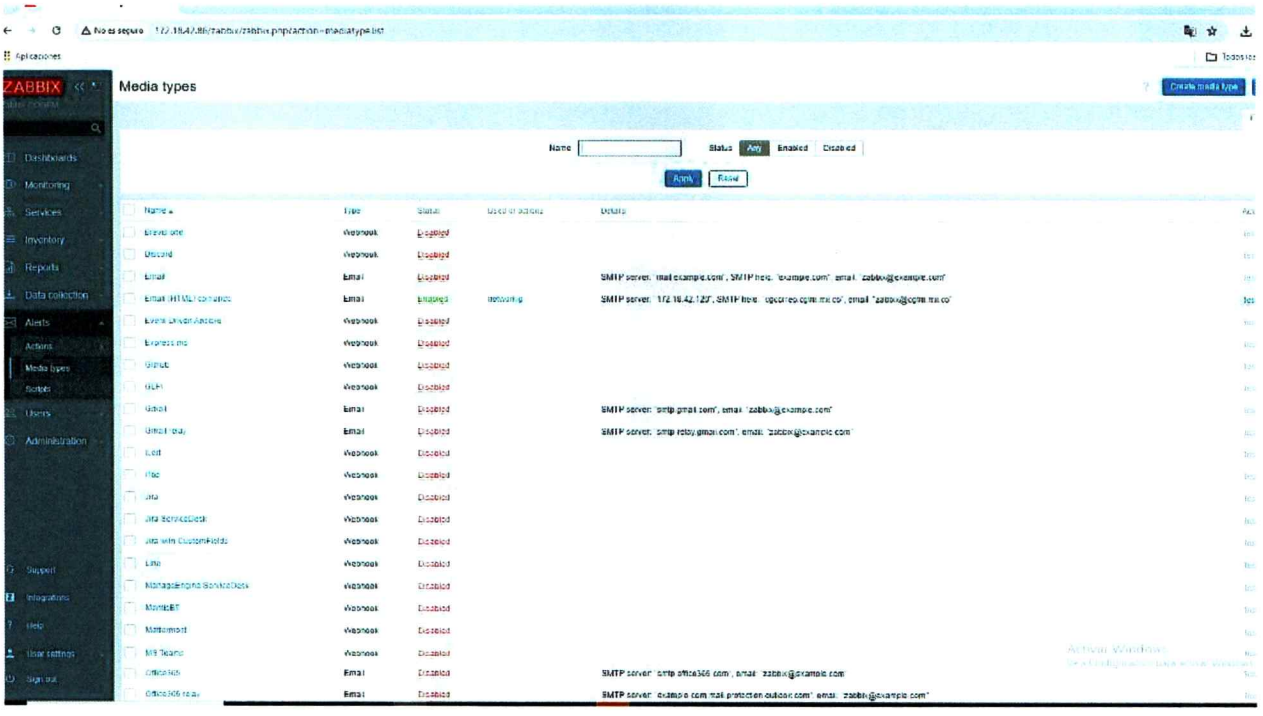
Se pueden observar múltiples incidencias reportadas por la herramienta de monitoreo entre estos:

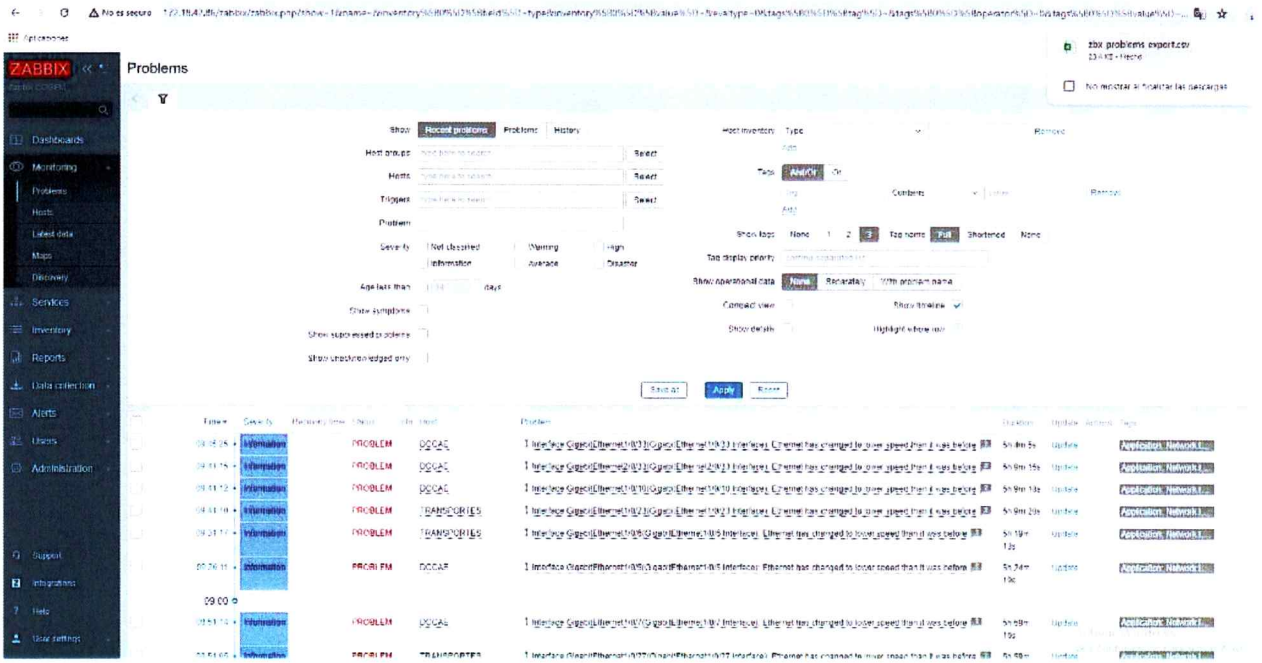


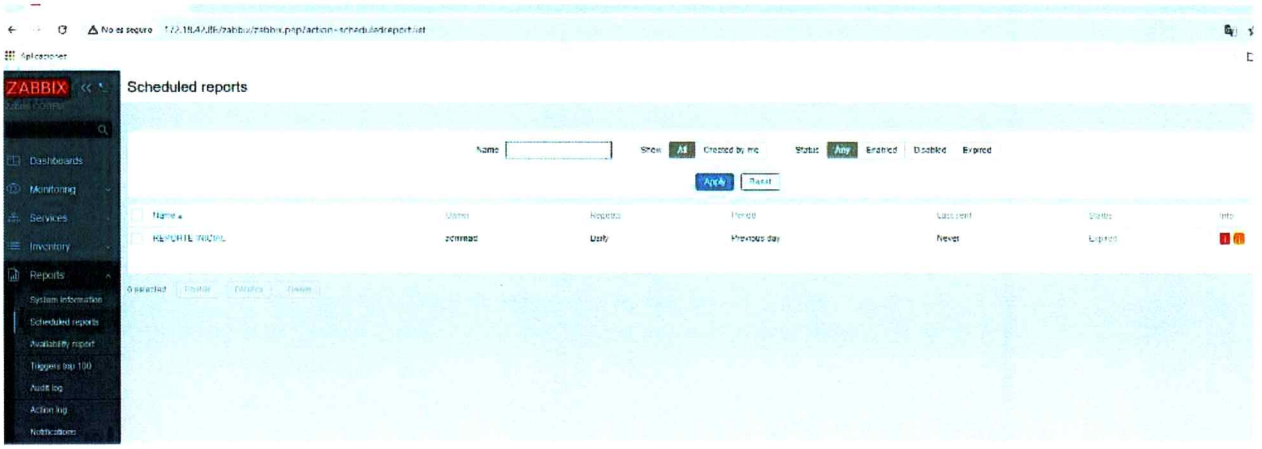


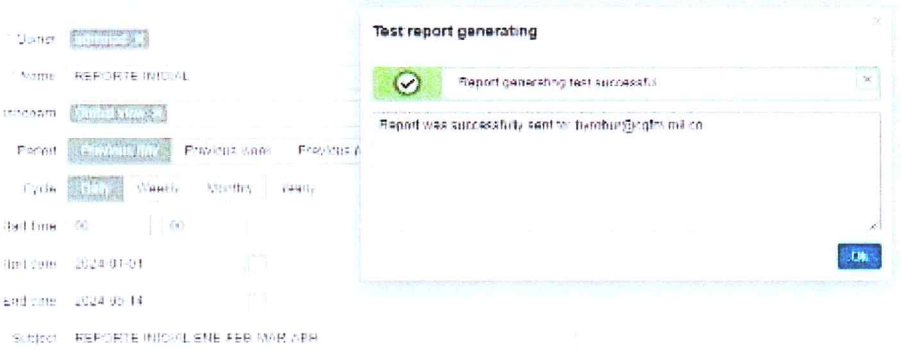
Se evidencia falta de espacio y sitio web caído en los activos .se recomiendo validar en conjunto esta incidencia criticas dentro de la infraestructura.



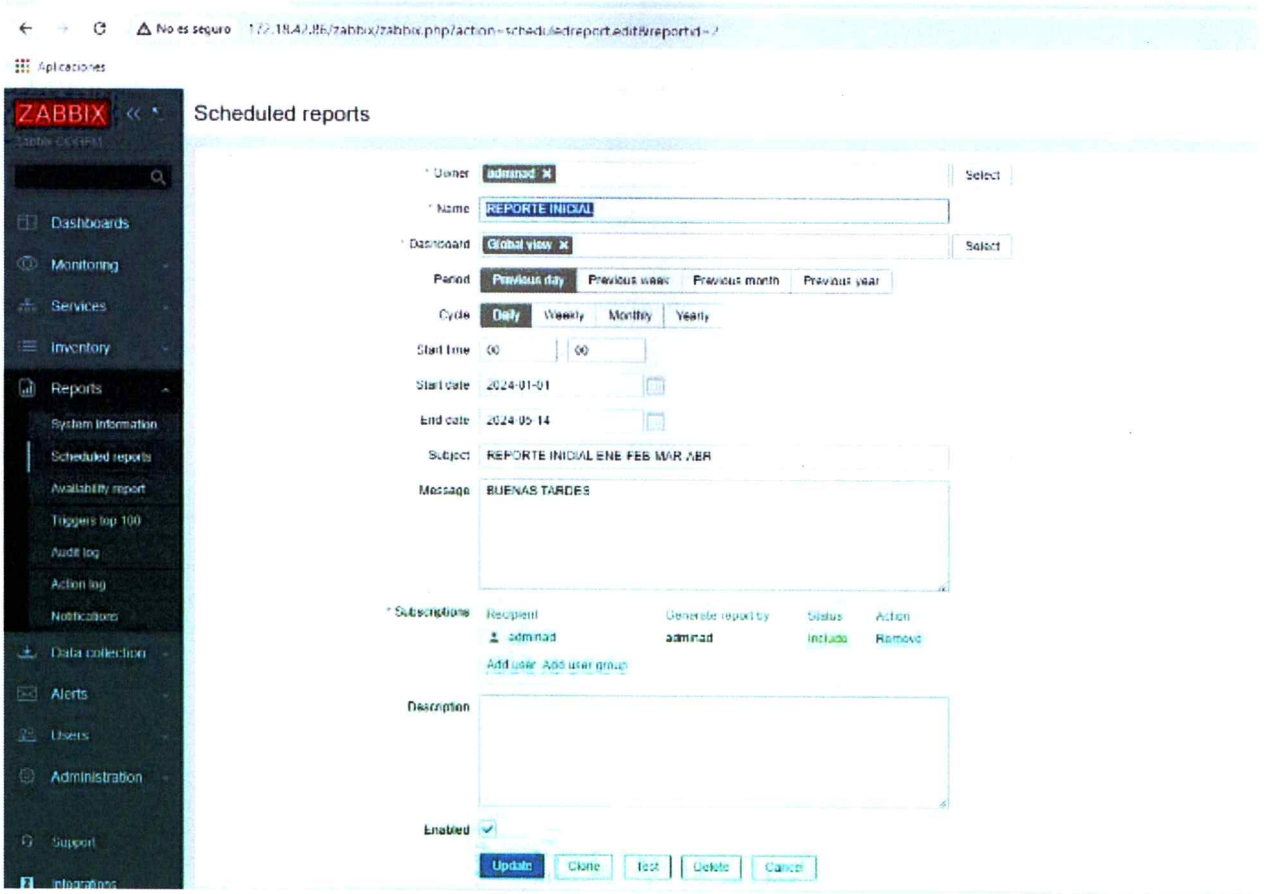


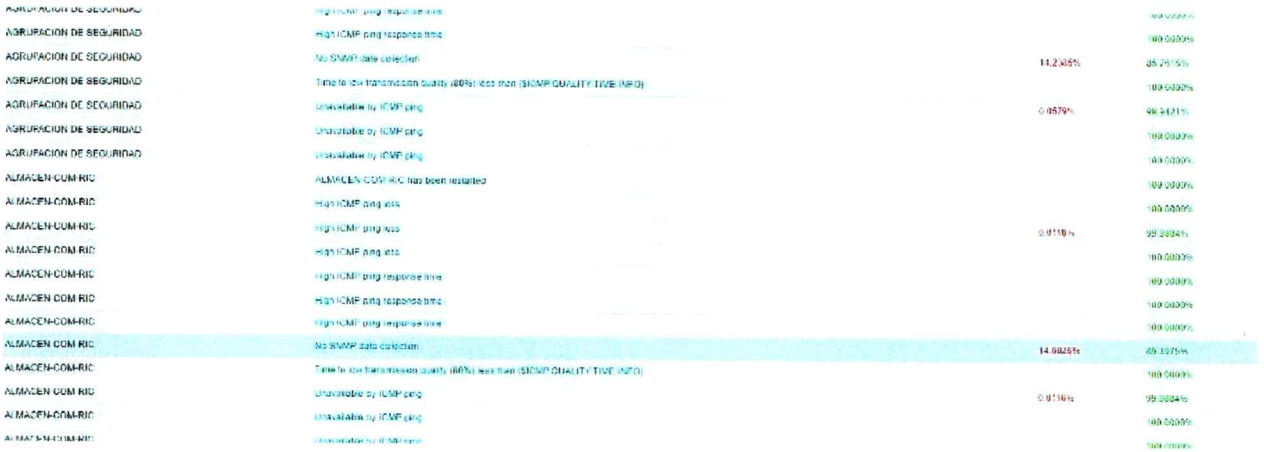

ZABBIX
Problems
Dashboards
Monitoring
Problems
Hosts
Latest data
Maps
Discovery
Services
Inventory
Reports
Data collection
Alerts
Users
Administration
Support
Integrations
Help
User settings
Apply
Reset


ZABBIX
Scheduled reports
Dashboards
Monitoring
Services
Inventory
Reports
System information
Scheduled reports
Availability report
Triggers top 100
Audit log
Action log
Notifications
Apply
Reset


Test report generating
Report generating test successful
Report was successfully sent to
Ok
Owner
Name
REPORTE INICIAL
Period
Cycle
Start time
Start date
End date
Subject

Se ha validado la entrega de reporte automático por pdf a través del correo. Sobre este reporte es necesario incluir el activo correspondiente y el responsable de dicho activo.




AGRUPACION DE SEGURIDAD
AGRUPACION DE SEGURIDAD
AGRUPACION DE SEGURIDAD
AGRUPACION DE SEGURIDAD
AGRUPACION DE SEGURIDAD
AGRUPACION DE SEGURIDAD
AGRUPACION DE SEGURIDAD
ALMACEN-COM-RIC
ALMACEN-COM-RIC
ALMACEN-COM-RIC
ALMACEN-COM-RIC
ALMACEN-COM-RIC
ALMACEN COM RIC
ALMACEN-COM-RIC
ALMACEN COM RIC
ALMACEN-COM-RIC
ALMACEN-COM-RIC
ALMACEN COM RIC
ALMACEN-COM-RIC
ALMACEN-COM-RIC
ALMACEN COM

CANCILLERIA-COGFM	Unavailable by ICMP ping	0.3535%	99.6465%
CANCILLERIA-COGFM	Unavailable by ICMP ping		100.0000%
CANCILLERIA-COGFM	Unavailable by ICMP ping		100.0000%
CCTVINDUVIL	CCTV-SCADA has been added		100.0000%
CCTVINDUVIL	High ICMP ping loss	2.3545%	97.6455%
CCTVINDUVIL	High ICMP ping loss	2.5275%	97.4725%
CCTVINDUVIL	High ICMP ping loss	1.4815%	98.5185%
CCTVINDUVIL	High ICMP ping response time		100.0000%
CCTVINDUVIL	High ICMP ping response time		100.0000%
CCTVINDUVIL	High ICMP ping response time		100.0000%
CCTVINDUVIL	No SNMP data collection	19.2481%	80.7519%
CCTVINDUVIL	Time to live exceeded (ttl = 0 eq)		100.0000%
CCTVINDUVIL	Unavailable by ICMP ping	19.4954%	80.5046%
CCTVINDUVIL	Unavailable by ICMP ping	19.2969%	80.7031%
CCTVINDUVIL	Unavailable by ICMP ping	20.0579%	79.9421%
CENTRO DE MONITOREO CCTV	CENTRO DE MONITOREO CCTV has been restarted		100.0000%
CENTRO DE MONITOREO CCTV	High ICMP ping loss		100.0000%
CENTRO DE MONITOREO CCTV	High ICMP ping loss		100.0000%

COBETA	4 H_ Disk is overloaded (util > 95% for 15m)	Warning	10
CODUJO	5_ Disk is overloaded (util > 95% for 15m)	Warning	10
COFRAMIRA	10_Disk is overloaded (util > 95% for 15m)	Warning	10
CONUKAK	14 E_ Disk is overloaded (util > 95% for 15m)	Warning	10
COADELA001	Host has been restarted (uptime < 10m)	Warning	10
Zabbix_Proxy_01	Linux: Number of installed packages has been changed	Warning	10
COPAJAO	The Memory Pagesisec is too high (over 1000 for 15m)	Warning	10
COALTA	Time to Critical Space less than 30d or 0	Warning	10
COPAJAO	1 D_ Disk is overloaded (util > 95% for 15m)	Warning	9
COFRAMIRA	5_Disk is overloaded (util > 95% for 15m)	Warning	8
COBETA	6 J_ Disk is overloaded (util > 95% for 15m)	Warning	8
COMATAPI	12_Disk is overloaded (util > 95% for 15m)	Warning	8
GUARDIA GENERALES	High ICMP ping loss	Warning	8
ALMACEN-COMERCIO	High ICMP ping loss	Warning	8
COYAQUA	Host has been restarted (uptime < 10m)	Warning	8
Zabbix DB	Linux: Number of installed packages has been changed	Warning	8
COBETA	Unavailable by ICMP ping	Warning	8
COYAQUA	Unavailable by ICMP ping	Warning	8
CONUKAK	Unavailable by ICMP ping	Warning	8
COBETA	Unavailable by ICMP ping	High	8
COYAQUA	Unavailable by ICMP ping	High	8
GUARDIA GENERALES	Unavailable by ICMP ping	High	8
GUARDIA-MODULO 8	Unavailable by ICMP ping	High	8
CENTRO DE MONITOREO CCTV	Unavailable by ICMP ping	High	8
CANCILLERIA-COGFM	Unavailable by ICMP ping	High	8
COMATAPI	Unavailable by ICMP ping	High	8
Zabbix server	Utilization of ODBC poller processes over 60%	High	6

Host	Trigger	Severity	Number of ev
CCTVINDUVIL	No SNMP data collection	Warning	1512
COMATAPI	8 Disk is overloaded (util > 95% for 15m)	Warning	742
COKOGI	9_Disk is overloaded (util > 95% for 15m)	Warning	515
CCTVINDUVIL	Unavailable by ICMP ping	Warning	476
CONUKAK	11 F_ Disk is overloaded (util > 95% for 15m)	Warning	459
COYAQUA	9_Disk is overloaded (util > 95% for 15m)	Warning	454
COMATAPI	The Memory Pagesisec is too high (over 1000 for 15m)	Warning	440
ASEGURACION DE SEGURIDAD	Interface GigabitEthernet1/0/40(GigabitEthernet1/0/40 Interface): In half duplex mode	Warning	360
Zabbix Proxy_01	Utilization of poller processes over 75%	Warning	360
GRUPO SEGURIDAD	Interface GigabitEthernet1/0/40(GigabitEthernet1/0/40 Interface): In half duplex mode	Warning	359
CCTVINDUVIL	Unavailable by ICMP ping	High	331
COBETA	1 E_ Disk is overloaded (util > 95% for 15m)	Warning	279
COYAQUA	The Memory Pagesisec is too high (over 1000 for 15m)	Warning	264
COKOGI	The Memory Pagesisec is too high (over 1000 for 15m)	Warning	240
CONUKAK	8 C_ Disk is overloaded (util > 95% for 15m)	Warning	230
Zabbix server	Zabbix server: Too many items having missing data for more than 10 minutes	Warning	227
COBETA	6 D_ Disk is overloaded (util > 95% for 15m)	Warning	195
CODUJO	10_Disk is overloaded (util > 95% for 15m)	Warning	194
COKOGI	13_Disk is overloaded (util > 95% for 15m)	Warning	178
COKOGI	10_Disk is overloaded (util > 95% for 15m)	Warning	162
COYAQUA	14_Disk is overloaded (util > 95% for 15m)	Warning	160
COPACHECO02	CPU queue length is too high (over 3 for 15m)	Warning	152

Sobre la incidencias críticas se le informa al personal a cargo sobre la situación para tener un escalamiento claro de las incidencias internas.

SWITCH AGREACION 172.18.30.253

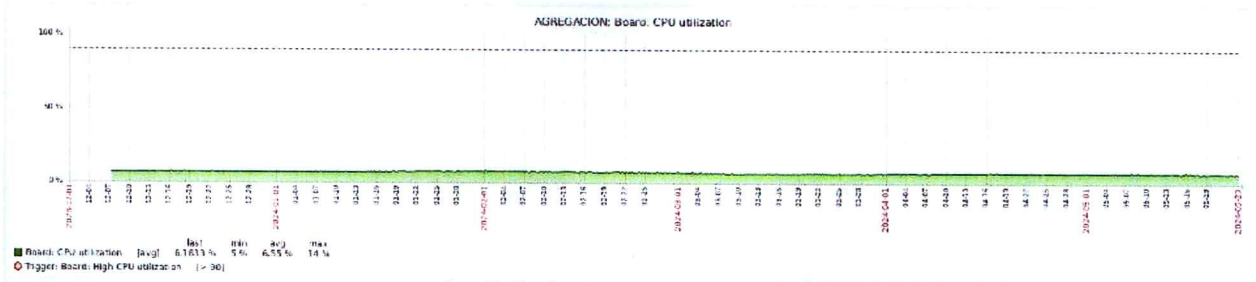


Imagen. Uso de CPU SWITCH de agregación

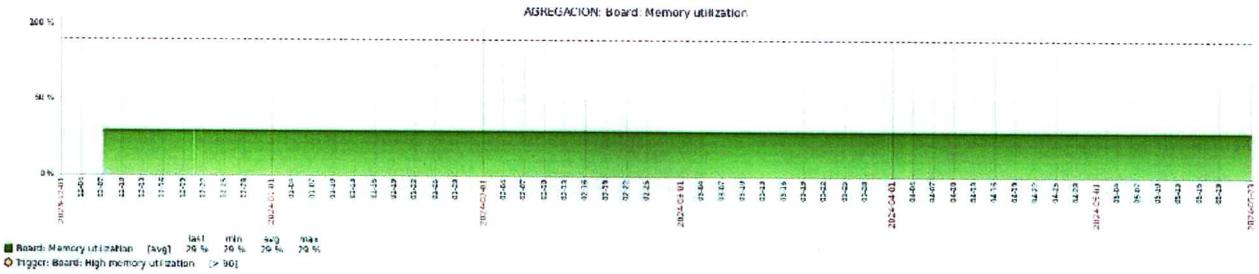


Imagen. Utilización de memoria SWITCH de agregación

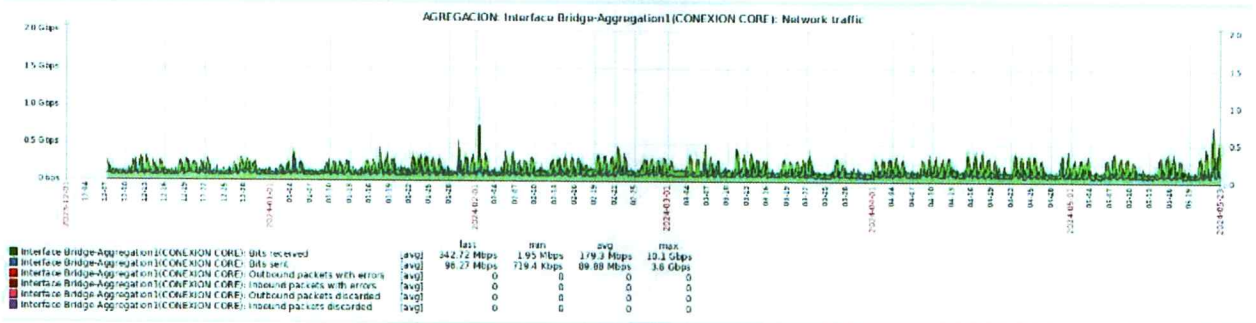


Imagen. Utilización de red SWITCH de agregación

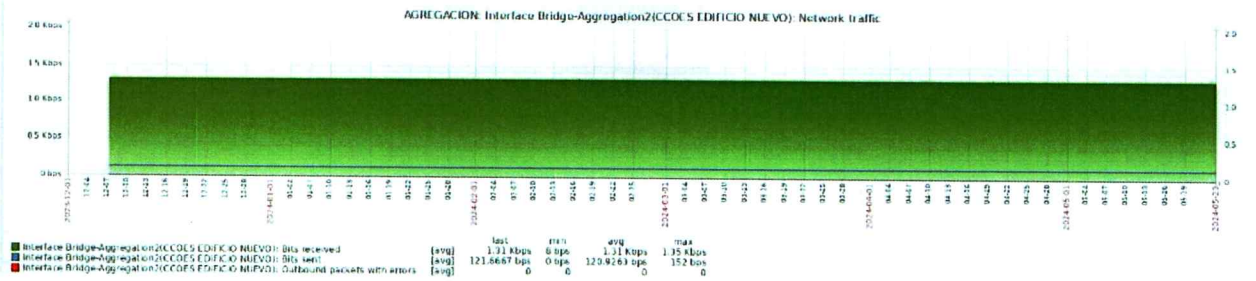


Imagen. Utilización de red SWITCH de agregación(CCOES EDIFICO NUEVO)

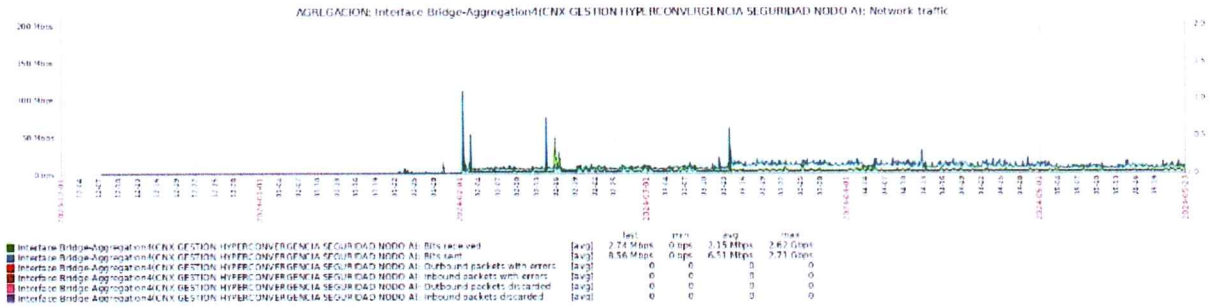


Imagen. Utilización de red SWITCH de agregación(GESTION DE HYPERCONVERGENCIA NODO A)

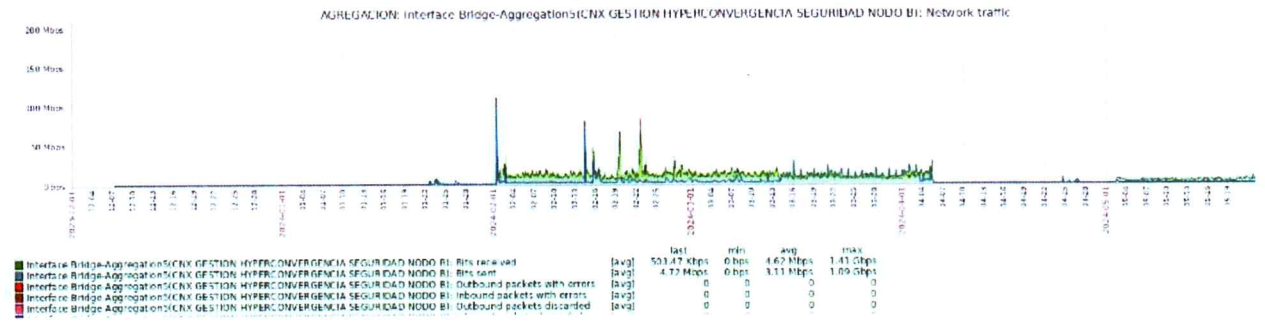


Imagen. Utilización de red SWITCH de agregación(GESTION DE HYPERCONVERGENCIA NODO B)

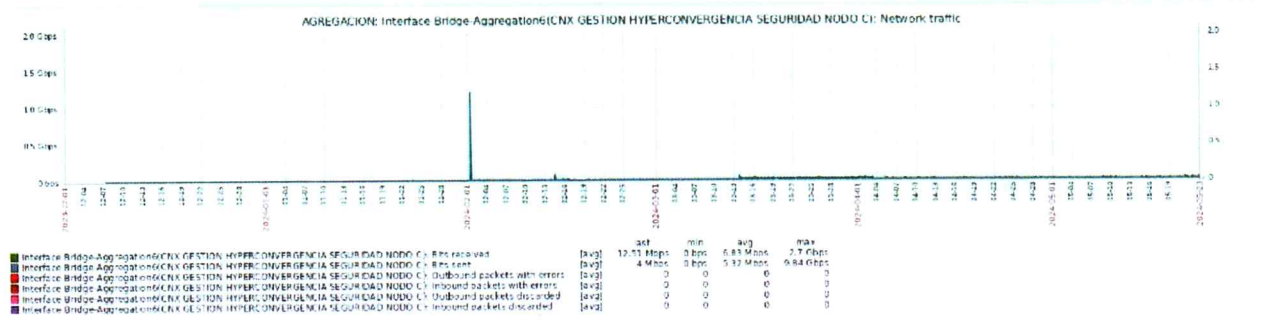


Imagen. Utilización de red SWITCH de agregación(GESTION DE HYPERCONVERGENCIA NODO C)

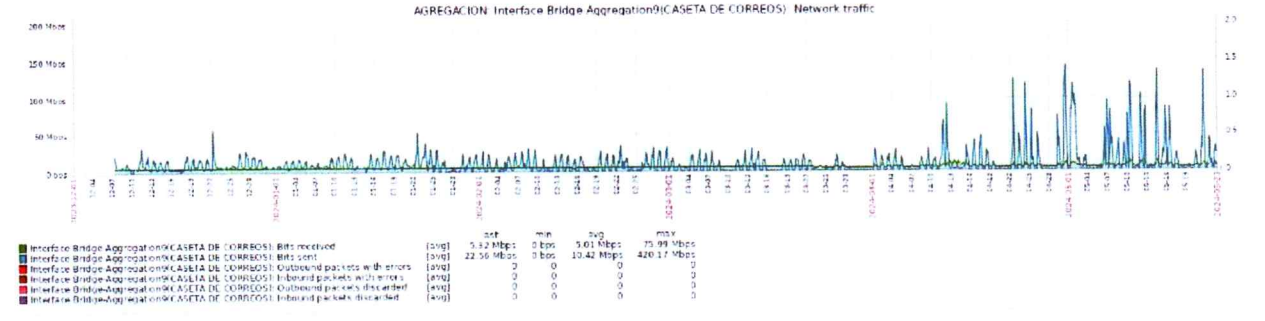


Imagen. Utilización de red SWITCH de agregación(caseta de correos)

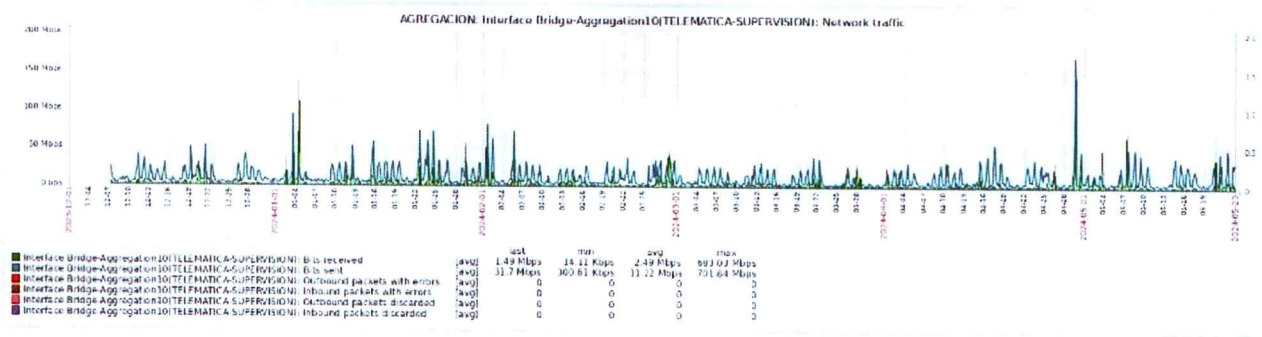


Imagen. Utilización de red SWITCH de agregación(telemática-supervisión)

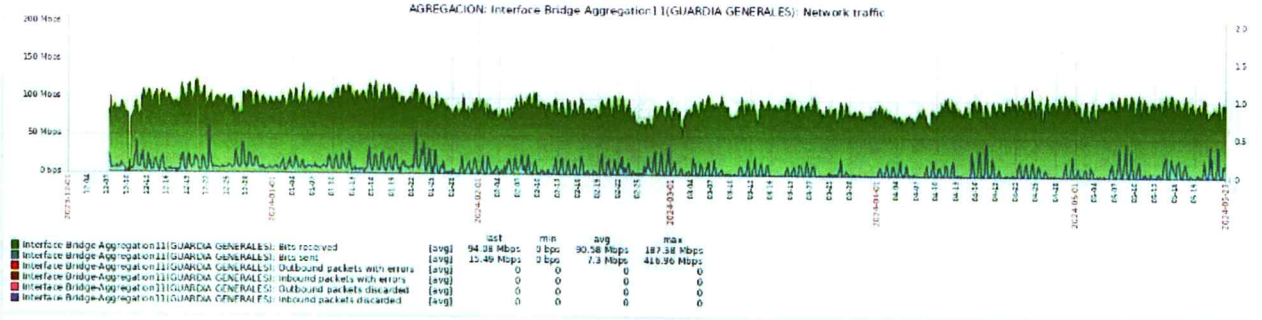


Imagen. Utilización de red SWITCH de agregación(Guardia generales)

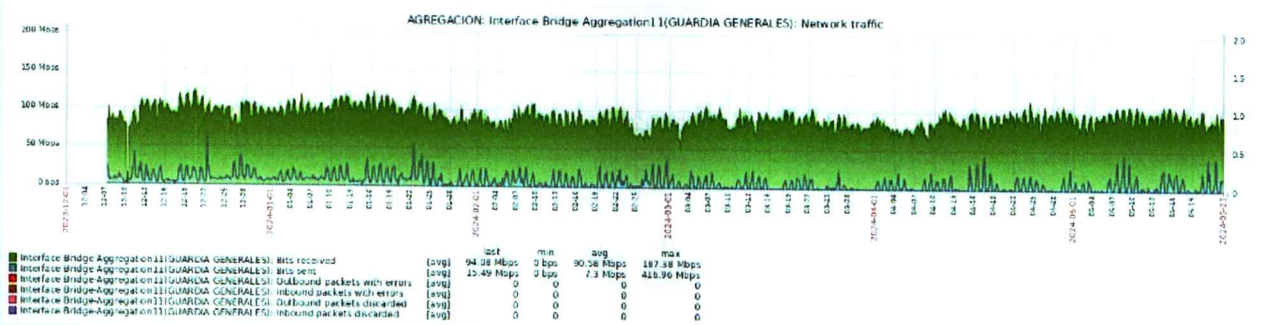


Imagen. Utilización de red SWITCH de agregación(Guardia generales)

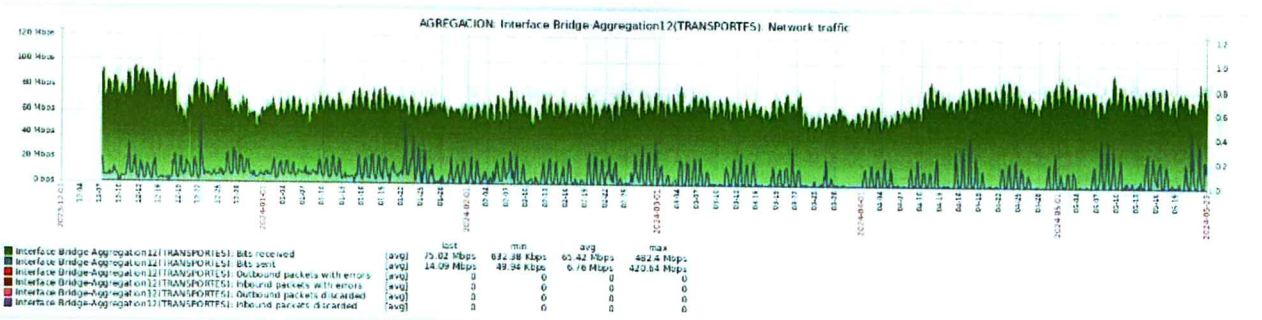


Imagen. Utilización de red SWITCH de agregación(transportes)

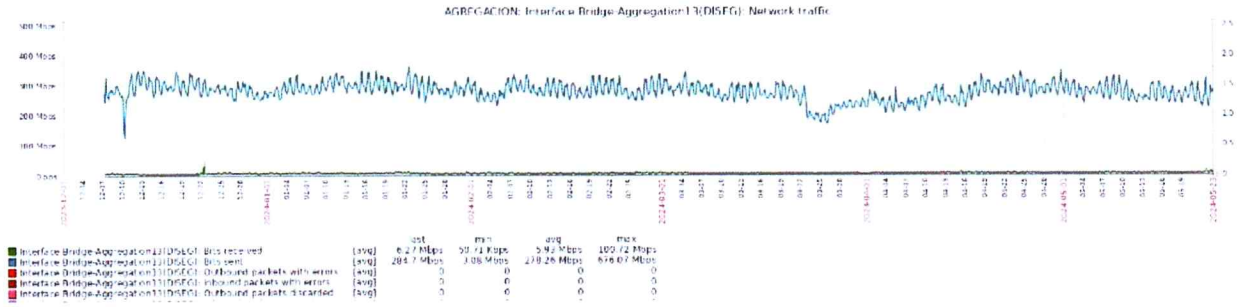


Imagen. Utilización de red SWITCH de agregación(DISEG)

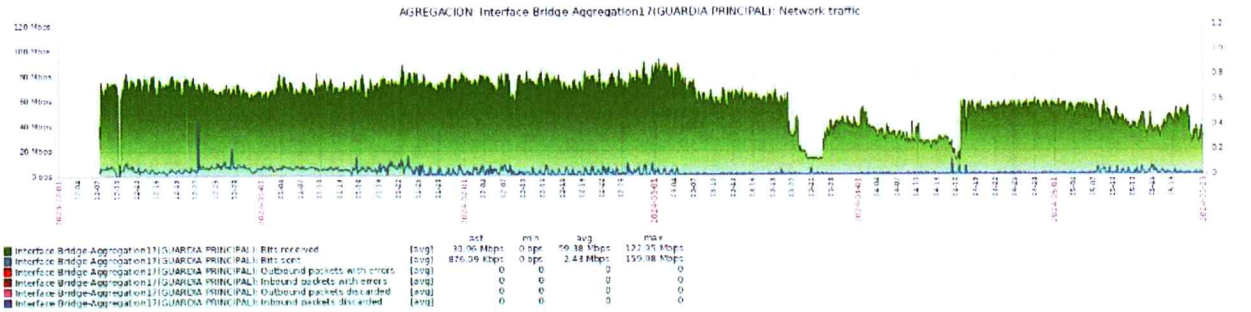


Imagen. Utilización de red SWITCH de agregación(GUARDIA PRINCIPAL)

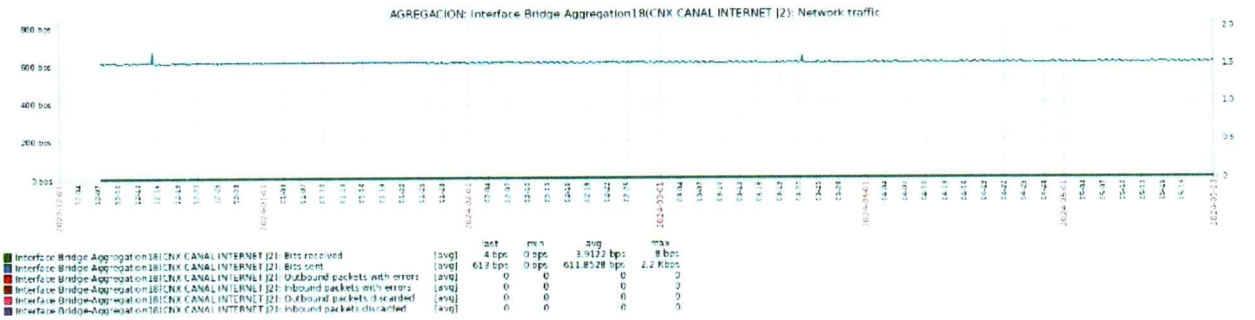


Imagen. Utilización de red SWITCH de agregación(CNX CANAL DE INTERNET 2)

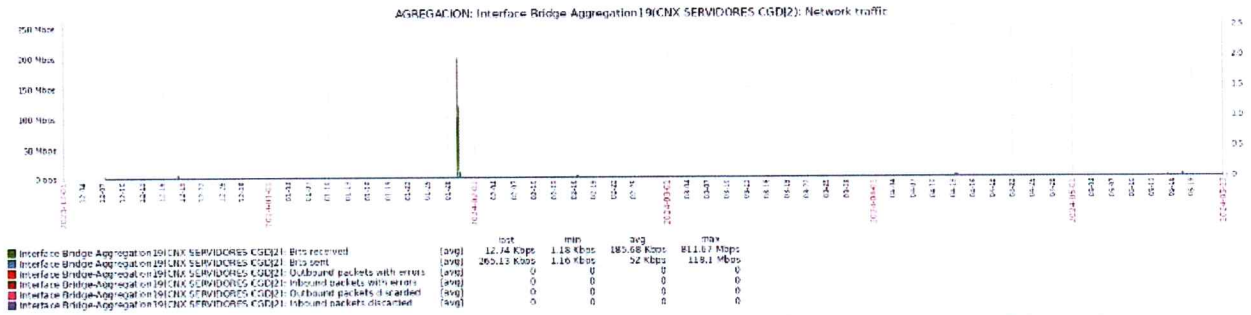


Imagen. Utilización de red SWITCH de agregación(CNX SWITCHES CGD2)

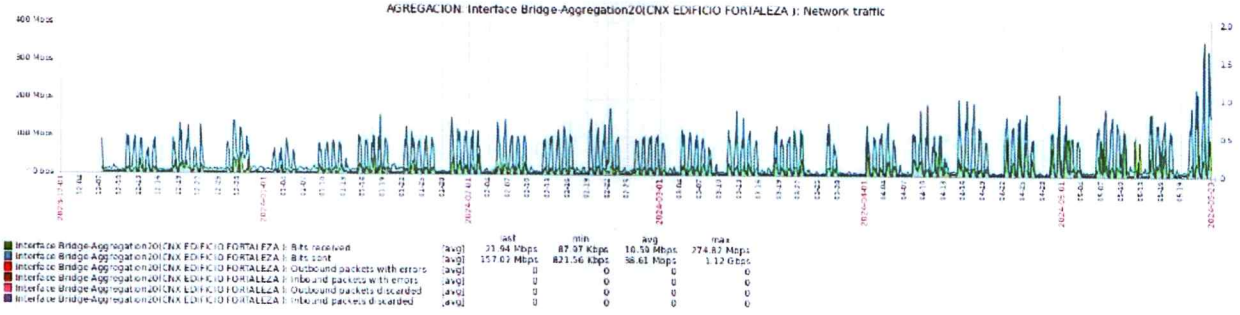


Imagen. Utilización de red SWITCH de agregación(CNX EDIFICO FORTALEZA)

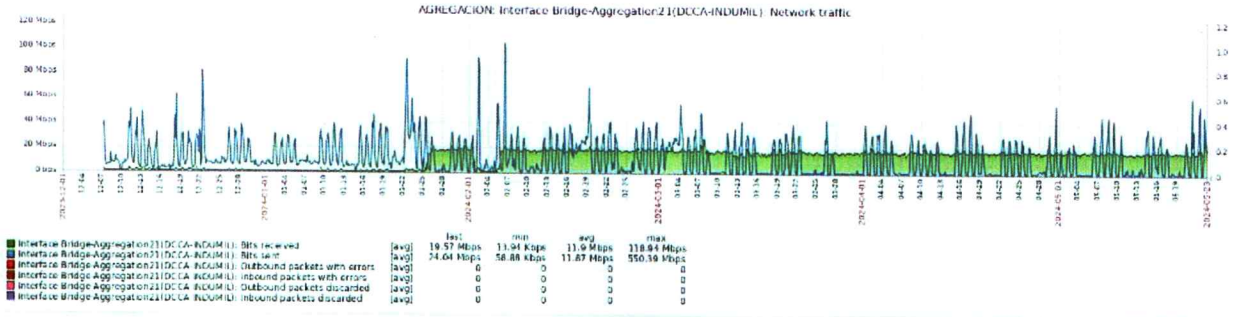


Imagen. Utilización de red SWITCH de agregación(DCCA-INDUMIL)

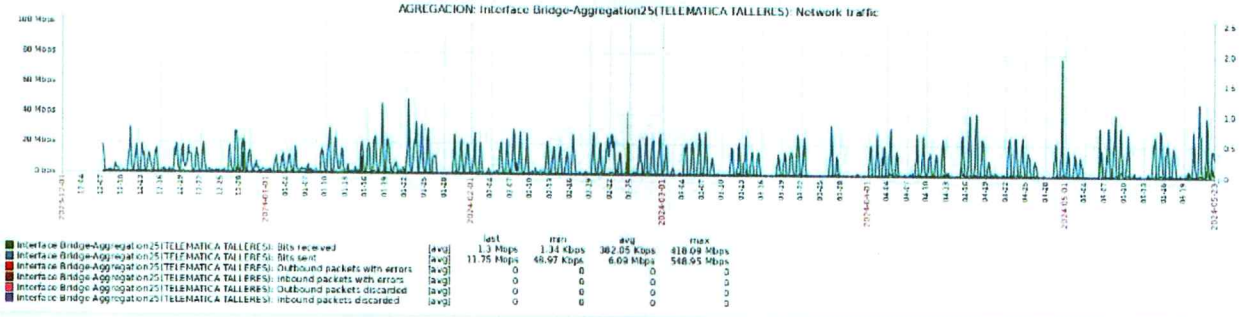


Imagen. Utilización de red SWITCH de agregación(TELEMATICA-TALLERES)

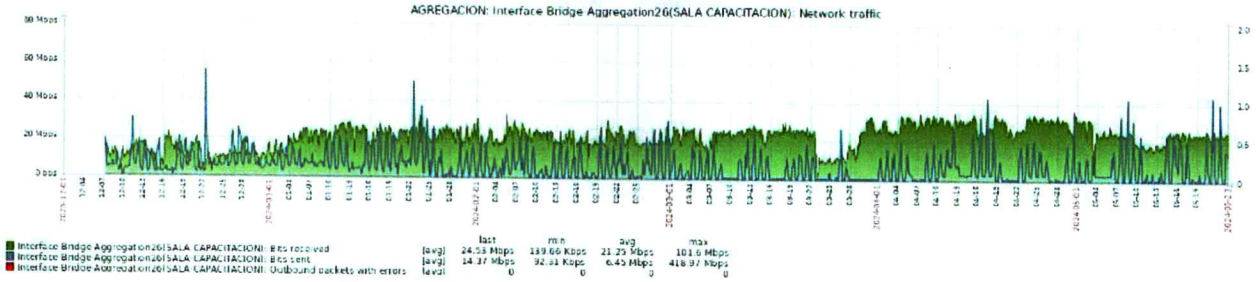


Imagen. Utilización de red SWITCH de agregación(SALA DE CAPACITACION)

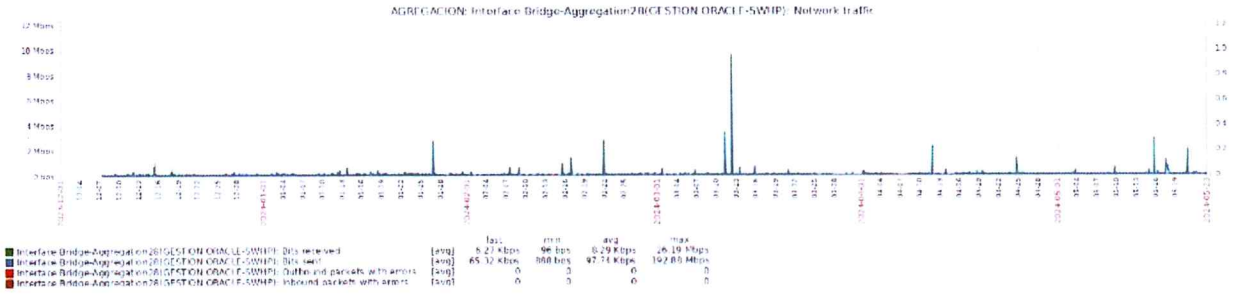


Imagen. Utilización de red SWITCH de agregación(GESTION ORACLE-SWHP)

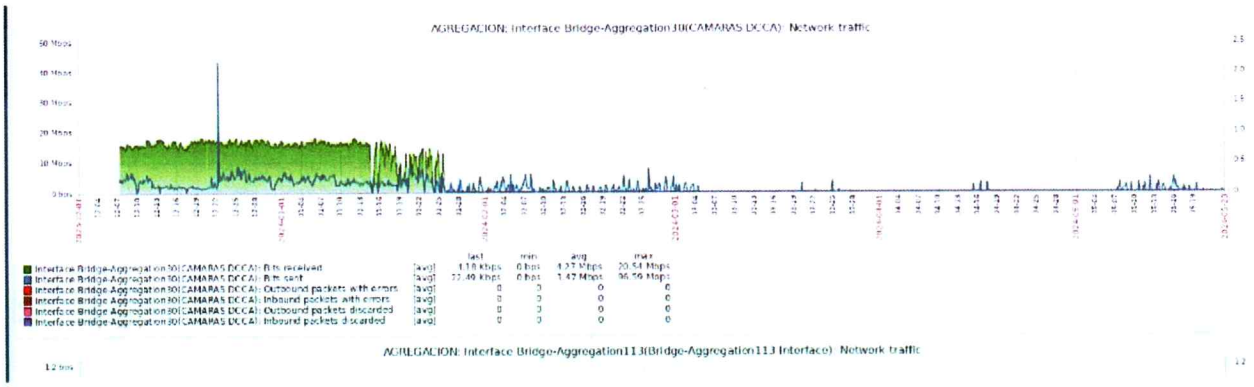


Imagen. Utilización de red SWITCH de agregación(CAMARAS DDCA)

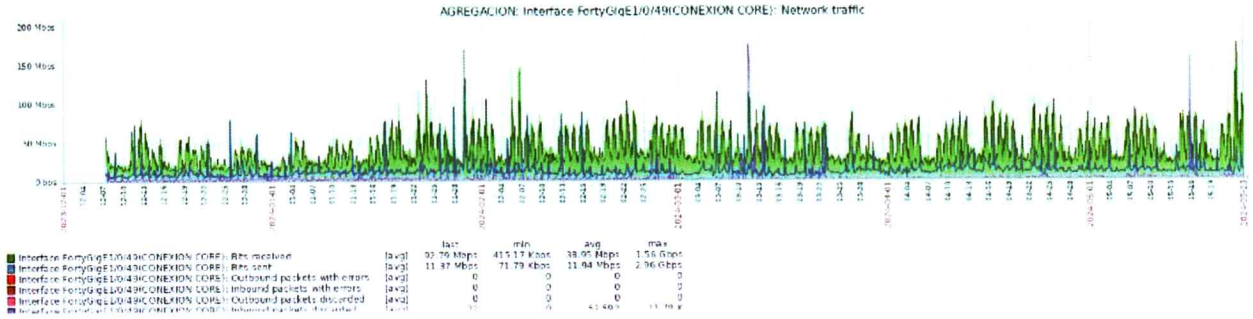


Imagen. Utilización de red SWITCH de agregación(CONEXION CORE FORTYGIGe1/0/49)

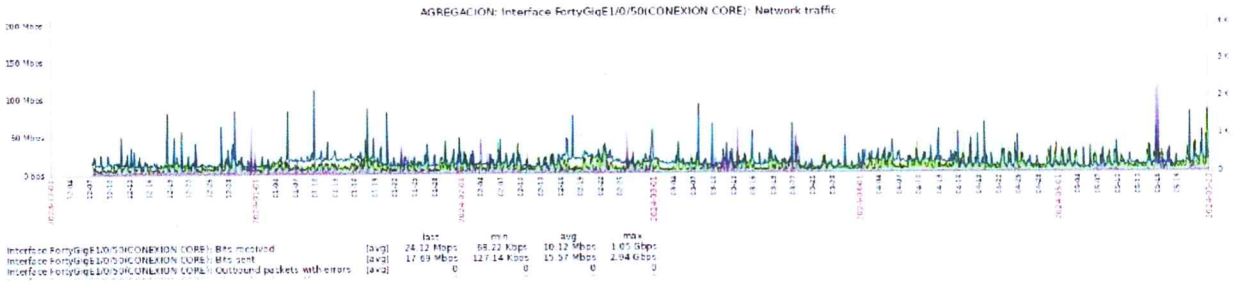


Imagen. Utilización de red SWITCH de agregación(CONEXION CORE FORTYGIGe1/0/50)

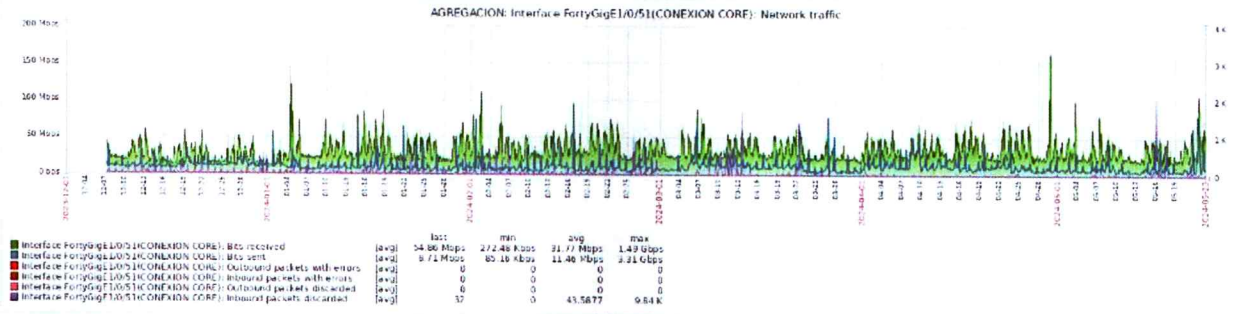


Imagen. Utilización de red SWITCH de agregación(CONEXION CORE FORTYGIGe1/0/51)

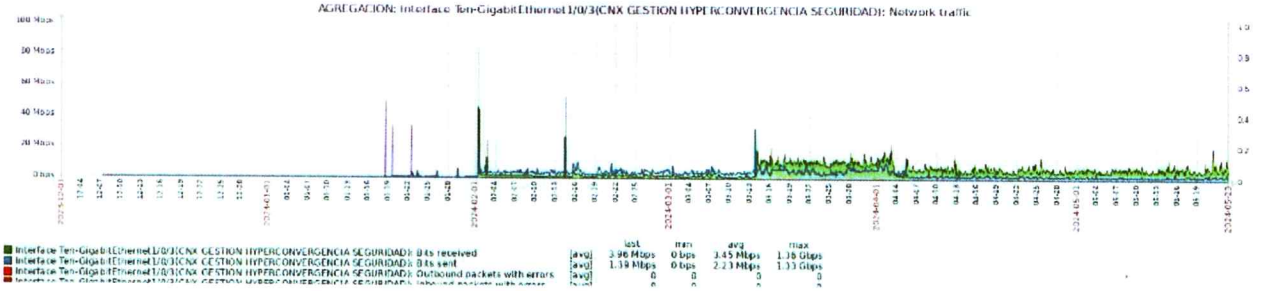


Imagen. Utilización de red SWITCH de agregación(TEN-1/0/3 CNX GESTION HYPERCONVERGENCIA SEGURIDAD)

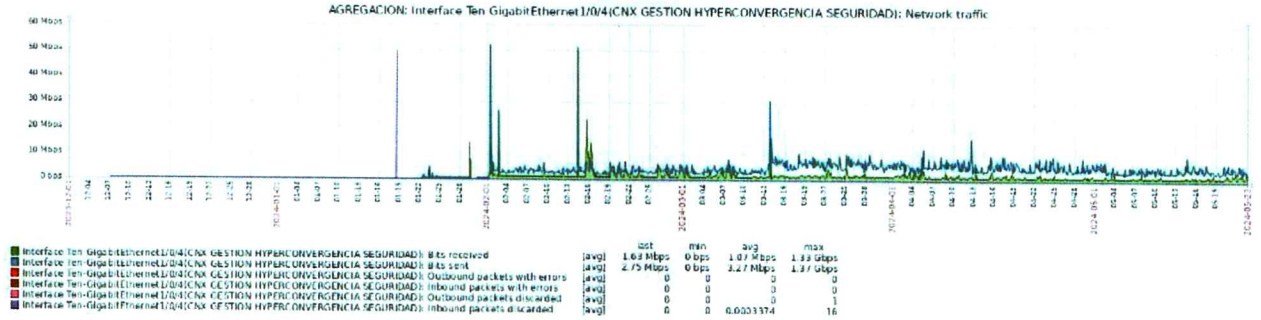


Imagen. Utilización de red SWITCH de agregación(TEN-1/0/4 CNX GESTION HYPERCONVERGENCIA SEGURIDAD)

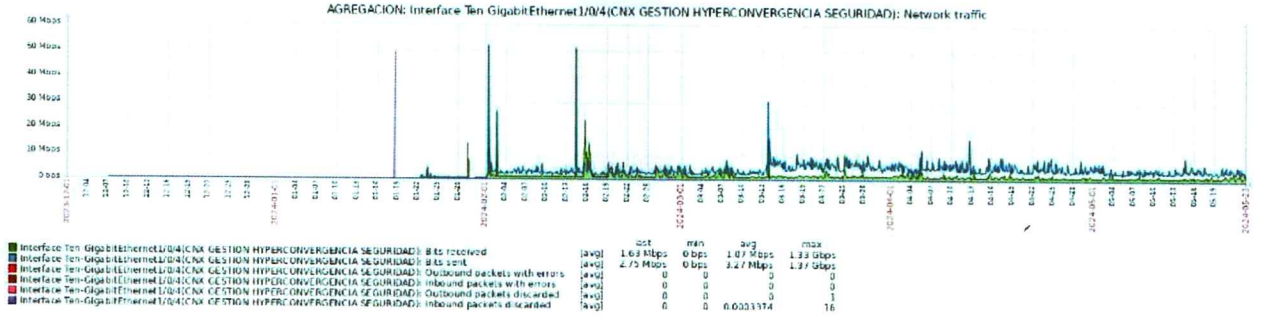


Imagen. Utilización de red SWITCH de agregación(TEN-1/0/5 CNX GESTION HYPERCONVERGENCIA SEGURIDAD)

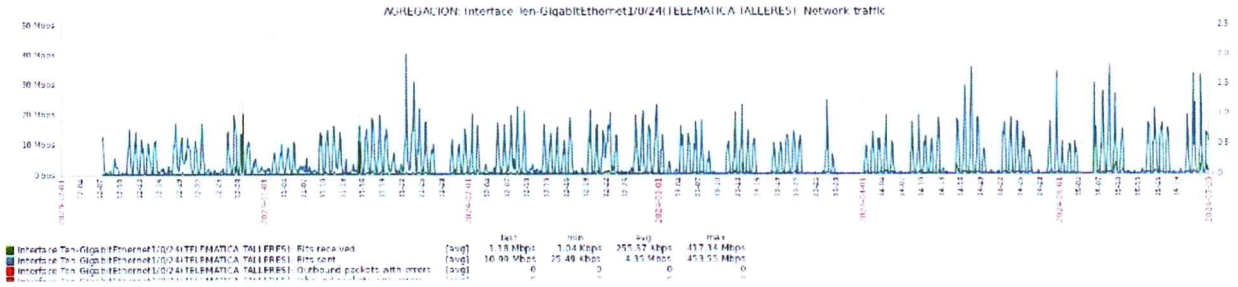


Imagen. Utilización de red SWITCH de agregación(TELEMATICAS TALLERES)

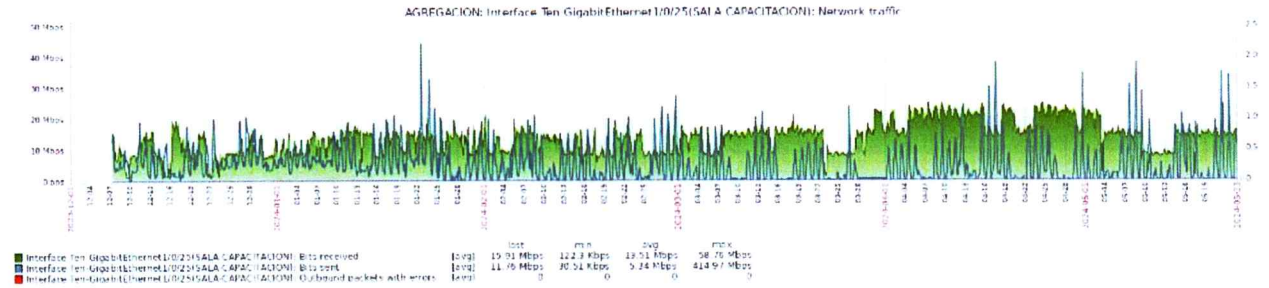


Imagen. Utilización de red SWITCH de agregación(SAL-CAPACITACION)

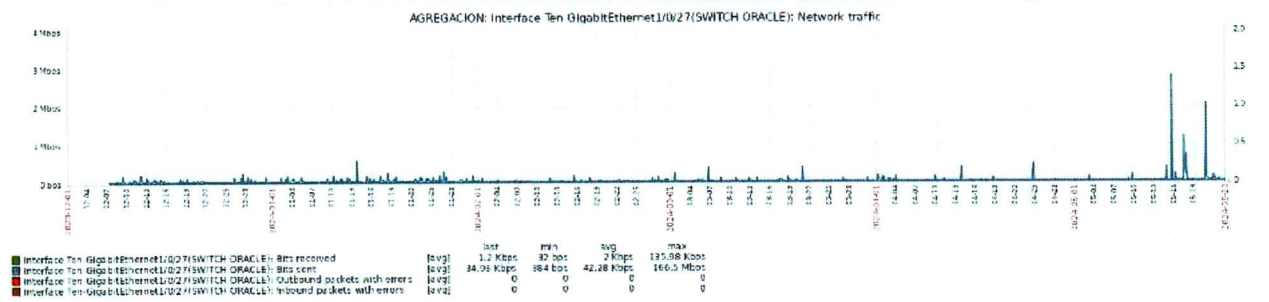


Imagen. Utilización de red SWITCH de agregación(switch oracle)

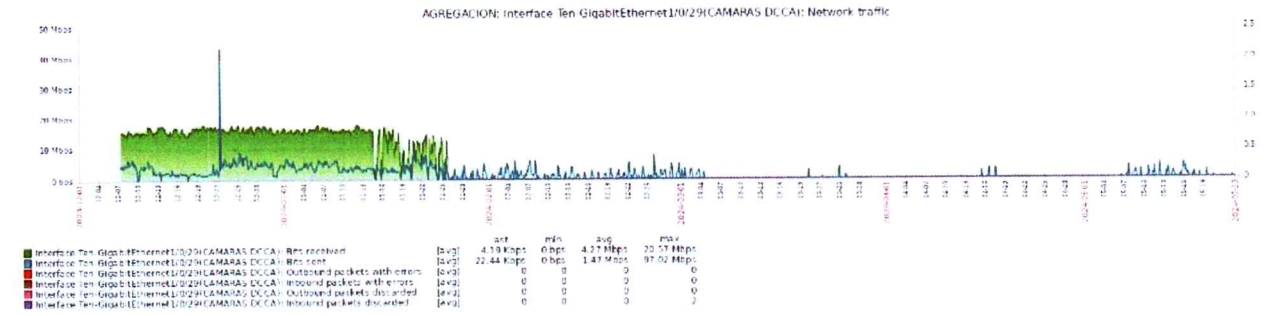


Imagen. Utilización de red SWITCH de agregación(CAMARAS DCCA)

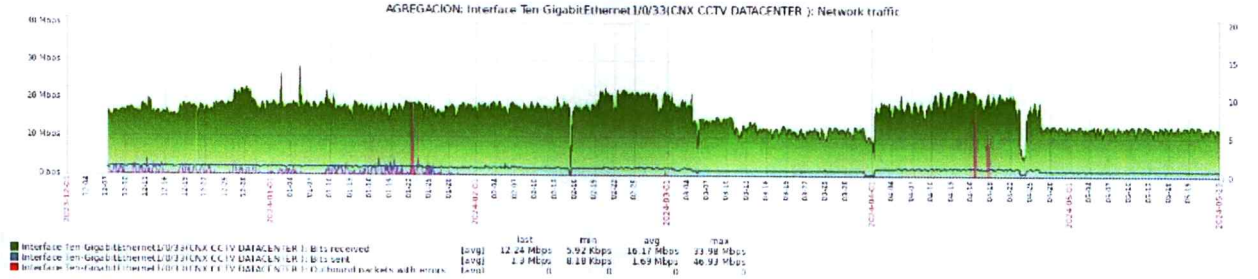


Imagen. Utilización de red SWITCH de agregación(CNX CCTV DATACENTER)

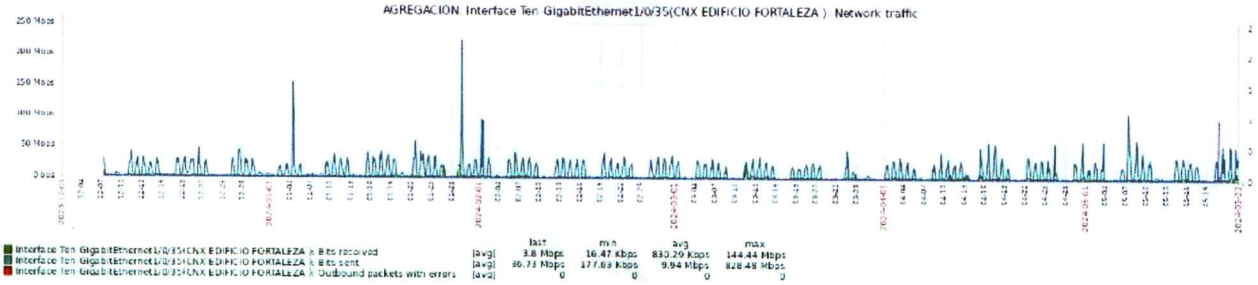


Imagen. Utilización de red SWITCH de agregación(CNX EDIFICO FORTALEZA)

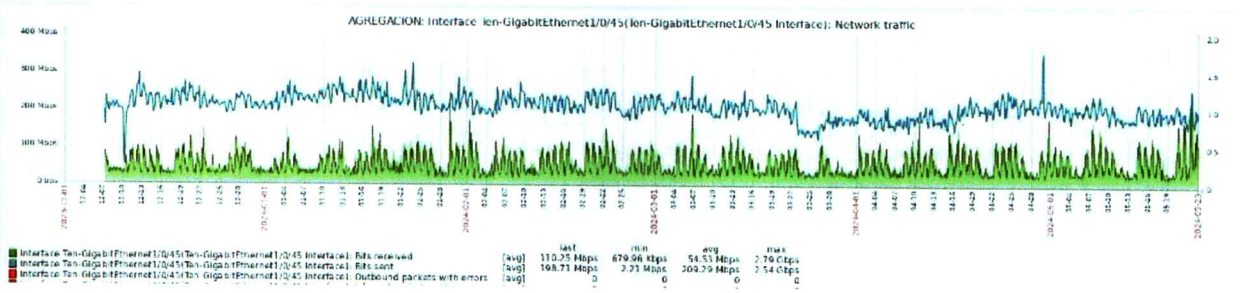


Imagen. Utilización de red SWITCH de agregación(TEN-1/0/45)

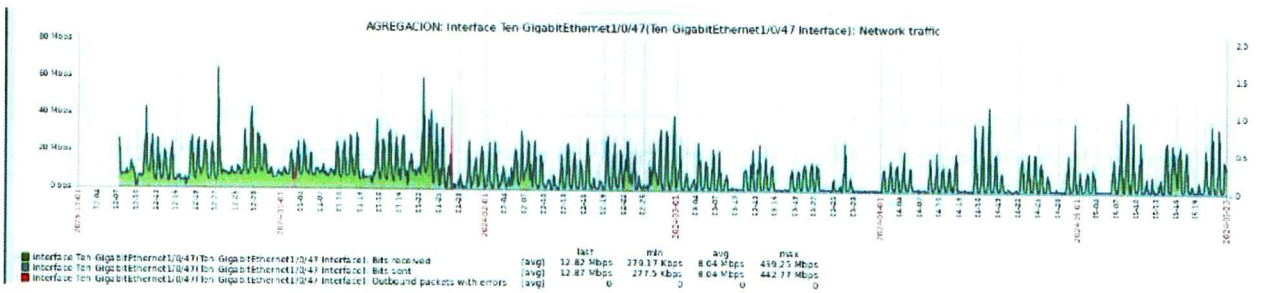


Imagen. Utilización de red SWITCH de agregación(TEN-1/0/47)

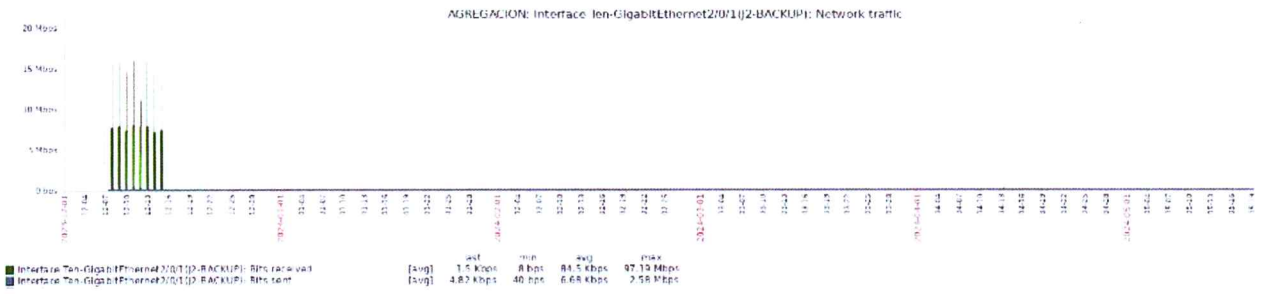


Imagen. Utilización de red SWITCH de agregación(j2-BACKUP)

9.CONCLUSIONES

El siguiente cuadro tiene como propósito tener realizar un análisis general de la cantidad de eventos y casos de uso que abrió la **CGFM.**

Se evidencia un aumento considerable en la cantidad de alertas reportadas por correo electrónico, se debe continuar reduciendo la cantidad de eventos con el fin de que únicamente lleguen correos de eventos críticos y no de falsos positivos.

Se ejecutaron los parches y actualizaciones correspondientes a la infraestructura tecnológica de **CGFM,** se evidencia un aumento de incidentes respecto al mes julio.

Se tiene un Backup de cada componente: bases de datos; proxy e interfaz gráfica sobre la plataforma d monitoreo.

Se encuentra siendo monitoreado el servidor Windows de manera satisfactoria, ya se tiene visibilidad y cumple con las expectativas que fueron colocadas en el inicialmente.

Se debe implementar el transporte de paquetes por SNMP para asegurar el correcto monitoreo.

IDENTIAN®	ACTA DE REUNIÓN	Código: FR-SI-SGSI-10 Fecha emisión: 10/07/2017 Versión: 01

FECHA: DD 27 MM 06 AAAA 2024

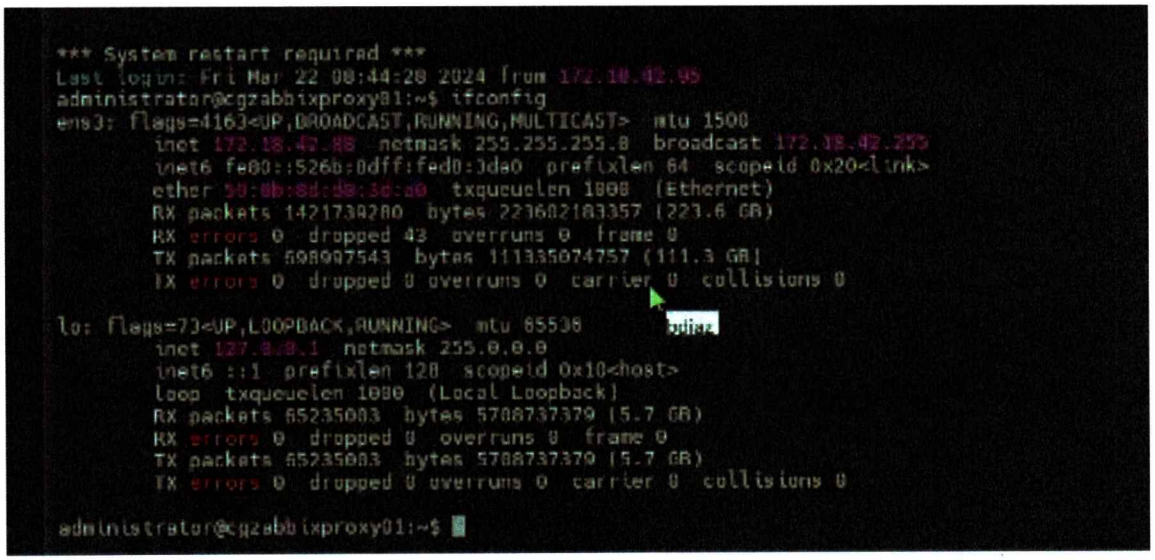
Motivo de reunión: Mantenimiento Zabbix – Tunning bases de datos MySQL	Hora de Inicio:	2:00pm
	Hora de Finalización:	5:00pm
Asistentes Byron Burgos Andrés Cardozo Brian Diaz	Cargos Cabo Director de Operaciones Consultor Técnico	

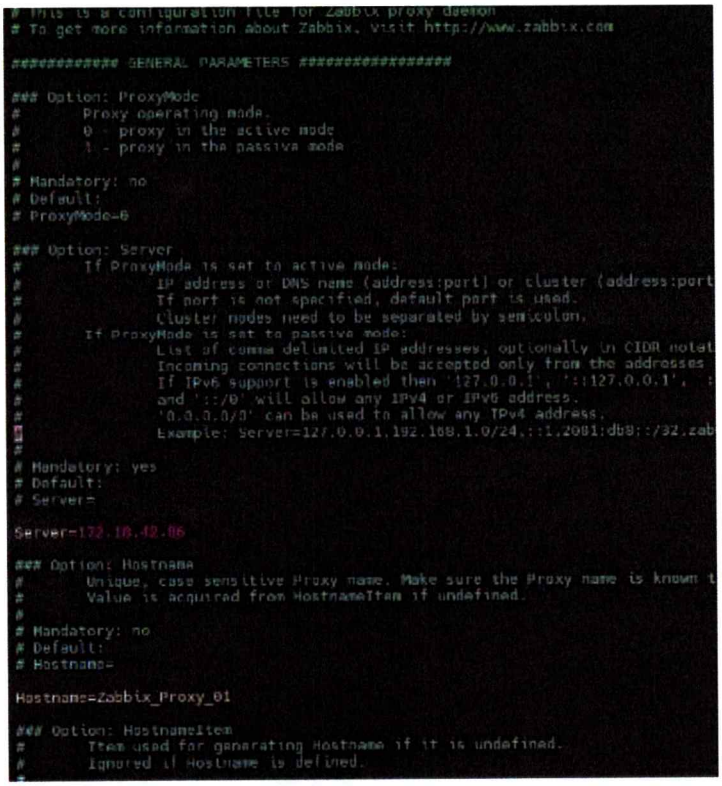
Se realiza el mantenimiento correspondiente al Backup de los archivos de configuración de zabbix y el Tunning de las bases de datos de MySQL.

172.18.42.86 zabbix-server

172.18.42.88 proxy

- 172.18.42.87 MySQL





Se valida la configuración del servidor de Proxy.

```
### Option: DBUser
#       Database user. Ignored for SQLite.
#
# Default:
# DBUser=

DBUser=zabbix

### Option: DBPassword
#       Database password. Ignored for SQLite.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
# DBPassword=

### Option: DBSocket
#       Path to MySQL socket.
#
# Mandatory: no
# Default:
# DBSocket=

# Option: DBPort
#       Database port when not using local socket. Ignored for SQLite.
#       If the Net Service Name connection method is used to connect to Oracle database, the port number from the
#       tnsnames.ora file will be used. The port number set here will be ignored.
#
# Mandatory: no
# Default:
# DBPort=
```

Se valida los usuarios correspondientes al servidor de Proxy. La configuración del proxy apunta sobre el Hostname ZBX_PROXY_01

```
#
# Mandatory: no
# Default:
# TLSKeyFile=

### Option: TLSPSKIdentity
#       Unique, case sensitive string used to identify the pre-shared key.
#
# Mandatory: no
# Default:
# TLSPSKIdentity=

TLSPSKIdentity=ZBX_PROXY_01

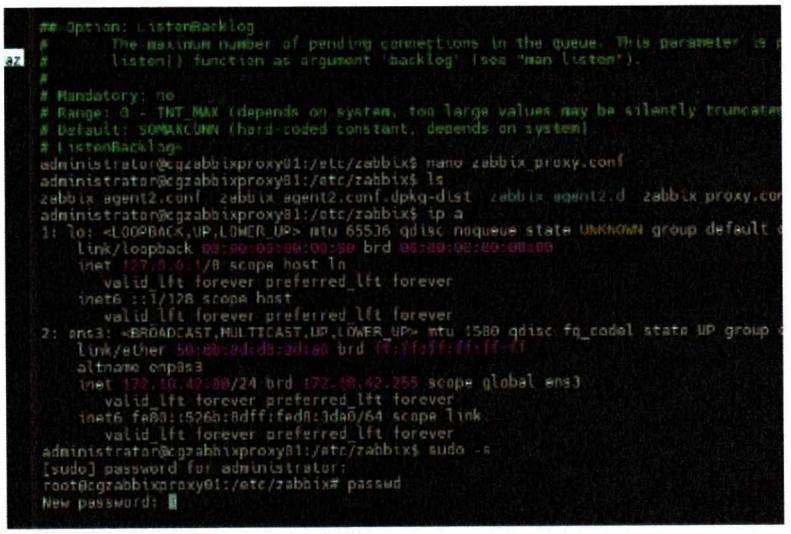
### Option: TLSPSKFile
#       Full pathname of a file containing the pre-shared key.
#
# Mandatory: no
# Default:
# TLSPSKFile=

TLSPSKFile=/var/lib/zabbix/.psk/zabbix_proxy.psk

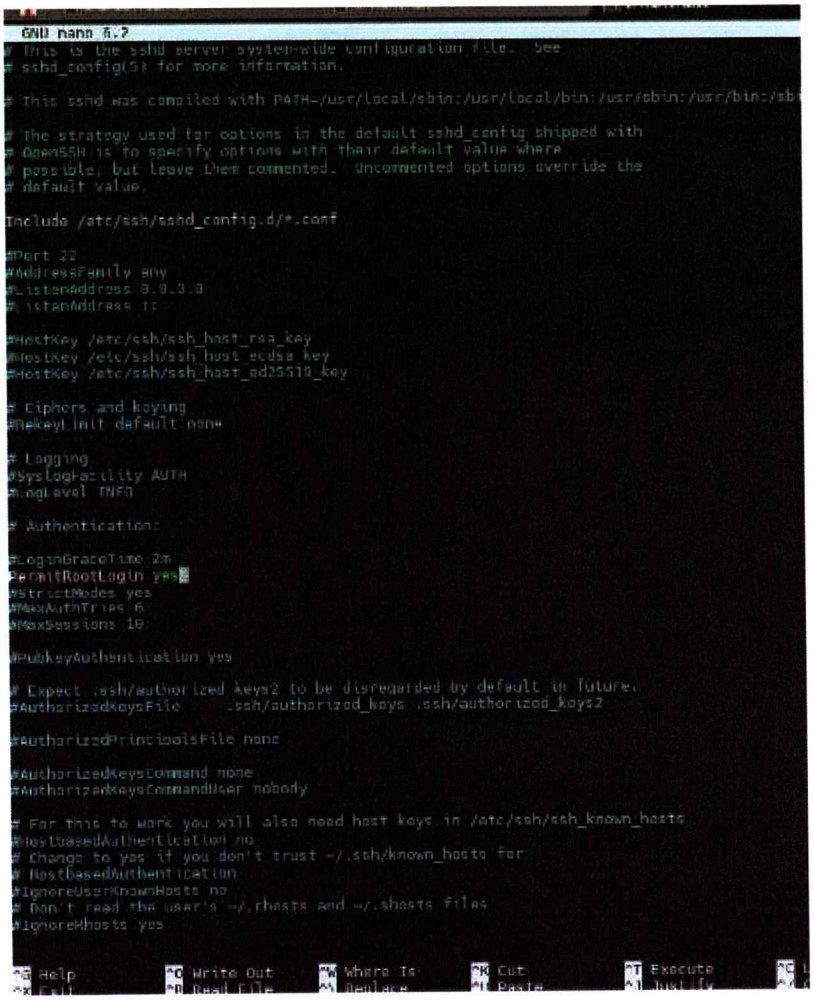
######## For advanced users - TLS ciphersuite selection criteria ########

### Option: TLSCipherCert13
#       Cipher string for OpenSSL 1.1.1 or newer in TLS 1.3.
#       Override the default ciphersuite selection criteria for certificate-based encryption.
#
# Mandatory: no
```

A continuación, realizamos la configuración del usuario root para el ingreso de archivos por sftp.



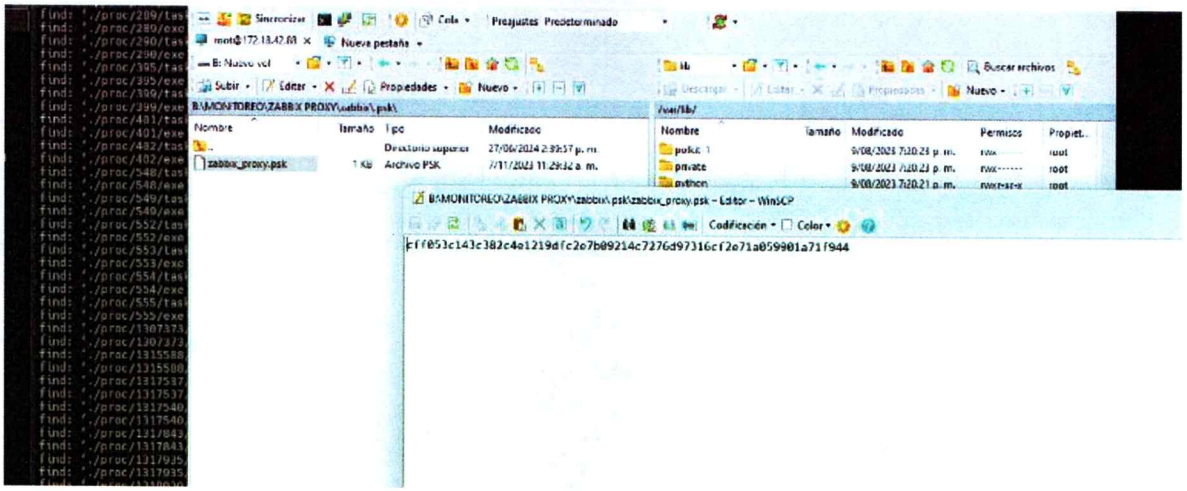
Para ello realizamos el cambio de configuración del protocolo ssh.



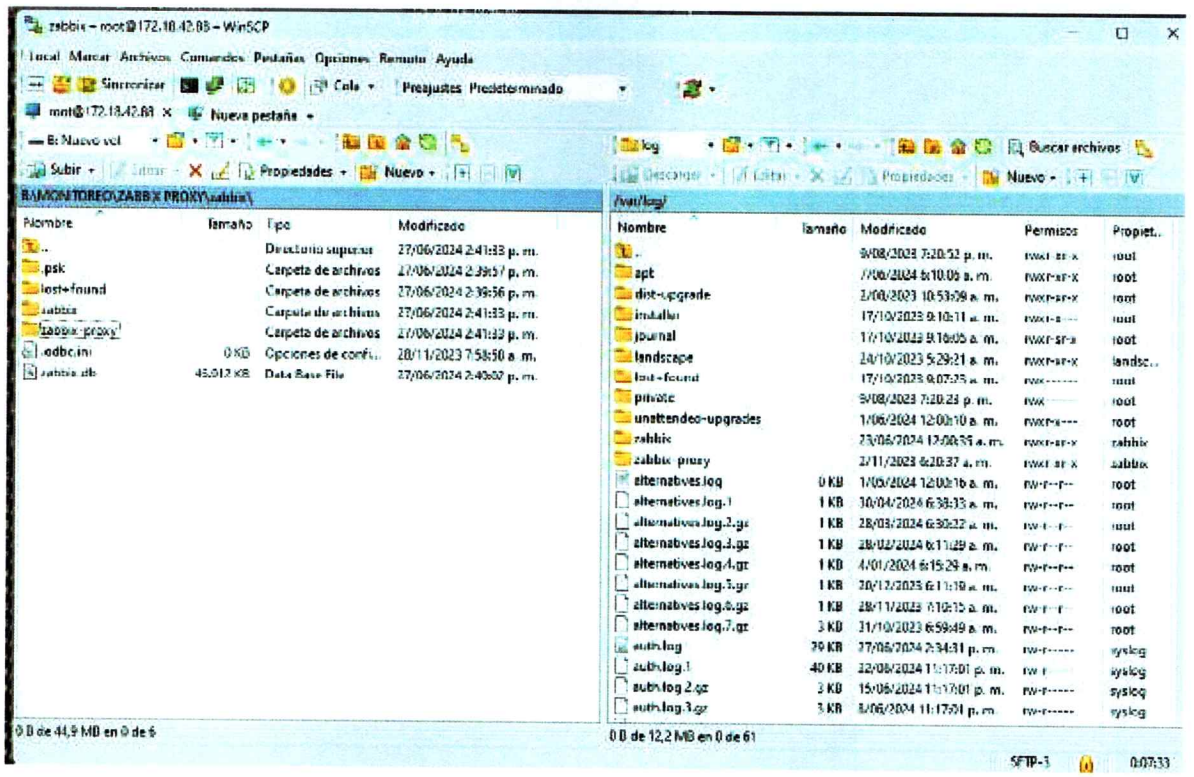
Se procede a realiza copia de seguridad sobre estas carpetas

```
find: unknown predicate `-nmae'
root@cgzabbixproxy01:/# find  nmae zabbix
./run/zabbix
./usr/lib/zabbix
./var/lib/zabbix
./var/log/zabbix
./etc/zabbix
root@cgzabbixproxy01:/#
```

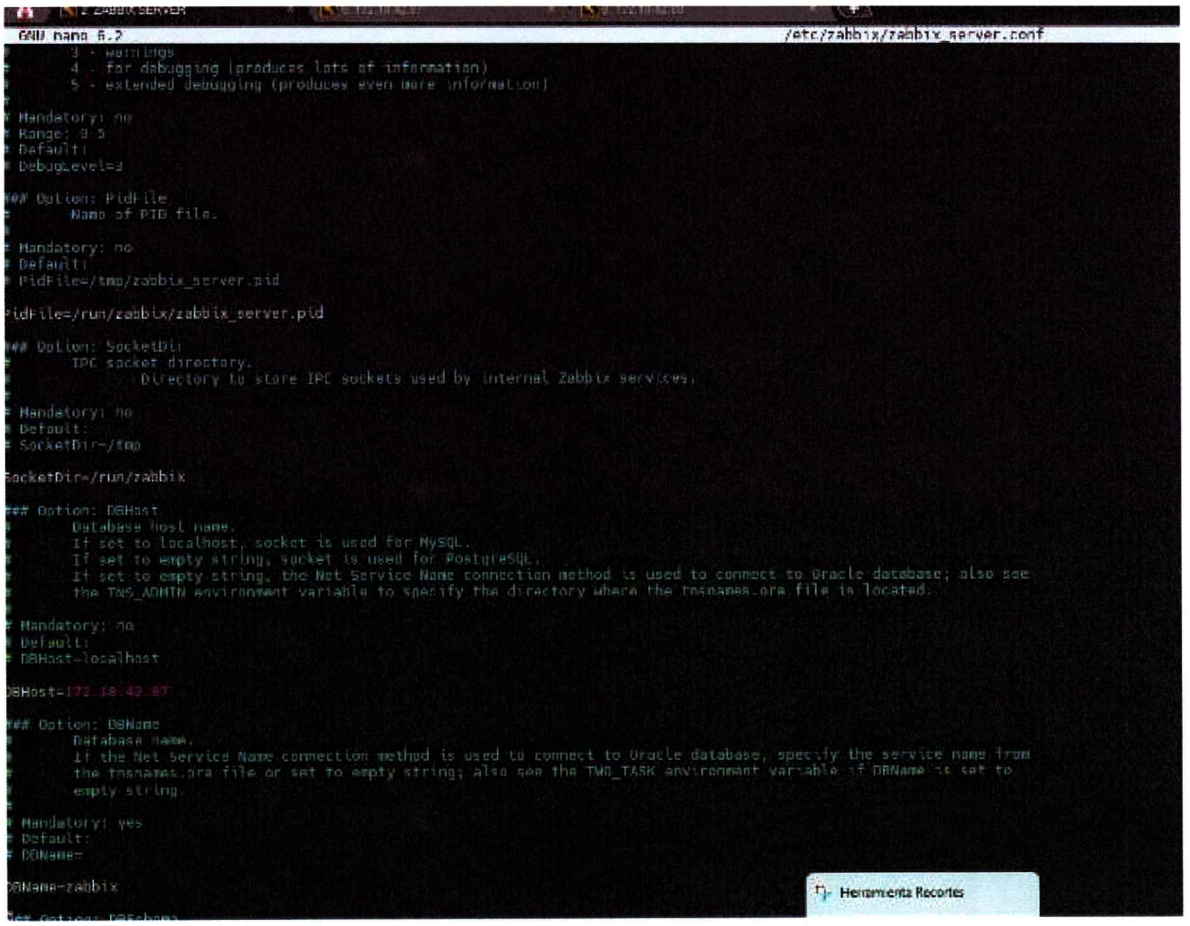
Se encuentra .psk zabbix para la autenticación de agentes.



Se realiza el Backup de odc.ini y de los logs de configuración del proxy

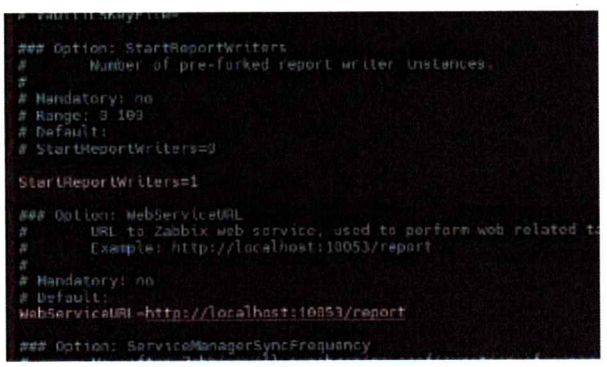


Ahora ingresamos al servidor de zabbix para verificar la configuración del servidor.



DBHOST=172.18.42.87
DBNAME=ZABBIX
DBUSER=zabbix-server
Dbpassword=CComando2023¡

Se ha configurado la conexión de los reportes automáticos de Zabbix. estos archivos de configuración se realizan sobre el archivo de configuración del zabbix-server para la impresión de reporte PDF.



```
# DBSchema=

### Option: DBUser
#       Database user.
#
# Mandatory: no
# Default:
# DBUser=

DBUser=zabbix_server

### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
# DBPassword=

DBPassword=CComando2023!

### Option: DBSocket
#       Path to MySQL socket.
#
# Mandatory: no
# Default:
# DBSocket=

### Option: DBPort
#       Database port when not using local socket.
#       If the Net Service Name connection method is used to connect to Oracle database, the port number from the
#       tnsnames.ora file will be used. The port number set here will be ignored.
#
# Mandatory: no
```

Este es el archivo de configuración de zabbix_web_Server.conf

```
GNU nano 6.2                                                    zabbix
## Option: DebugLevel
        Specifies debug level:
        0 - basic information about starting and stopping of Zabbix processes
        1 - critical information
        2 - error information
        3 - warnings
        4 - for debugging (produces lots of information)
        5 - extended debugging (produces even more information)

 Mandatory: no
 Range: 0-5
 Default:
 DebugLevel=3

## Option: AllowedIP
        List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix se
        Incoming connections will be accepted only from the hosts listed here.
        If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated e
        and '::/0' will allow any IPv4 or IPv6 address.
        '0.0.0.0/0' can be used to allow any IPv4 address.
        Example: AllowedIP=127.0.0.1,192.168.1.0/24,::1,2001:db0::/32,zabbix.example.com

 Mandatory: yes
 Default:
 AllowedIP=

llowedIP=127.0.0.1,::1

## Option: ListenPort
        Service will listen on this port for connections from the server.

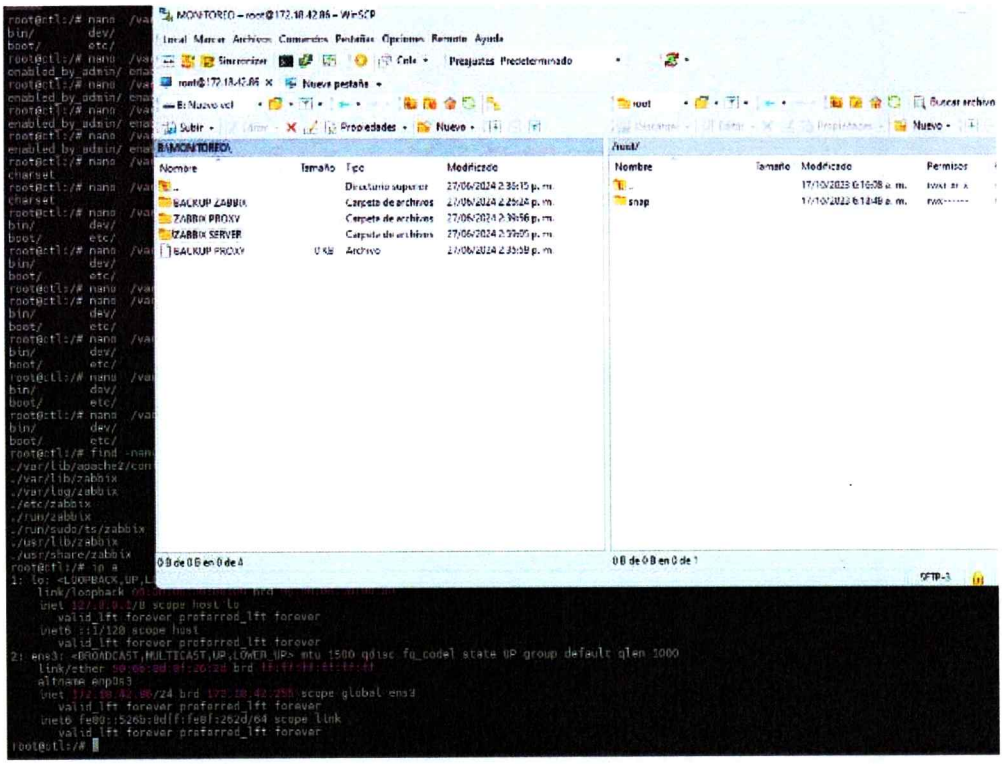
 Mandatory: no
 Range: 1024-32767
 Default:
istenPort=10051

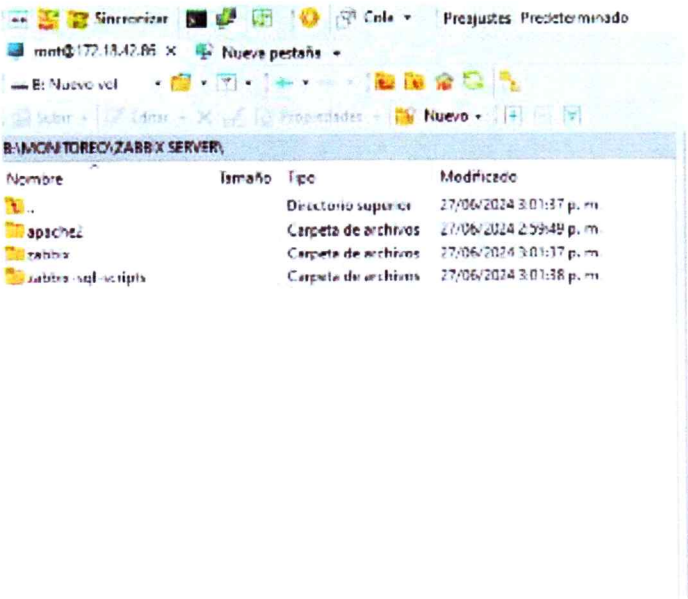
## Option: Timeout
        Spend no more than Timeout seconds on processing

 Mandatory: no
 Range: 1-30
 Default:
 Timeout=3
```

Se procede a realiza la copia de seguridad de los siguientes directorios del servidor de zabbix.

```
root@ctl:/# find -name  zabbix
/var/lib/apache2/conf/enabled_by_admin/zabbix
/var/lib/zabbix
/var/log/zabbix
/etc/zabbix
/run/zabbix
/run/sudo/ts/zabbix
/usr/lib/zabbix
/usr/share/zabbix
root@ctl:/#
```

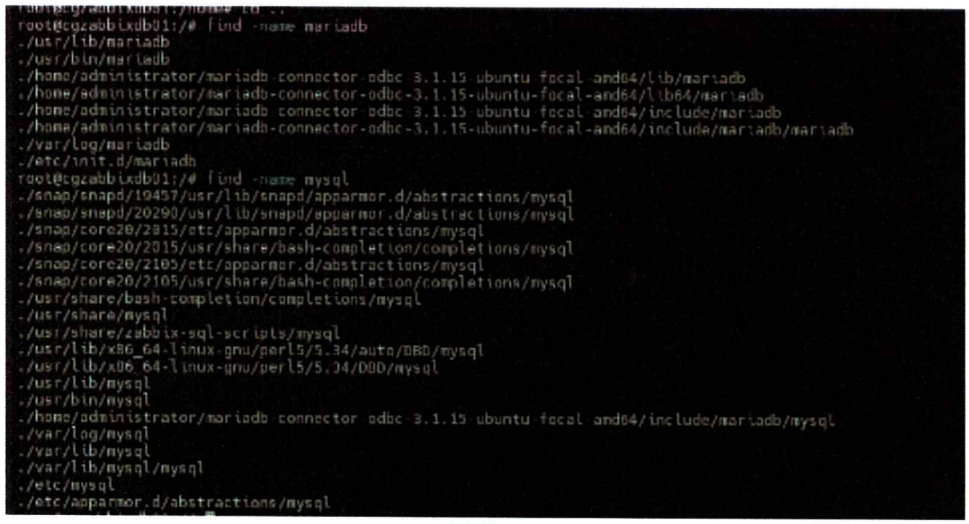


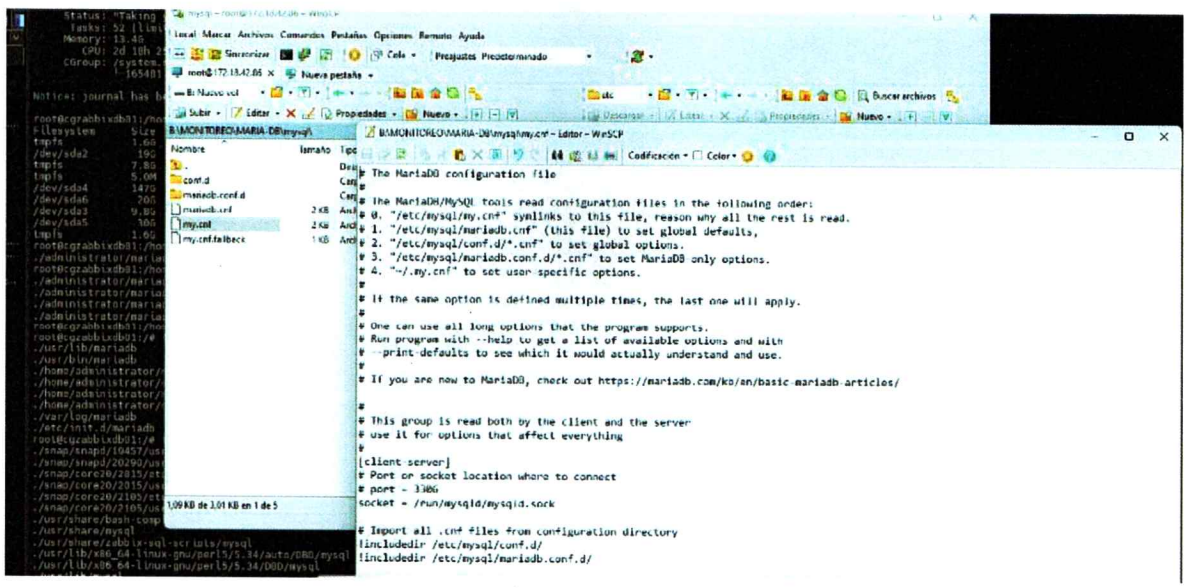


Procedemos a validar la versión de MySQL instalada en el servidor mariadb.service - MariaDB 10.6.16 database server



Ahora realizamos la configuración de los archivos de MySQL. Para ello realizamos la búsqueda de los archivos correspondientes.





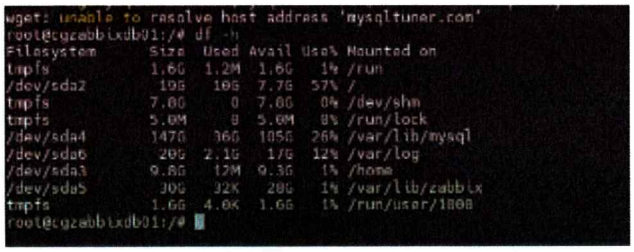
Estos archivos son la configuración de las bases de datos de MySQL.

Ingresamos en la carpeta temporal:
cd /tmp

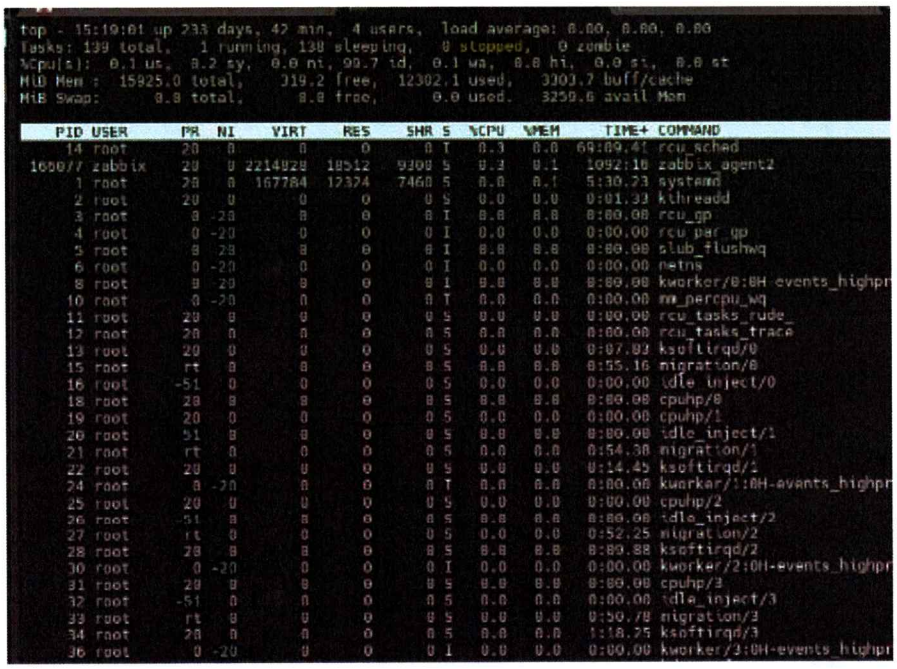
Descargamos el script:
wget http://mysqltuner.com/mysqltuner.pl

Tenemos que hacer el script ejecutable:
chmod +x mysqltuner.pl

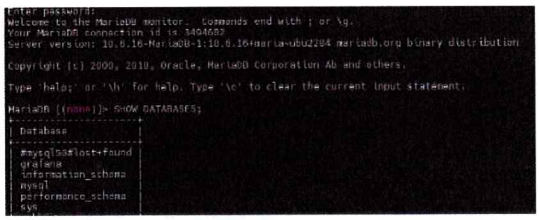
Lo iniciamos:
./mysqltuner.pl



Se valida espacio suficiente para el almacenamiento de registros de zabbix.



Se valida en el servidor 16 en ram, la memoria y la cpu no está afectadas.



Se encuentra las bases de datos de grafana,mysql,infromation_schema,perfomanance_shcema,SYS Y ZABBIX
Se hace el ajuste de la memoria cache

```
MariaDB [(none)]> SHOW VARIABLES LIKE 'have_query_cache';
+------------------+-------+
| Variable_name    | Value |
+------------------+-------+
| have_query_cache | YES   |
+------------------+-------+
1 row in set (0.000 sec)
```

```
MariaDB [(none)]> SHOW VARIABLES LIKE 'query_cache_type';
+------------------+-------+
| Variable_name    | Value |
+------------------+-------+
| query_cache_type | OFF   |
+------------------+-------+
1 row in set (0.000 sec)

MariaDB [(none)]>
```

SHOW VARIABLES LIKE 'query_cache_size';

```
MariaDB [(none)]> SHOW VARIABLES LIKE 'query_cache_size';
+------------------+-------+
| Variable_name    | Value |
+------------------+-------+
| query_cache_size | 0     |
+------------------+-------+
1 row in set (0.000 sec)
```

En primer lugar, la variable query_cache_size debe ser lo suficientemente grande como para contener el resultado de sus consultas. Si es demasiado pequeña, no se almacenará nada en la caché.

```
MariaDB [(none)]> show variables like 'wait%';
+---------------+-------+
| Variable_name | Value |
+---------------+-------+
| wait_timeout  | 300   |
+---------------+-------+
1 row in set (0.000 sec)
```

```
MariaDB [(none)]> show variables like 'thread_pool_size';
+-----------------+-------+
| Variable_name   | Value |
+-----------------+-------+
| thread_pool_size | 4    |
+-----------------+-------+
1 row in set (0.000 sec)
```

MySQL viene con un pool de hilos — un número fijo de hilos que forman parte de un pool al inicio:

Adicionalmente validamos el estatus de las bases de datos para que el rendimiento de la plataforma sea optimo. Las consultas están tuneadas.

```
MariaDB [(none)]> SHOW STATUS;
+----------------------------------------------------+-----------------------+
| Variable_name                                      | Value                 |
+----------------------------------------------------+-----------------------+
| Aborted_clients                                    | 286723                |
| Aborted_connects                                   | 5                     |
| Aborted_connects_preauth                           | 1                     |
| Access_denied_errors                               | 0                     |
| Acl_column_grants                                  | 0                     |
| Acl_database_grants                                | 7                     |
| Acl_function_grants                                | 0                     |
| Acl_procedure_grants                               | 0                     |
| Acl_package_spec_grants                            | 0                     |
| Acl_package_body_grants                            | 0                     |
| Acl_proxy_users                                    | 1                     |
| Acl_role_grants                                    | 0                     |
| Acl_roles                                          | 0                     |
| Acl_table_grants                                   | 1                     |
| Acl_users                                          | 11                    |
| Aria_pagecache_blocks_not_flushed                  | 0                     |
| Aria_pagecache_blocks_unused                       | 15627                 |
| Aria_pagecache_blocks_used                         | 107                   |
| Aria_pagecache_read_requests                       | 7945775               |
| Aria_pagecache_reads                               | 65898                 |
| Aria_pagecache_write_requests                      | 260480                |
| Aria_pagecache_writes                              | 141718                |
| Aria_transaction_log_syncs                         | 112                   |
| Binlog_commits                                     | 0                     |
| Binlog_group_commits                               | 0                     |
| Binlog_group_commit_trigger_count                  | 0                     |
| Binlog_group_commit_trigger_lock_wait              | 0                     |
| Binlog_group_commit_trigger_timeout                | 0                     |
| Binlog_snapshot_file                               |                       |
| Binlog_snapshot_position                           | 0                     |
| Binlog_bytes_written                               | 0                     |
| Binlog_cache_disk_use                              | 0                     |
| Binlog_cache_use                                   | 0                     |
| Binlog_stmt_cache_disk_use                         | 0                     |
| Binlog_stmt_cache_use                              | 0                     |
```

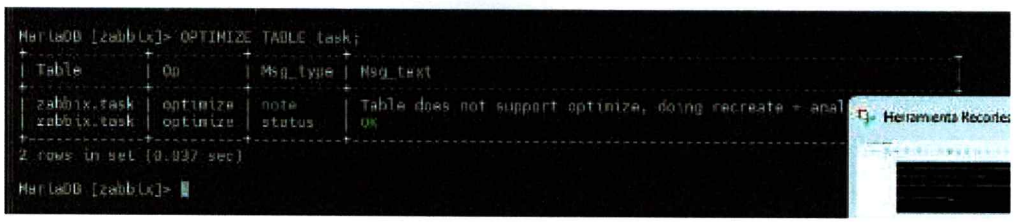
```
| Innodb_adaptive_hash_hash_searches                 | 0                                                |
| Innodb_adaptive_hash_non_hash_searches             | 0                                                |
| Innodb_background_log_sync                         | 16313592                                         |
| Innodb_buffer_pool_dump_status                     |                                                  |
| Innodb_buffer_pool_load_status                     | Buffer pool(s) load completed at 231221 11:51:54 |
| Innodb_buffer_pool_resize_status                   |                                                  |
| Innodb_buffer_pool_load_incomplete                 | OFF                                              |
| Innodb_buffer_pool_pages_data                      | 648959                                           |
| Innodb_buffer_pool_bytes_data                      | 10632544256                                      |
| Innodb_buffer_pool_pages_dirty                     | 150103                                           |
| Innodb_buffer_pool_bytes_dirty                     | 2459287552                                       |
| Innodb_buffer_pool_pages_flushed                   | 13632714                                         |
| Innodb_buffer_pool_pages_free                      | 1                                                |
| Innodb_buffer_pool_pages_made_not_young            | 63838956                                         |
| Innodb_buffer_pool_pages_made_young                | 4423674                                          |
| Innodb_buffer_pool_pages_misc                      | 0                                                |
| Innodb_buffer_pool_pages_old                       | 238537                                           |
| Innodb_buffer_pool_pages_total                     | 648960                                           |
| Innodb_buffer_pool_pages_lru_flushed               | 27296                                            |
| Innodb_buffer_pool_pages_lru_freed                 | 129052                                           |
| Innodb_buffer_pool_pages_split                     | 7986287                                          |
| Innodb_buffer_pool_read_ahead_rnd                  | 0                                                |
| Innodb_buffer_pool_read_ahead                      | 103442                                           |
| Innodb_buffer_pool_read_ahead_evicted              | 20393                                            |
| Innodb_buffer_pool_read_requests                   | 200505277507                                     |
| Innodb_buffer_pool_reads                           | 2039620                                          |
| Innodb_buffer_pool_wait_free                       | 84                                               |
| Innodb_buffer_pool_write_requests                  | 12518551898                                      |
| Innodb_checkpoint_age                              | 2674470447                                       |
| Innodb_checkpoint_max_age                          | 4347944940                                       |
| Innodb_data_fsyncs                                 | 16676106                                         |
| Innodb_data_pending_fsyncs                         | 0                                                |
| Innodb_data_pending_reads                          | 0                                                |
| Innodb_data_pending_writes                         | 0                                                |
| Innodb_data_read                                   | 46524465152                                      |
| Innodb_data_reads                                  | 2840116                                          |
| Innodb_data_writes                                 | 158861173                                        |
| Innodb_data_written                                | 3247794442176                                    |
| Innodb_dblwr_pages_written                         | 6190287                                          |
| Innodb_dblwr_writes                                | 53199                                            |
| Innodb_deadlocks                                   | 0                                                |
| Innodb_history_list_length                         | 1                                                |
```

```
Ssl_server_not_after
Ssl_server_not_before
Ssl_session_cache_hits                             0
Ssl_session_cache_misses                           0
Ssl_session_cache_mode                             NONE
Ssl_session_cache_overflows                        0
Ssl_session_cache_size                             0
Ssl_session_cache_timeouts                         0
Ssl_sessions_reused                                0
Ssl_used_session_cache_entries                     0
Ssl_verify_depth                                   0
Ssl_verify_mode                                    0
Ssl_version
Subquery_cache_hit                                 110703086
Subquery_cache_miss                                118465189
Syncs                                              25406
Table_locks_immediate                              4102
Table_locks_waited                                 0
Table_open_cache_active_instances                  1
Table_open_cache_hits                              0
Table_open_cache_misses                            0
Table_open_cache_overflows                         0
Tc_log_max_pages_used                              0
Tc_log_page_size                                   0
Tc_log_page_waits                                  0
Threadpool_idle_threads                            0
Threadpool_threads                                 6
Threads_cached                                     5
Threads_connected                                  36
Threads_created                                    73
Threads_running                                    1
Transactions_gtid_foreign_engine                   0
Transactions_multi_engine                          0
Update_scan                                        0
Uptime                                             16342705
Uptime_since_flush_status                          16342705
Wsrep
Wsrep_applier_thread_count                         0
Wsrep_cluster_capabilities                         0
Wsrep_cluster_conf_id                              18446744073709551615
Wsrep_cluster_size                                 0
Wsrep_cluster_state_uuid
Wsrep_cluster_status                               Disconnected
Wsrep_connected                                    OFF
Wsrep_local_bf_aborts                              0
Wsrep_local_index                                  18446744073709551615
Wsrep_provider_capabilities
```

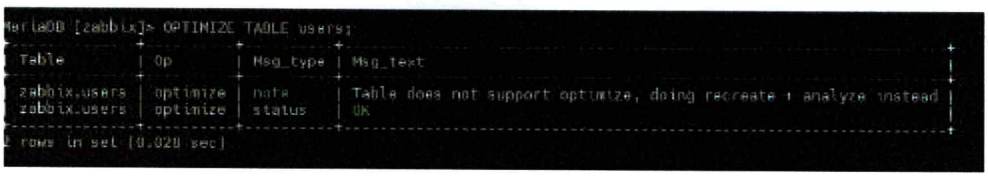
después de reindexar todas las tablas, es una buena práctica optimizar toda la base de datos para recuperar espacio y mejorar aún más el rendimiento:



Se realiza la configuración de las tablas sobre las bases de datos.

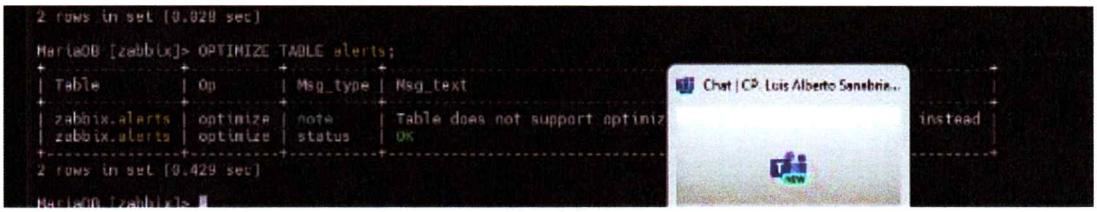


Optimización tabla tareas.



Optimización de los usuarios.

IDENTIAN®	ACTA DE REUNIÓN	Código: FR-SI-SGSI-10 Fecha emisión: 10/07/2017 Versión: 01



Optimización de la tabla de alertas.

Compromiso y/o acuerdo	Responsable	Plazo / Fecha	Estado
Revisión de Grafana	Brian Diaz	04 de Julio de 2024	No realizado
Fecha Próxima Reunión		04 de julio de 2024	

Observaciones: N/A

Firmas:

Firma del Cliente

Firma del Proveedor

iDENTIAN®	ACTA DE REUNIÓN	Código: FR-SI-SGSI-10 Fecha emisión: 10/07/2017 Versión: 01

FECHA: DD 15 MM 07 AAAA 2024

ACTA DE ACTIVIDADES REALIZADAS EN LA VIGENCIA DEL CONTRATO

- Se realiza el seguimiento de las actividades del proyecto de COMANDO GENERAL DE LAS FUERZAS MILITARES.
- Se ha prestado soporte 7x24 durante 3 de 12 meses del contrato, por medio de acceso remoto, soporte telefónico y personal en sitio cumpliendo los siguientes ANS:
  - Soporte de manera remota con tiempos de atención de máximo 4 horas después de reportar la falla.
  - Atención en sitio con menos de 2 horas de respuesta para incidentes críticos.
- El servicio se ha prestado de manera remota y presencial durante la vigencia del contrato como consta en las actas.
- Para escalamientos y reportes de incidentes se realizó por medio del número 322 682 4932 y el correo operaciones@identian.co
- Durante los meses que se ha prestado el servicio, se han realizado las siguientes actividades:
  - Actualizaciones (Update, upgrade y críticas de seguridad)
  - Revisión y solución de errores.
  - Realización y programación de copias de seguridad.
  - Revisión de logs.
- Las actividades anteriormente expuestas se realizaron sin generar ningún tipo de indisponibilidad.

Observaciones: N/A

Firmas:



Firma del Proveedor

Bogotá, julio 23 de 2024

Señores:
COGFM
Bogotá D.C.

Asunto: Actividades realizadas en la vigencia del contrato.

Estimados Señores:

De acuerdo con el contrato, se realizan actividades correspondientes al proyecto de COMANDO GENERAL DE LAS FUERZAS MILITARES, teniendo en cuenta lo anterior, se presta soporte 7x24 durante la vigencia del contrato, por medio de acceso remoto, soporte telefónico y personal en sitio cumpliendo los siguientes ANS:

Soporte de manera remota con tiempos de atención de máximo 4 horas después de reportar la falla.
Atención en sitio con menos de 2 horas de respuesta para incidentes críticos.

Dicho servicio se entrega de manera remota y presencial como consta en las actas. Cabe resaltar que para escalamientos y reportes de incidentes se han realizado por medio del número 322 682 4932 y el correo operaciones@identian.co con el Ing. Andres Cardozo Rodríguez.

Saludos,

Robin José Salcedo Buelvas
Representante Legal
CC. 77.090.560 de Valledupar
rsalcedo@identian.co
www.identian.co
PBX. 601-7042400 - 3014873962

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE	DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900678711-3	IDENTIAN SAS	CR 80b#24a-40	3014873962	INFO@IDENTIAN.CO	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL / CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO		
ÚNICA	B – menos de 200 c		BOGOTÁ D. C.	BOGOTÁ, D.C.		SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
					10	0
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR	
2024-07	2024-06	E	03/07/2024	78396946	$7.932.700	

TOTALES POR SUBSISTEMAS

TOTALES SALUD

Código EPS	Nombre	NIT	Cotización Obligatoria	UPC Adicional	Incapacidades		Licencia Maternidad		Días Mora	Valor Mora Cotización	Valor Mora UPC	Total a Pagar	No. Afiliados
					No. Autorización	Valor	No. Autorización	Valor					
EPS001	ALIANSALUD EPS S.A.	830113831-0	440.000	0		0		0	0	0	0	440.000	1
EPS002	Salud Total EPS	800130907-4	112.000	0		0		0	0	0	0	112.000	2
EPS005	Sanitas EPS	800251440-6	476.000	0		0		0	0	0	0	476.000	3
EPS008	Compensar EPS	860066942-7	52.000	0		0		0	0	0	0	52.000	1
EPS017	Famisanar EPS	830003564-7	124.000	0		0		0	0	0	0	124.000	2
EPS037	Nueva EPS	900156264-2	72.000	0		0		0	0	0	0	72.000	1

TOTALES PENSIÓN

Código AFP	Nombre	NIT	Cotización Obligatoria	Aporte Voluntario Afiliado	Aporte Voluntario Aportante	Aporte FSP - Solidaridad	Aporte FSP - Subsistencia	Días Mora	Valor Mora Cotización	Valor Mora FSP	Total a Pagar	No. Afiliados
230201	Proteccion (ING + Proteccion)	800229739-0	448.000	0	0	0	0	0	0		448.000	2
230301	Porvenir	800224808-8	1.376.000	0	0	0	0	0	0		1.376.000	5
230901	Skandia Pensiones Obligatorias	800253055-2	1.759.900	0	0	55.000	55.000	0	0		1.869.900	1
231001	Colfondos	800227940-6	720.000	0	0	0	0	0	0		720.000	1
25-14	Colpensiones	900336004-7	800.000	0	0	0	0	0	0		800.000	1

TOTALES RIESGOS LABORALES

Código ARL	Nombre	NIT	Cotización Obligatoria	Incapacidades		Aportes Otros Sistemas	Valor Neto Cotización	Días Mora	Valor Mora Cotización	Subtotal Cotización	No. Radicado Saldo a Favor	Valor Saldo a Favor	Fondo Solidaridad	Total a Pagar	No. Afiliados
				No. Autorización	Valor										
14-11	ARL SURA	890903790-5	166.800				166.800	0	0	166.800			1.668	166.800	10

TOTALES CAJAS

Código CCF	Nombre	NIT	Valor Aporte	Días Mora	Valor Mora Aporte	Total a Pagar	No. Afiliados
CCF24	Compensar Caja	860066942-7	1.276.000	0	0	1.276.000	10

PAGADA

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE		DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900678711-3	IDENTIAN SAS		CR 80b#24a-40	3014873962	INFO@IDENTIAN.CO	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO		
ÚNICA	B – menos de 200 c			BOGOTÁ D. C.	BOGOTÁ, D.C.		SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
					10	0
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR	
2024-07	2024-06	E	03/07/2024	78396946	$7.932.700	

TOTALES PARAFISCALES				
Valor Aporte	Días Mora	Valor Mora Aporte	Total a Pagar	No. Afiliados
SENA				
0	0	0	0	0
ICBF				
0	0	0	0	0
ESAP				
MEN				

TOTALES POR SUBSISTEMA			
Tipo Administradora	No. Administradoras Reportadas	Valor antes de IGE, LMA, IRP y Mora	Total a Pagar
Salud	6	1.276.000	1.276.000
Pensión	5	5.213.900	5.213.900
Riesgos Laborales	1	166.800	166.800
CCF	1	1.276.000	1.276.000
ESAP	0	0	0
ICBF	0	0	0
MEN	0	0	0
SENA	0	0	0
TOTALES	**13**	7.932.700	7.932.700

PAGADA

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE		DIRECCIÓN	TELÉFONO	CORREO
NI	900678711-3	IDENTIAN SAS		CR 80b#24a-40	3014873962	INFO@IDENTIAN.CO
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	
ÚNICA	B – menos de 200 c			BOGOTÁ D. C.	BOGOTÁ, D.C.	

EXONERADO PAGO PARAFISCALES Y SALUD
SI

DATOS DE LA PLANILLA					
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD
					EMPLEADOS: 10 / UPC: 0
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR
2024-07	2024-06	E	03/07/2024	78396946	$7.932.700

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE									INFORMACIÓN NOVEDADES																PENSIÓN							SALUD			RIESGOS LABORALES				CCF				PARAFISCALES				
No.	Tipo	No. de Identificación	Apellidos y Nombres	Cotizante	Subtipo	Extranjero	Cotiza. exterior	Exonerado	ING	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRL	CORRECCIÓN	Cód. AFP	IBC AFP	Cotización	Voluntario Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Clase de Riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Ap M
1	CC	1000617102	SANABRIA HERNANDEZ MAYRA ALEJANDRA	1	0			S																	230201	1.500.000	240.000	0	0	0	0	EPS002	1.500.000	60.000	14-11	1.500.000	1	7.900	CCF24	1.500.000	60.000	0	0	0	0	
2	CC	1003400525	HUERTAS ORTIZ GABRIEL ENRIQUE	1	0			S																	230301	1.300.000	208.000	0	0	0	0	EPS008	1.300.000	52.000	14-11	1.300.000	1	6.800	CCF24	1.300.000	52.000	0	0	0	0	
3	CC	1012375277	DIAZ NEISA BRIAN ALEXANDER	1	0			S																	230301	1.800.000	288.000	0	0	0	0	EPS017	1.800.000	72.000	14-11	1.800.000	1	9.400	CCF24	1.800.000	72.000	0	0	0	0	
4	CC	1016060373	CASTRO CARRILLO MONICA FERNANDA	1	0			S																	230301	1.800.000	288.000	0	0	0	0	EPS037	1.800.000	72.000	14-11	1.800.000	1	9.400	CCF24	1.800.000	72.000	0	0	0	0	
5	CC	1018440090	CARDOZO RODRIGUEZ ANDRES DAVID	1	0			S	X																231001	4.500.000	720.000	0	0	0	0	EPS005	4.500.000	180.000	14-11	4.500.000	1	23.500	CCF24	4.500.000	180.000	0	0	0	0	
6	CC	1028781290	GONZALEZ VALDERRAMA JASETH STIVEN	1	0			S																	230301	1.300.000	208.000	0	0	0	0	EPS002	1.300.000	52.000	14-11	1.300.000	1	6.800	CCF24	1.300.000	52.000	0	0	0	0	
7	CC	77090560	SALCEDO BUELVAS ROBIN JOSE	1	0			S																	230901	10.999.017	1.759.900	0	0	55.000	55.000	EPS001	10.999.017	440.000	14-11	10.999.017	1	57.500	CCF24	10.999.017	440.000	0	0	0	0	
8	CC	79629459	GRANADOS CASTRO HENRY	1	0			S	X																230301	2.400.000	384.000	0	0	0	0	EPS005	2.400.000	96.000	14-11	2.400.000	1	12.600	CCF24	2.400.000	96.000	0	0	0	0	
9	CC	80154844	DI Z OR IZ R HUZ GIOVA Y	1	0			S																	25-14	5.000.000	800.000	0	0	0	0	EPS008	5.000.000	200.000	14-11	5.000.000	1	26.100	CCF24	5.000.000	200.000	0	0	0	0	
10	CC	1077145726	CARDENAS AREVALO DANIEL ANDRES	1	0			S																	230201	1.300.000	208.000	0	0	0	0	EPS017	1.300.000	52.000	14-11	1.300.000	1	6.800	CCF24	1.300.000	52.000	0	0	0	0	

PAGADA

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

Señores
IDENTIAN S.A.S.
Bogotá D.C.

Fui nombrado revisor fiscal de IDENTIAN S.A.S., identificada con NIT. 900.678.711-3 el 01 de abril de 2024. Desde mi nombramiento he desarrollado los procedimientos necesarios para cumplir con mis funciones como Revisor Fiscal.

Los registros auditados por el periodo de seis meses comprendido entre el 1 de enero y el 30 de junio de 2024 d las ubcuentas 23 5 "Aporte Salud", 37 5 "Aport s ARL", 23 01 "Aportes Caja d Compensación y 2 8 "F nd d Pensiones , incluyen la causación de los aportes a los sistemas de salud, riesgos laborales, aportes al fondo de pensiones obligatorio, aportes a las cajas de compensación familiar, la entidad no realiza aportes al Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, conforme al artículo 114-1 del Estatuto Tributario. Las planillas integradas liquidación evidencian el pago de los aportes por el periodo antes mencionado.

La información financiera y contable, es responsabilidad de la Administración de la Compañía.

Con base a los procedimientos ejecutados a la fecha, no estoy enterado de situaciones que impliquen cambios significativos a la información anteriormente indicada.

Esta certificación se expide por solicitud de la Compañía en cumplimiento del artículo 50 de la ley 789 de 2002, y no debe ser utilizada para ningún otro propósito.

JAVIER STIVEN MUÑOZ URIBE
Revisor Fiscal
TP 258022 – T
Bogotá, D.C, 17 de julio de 2024

Bogotá, Julio 11 de 2024

Señores:
CGFM
Ciudad

Asunto: Facturación de contrato150COGFM DIADF2024

Estimados Señores:

Te iendo cuenta el contrato 150COG M DIAD 2024, cuyo objeto s "Servicio de Mantenimiento para la Herramienta de Monitoreo, Detección y Alertamiento de Eventos sobre la Infraestructura de TI de COGFM", y que el Supervisor del Contrato el Sr. Teniente Nicolas Ramirez, realiza la solicitud de generación de factura por el cincuenta porciento (50%)
Hemos emitido la Factura FAID 1001 por valor de $49.500.00.01 y encontramos que se presenta una diferencia de mayor valor frente a lo estipulado en la liquidación por un centavo ($0.01) en el valor del IVA, esta diferencia se presenta porque al subir el valor de la base de la factura a nuestra plataforma contable (SIIGO), el valor del IVA se aproxima al siguiente decimal, ocasionando en el valor total de la factura haya un centavo ($0.01) de diferencia, elevamos esta consulta a asesoría en la DIAN y nos dicen que no es posible hacer una NC por un centavo ($0.01) ya que se afectaría el valor base de la factura.
Teniendo esto en cuenta certificamos y confirmamos con este documento que Identian no cobrará esta diferencia y asume ese centavo ($0.01) en la diferencia del IVA y no hará cobro de él, esta situación también está en conocimiento del Supervisor del contrato el Teniente Nicolas Ramirez.
Por lo tanto el valor a cancelar por parte del Comando General de las Fuerzas Militares será de $49.500.000.00= Cuarenta y nueve millones quinientos mil pesos.

Agradecemos de antemano su amable atención y gestión.

Saludos,

Robin José Salcedo Buelvas
Representante Legal
CC. 77.090.560 de Valledupar
rsalcedo@identian.co
www.identian.co
PBX. 601-7042400 - 3014873962