



UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE INGENIERÍA Y ARQUITECTURA**  
**ESCUELA PROFESIONAL DE INGENIERÍA DE**  
**SISTEMAS**

Unified Threat Management (UTM) para la gestión de los servicios de seguridad basado en COBIT 5 en la empresa REM SYSTEMS S. A. C.

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:**

**Ingeniero de Sistemas**

**AUTOR:**

Godoy Fuentes, Luis Arnaldo (orcid.org/0000-0002-3910-219X)

**ASESOR:**

Mg. Ormeño Rojas, Robert Eduardo (orcid.org/0000-0002-8104-9310)

**LÍNEA DE INVESTIGACIÓN:**

Infraestructura de Servicio de Redes y Comunicaciones

**LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:**

Desarrollo económico, empleo y emprendimiento

**LIMA – PERÚ**

**2021**

### **Dedicatoria**

Este trabajo de tesis es dedicado a Dios todo poderoso por darme salud y por guiar cada uno de mis pasos. A mi adorada mamá Marlene Fuentes Obregón que amo con todo mi corazón por alentarme desde niño a salir adelante y luchar por alcanzar mis sueños. A mi hermana Cheltsi Godoy Fuentes por todo su apoyo y su aliento.

## **Agradecimiento**

En primer lugar, doy gracias a Dios por acompañarme y conducir cada uno de mis pasos. A mis queridos tíos Arnaldo Fuentes y Belfor Fuentes por todo su apoyo y sus consejos, y finalmente a la empresa Rem Systems por brindarme todas las facilidades para el desarrollo del proyecto.

## Índice de contenidos

Carátula.....	i
Dedicatoria .....	ii
Agradecimiento .....	iii
Índice de contenidos .....	iv
Índice de tablas .....	v
Índice de figuras .....	vi
Resumen .....	vii
Abstract .....	viii
I. INTRODUCCIÓN.....	1
II. MARCO TEÓRICO.....	5
III. METODOLOGÍA.....	31
3.1 Tipo y diseño de la metodología.....	31
3.2 Variables y operacionalización.....	33
3.3 Población, muestra y muestreo.....	35
3.4 Técnicas e instrumentos de recolección de datos.....	36
3.5 Procedimiento.....	37
3.6 Métodos de análisis de datos.....	41
3.7 Aspectos éticos .....	46
IV. RESULTADOS .....	47
V. DISCUSIÓN.....	62
VI. CONCLUSIONES.....	64
VII. RECOMENDACIONES .....	65
REFERENCIAS .....	66
ANEXOS.....	71



## Índice de tablas

Tabla 1: Operacionalización de variables .....	33
Tabla 2: Indicadores de la variable dependiente .....	344
Tabla 3: Validez de las fichas de registro .....	37
Tabla 4: Grados de correlación de Pearson .....	39
Tabla 5: SPSS – Número de vulnerabilidades descubiertas (NVD) .....	40
Tabla 6: SPSS - Número de incidentes en dispositivos de usuario final (NIF) .....	40
Tabla 7: Medidas descriptivas del indicador “número de vulnerabilidades descubiertas” antes y después de la implementación del “Unified Threat Management (UTM)” .....	47
Tabla 8: Medidas descriptivas del indicador “número de incidentes en dispositivos de usuario final” antes y después de la implementación del “Unified Threat Management (UTM)” .....	49
Tabla 9: Prueba de normalidad del indicador “número de vulnerabilidades descubiertas” antes y después de implementar el “Unified Threat Management (UTM)” .....	51
Tabla 10: Prueba de normalidad del indicador “número de incidentes en dispositivos de usuario final” antes y después de implementar el “Unified Threat Management (UTM)”	53

## Índice de figuras

Figura 1: Unified Threat Management .....	15
Figura 2: Appliance Hardware UTM .....	16
Figura 3: Appliance Software UTM.....	17
Figura 4: Seguridad perimetral .....	18
Figura 5: Familia de productos de COBIT 5 .....	19
Figura 6: Modelo de referencia de procesos de COBIT 5 .....	21
Figura 7: Métricas del proceso DSS05.....	22
Figura 8: Prácticas de gestión del proceso DSS05 “Gestionar servicios de seguridad”.....	23
Figura 9: Coeficiente de correlación de Pearson.....	38
Figura 10: Nivel de significancia y confiabilidad .....	45
Figura 11: Número de vulnerabilidades descubiertas antes y después de implementar el “Unified Threat Management (UTM)” .....	48
Figura 12: Número de incidentes en dispositivos de usuario final antes y después de implementar el “Unified Threat Management (UTM)” .....	50
Figura 13: Prueba de normalidad del indicador número de vulnerabilidades descubiertas antes de implementar el Unified Threat Management (UTM).....	52
Figura 14: Prueba de normalidad del indicador número de vulnerabilidades descubiertas después de implementar el Unified Threat Management (UTM).....	53
Figura 15: Prueba de normalidad del indicador número de incidentes en dispositivos de usuario antes de implementar el Unified Threat Management (UTM) .....	54
Figura 16: Prueba de normalidad del indicador número de incidentes en dispositivos de usuario después de implementar el Unified Threat Management (UTM) .....	55
Figura 17: Número de vulnerabilidades descubiertas antes de implementar el Unified Threat Management (UTM) .....	57
Figura 18: Número de vulnerabilidades descubiertas antes de implementar el Unified Threat Management (UTM) .....	57
Figura 19: Número de vulnerabilidades descubiertas (Comparativa general) .....	58
Figura 20: Número de incidentes en dispositivos de usuario final antes de implementar el Unified Threat Management (UTM) .....	60
Figura 21: Número de incidentes en dispositivos de usuario final después de implementar el Unified Threat Management (UTM).....	60
Figura 22: Número de incidentes en dispositivos de usuario final (Comparativa general)61	

## Resumen

Este trabajo de investigación propone y tiene como objetivo principal la implementación de un “Unified Threat Management” (UTM) para la gestión de servicios de seguridad basado en COBIT 5 en la empresa REM Systems SAC con el fin de reducir el número de vulnerabilidades, el número de incidentes en los dispositivos de los usuarios finales y garantizar la protección de la red interna frente a amenazas de ciberseguridad.

En el desarrollo del proyecto se utilizó el marco de gobierno y gestión de “COBIT 5 para la seguridad de la información”. Como investigación aplicada, su diseño es experimental con un diseño de investigación de tipo preexperimental. De esa forma, se tomó como población el número de vulnerabilidades e incidentes semanales registrados en 2 hojas de reporte, y teniendo como muestra para el indicador el índice del número de vulnerabilidades descubiertas, de dos hojas de reporte semanales se tomaron 14 días. Para el indicador, el índice del número de incidentes en los dispositivos de los usuarios finales, se tomaron 14 días de dos hojas de reporte semanales. Se utilizaron como técnica herramientas de registro e investigación como el formulario de registro.

Al final de la implementación de la UTM, el número de vulnerabilidades descubiertas se ha reducido y lo podemos demostrar comparando estas cifras: antes de la implementación había un promedio de 83,14 vulnerabilidades diarias, después de haber realizado la implementación se ha reducido a 1,29 vulnerabilidades diarias. Del mismo modo, se ha reducido el número de incidencias en los dispositivos de los usuarios finales. Antes de la implementación, se producía una media de 252,86 incidentes por día. Tras la implantación se ha reducido a 3,86 incidencias diarias.

Finalmente, se concluye demostrando que la implementación de una “Gestión Unificada de Amenazas (UTM)” garantiza una medida efectiva de protección y contención contra ataques, vulnerabilidades y amenazas de ciberseguridad en la empresa REM Systems S.A.C.

**Palabras clave:** Unified Threat Management, UTM, gestión de servicios de seguridad.

## Abstract

This research work proposes and has as its main objective the implementation of a “Unified Threat Management” (UTM) for the management of security services based on COBIT 5 in the company REM Systems SAC in order to reduce the number of vulnerabilities, the number of incidents on end-user devices and ensure the protection of the internal network from cybersecurity threats.

In the development of the project, the governance and management framework of “COBIT 5 for information security” was used. As applied research, its design is experimental with a pre-experimental research design type. In that way, the number of weekly vulnerabilities and incidents recorded in 2 report sheets was taken as the population, and having as a sample for the indicator the index of the number of vulnerabilities discovered, 14 days were taken from two weekly report sheets. For the indicator, the index of the number of incidents on end-user devices, 14 days were taken from two weekly report sheets. Recording and research tools such as the registration form were used as a technique.

At the end of the implementation of the UTM, the number of the discovered vulnerabilities has been reduced and we can demonstrate this by comparing these figures: before the implementation there was an average of 83.14 daily vulnerabilities, after having carried out the implementation it has been reduced to 1.29 daily vulnerabilities. In the same way, the number of incidents on end-user devices has been reduced. Before the implementation, there was an average of 252.86 incidents per day. After the implementation, it has been reduced to 3.86 incidents per day.

Finally, it is concluded by demonstrating that the implementation of a “Unified Threat Management (UTM)” guarantees an effective protection and containment measure against attacks, vulnerabilities and cybersecurity threats in the company REM Systems S.A.C.

**Keywords:** Unified Threat Management, UTM, security services management.

## I. INTRODUCCIÓN

La presente investigación se refiere a un tema actual de gran importancia a nivel mundial, tan solo a inicios del año 2020 se han registrado más de 443 millones de ciberataques en el Perú, actualmente todas las empresas de toda índole hacen uso de tecnologías computacionales para poder automatizar sus procesos, operaciones, agilizar su manufactura, ingresar a nuevos mercados, realizar transacciones comerciales, etc. Todo ello para lograr sus metas trazadas como empresas, instituciones u organización.

Este proyecto de investigación trata de la implementación de un Unified Threat Management (UTM) para la gestión de servicios de seguridad basado en COBIT 5 en la empresa REM Systems S.A.C. La implementación de este proyecto va permitir reducir el número de vulnerabilidades descubiertas y reducir el número de incidentes en dispositivos de usuario final, de esta manera minimizaremos todos los riesgos y amenazas de ciberseguridad, haciendo uso de las mejores tecnologías en seguridad informática según el cuadrante de Garner como Fortinet, además de seguir las recomendaciones de su implementación basados en el NIST y las buenas prácticas de COBIT 5 en su guía profesional de “Para la seguridad de la información”.

La presente investigación se subdivide en los siguientes capítulos: El capítulo I Introducción, donde se detalla la realidad problemática, antecedentes, teorías, justificación del estudio, hipótesis y objetivos. El capítulo II Método, donde detalla el diseño de investigación, las variables, población, muestra, técnica e instrumentos, métodos de análisis y aspectos éticos que se va emplear en la investigación. El capítulo III detalla los resultados que se obtuvieron en la investigación. El capítulo IV indica la discusión que se pudo llegar de la investigación. El capítulo V presenta las conclusiones obtenidas en la investigación. El capítulo VI detalla las recomendaciones que se debe tomar en cuenta. Y por último en el capítulo VII se detalla las referencias bibliográficas de la investigación.

Según Barrientos (2017, p.43) Actualmente las empresas han cambiado de manera significativa con la llegada del internet, aquella empresa que no hace uso de internet y se adapta, no tendrá éxito y terminará saliendo del mercado; es por ello que actualmente la el internet es una necesidad indispensable y vital para el negocio.

Para Javier y Santiago (2017, p.6) “El uso de internet en los procesos de negocio no solo trae beneficios importantes a las empresas y a los usuarios, también implica muchos y potenciales riesgos de seguridad, es por ello que la interconexión entre la red interna y la red externa (internet) no solo expande el mercado corporativo, sino que también la expone a los activos de información a una gran cantidad de vulnerabilidades y amenazas. “

Según Dejan Kosutic (2012, p.14) “Los ataques cibernéticos y las violaciones de seguridad suceden a cada minuto y son demasiado generalizadas como para localizarlas, algunas son más destructivas y maliciosas que otras, algunas logran su cometido y otras no. Pero los daños pueden ser incalculables e irreversibles”

Marañón y Pérez (2021) Mencionó: Según todos los estudios realizados, las grandes empresas son las más atacadas y en menor medida las medianas y las pequeñas que son también principales objetivos. El hecho de que más del 80% de ataques se realiza en forma remota. Las dos mayores amenazas a las que se encuentran expuestos los equipos de una organización como los servidores y las estaciones de trabajo e implícitamente los datos, son los hackers y el malware.

Según Zambrano (2015) “Por medio de una investigación realizada se evidencia al Perú como el quinto país de Latinoamérica que recibe más ataques cibernéticos llegando a un índice de 11.22% de los 19% de ataques que sufre el continente americano a nivel global. El sector financiero a nivel de la región ha pasado del segundo al primer puesto en cuando a incidentes de cibernéticos con el 75.29% de casos, dando un margen de 6.6 millones de ataques por día.”

Rem Systems SAC es una empresa de servicios, proyectos y consultoría de TI, partner de las principales marcas en tecnologías de la información como Microsoft, Veeam, Red Hat, McAfee, HP y otros. La empresa realiza servicios a clientes en sitio como tercero en administración y gestión de TI, implementación y mantenimiento de infraestructura de TI, soporte técnico, redes; y desde sus instalaciones brinda el servicio de mesa de ayuda.

La problemática en la empresa Rem Systems SAC se encuentra en la seguridad de la red perimetral, ya que en su centro de datos solo cuenta con un Firewall/Proxy basado en Linux Red Hat que es ineficiente ante los diversos y avanzados tipos de ataques maliciosos provenientes desde la red externa (internet); actualmente todo el tráfico proveniente y saliente desde internet fluye sin protección criptográfica, no existen mecanismos de detección y prevención de intrusiones, tampoco existen servicios de análisis y eliminación de amenazas de tráfico web y tráfico de correo, finalmente, el servidor Firewall/proxy no permite realizar monitoreo ni brinda métricas para una buena gestión de la seguridad perimetral.

La pandemia del COVID-19 ha originado que el presente proyecto sea más ambicioso, porque el gobierno peruano a través de un decreto supremo dispuso cuarentena general en el país, por ello, todas las actividades laborales de la empresa Rem Systems SAC tuvieron que realizarse de forma remota desde las casas de nuestros colaboradores

a través de aplicaciones de escritorio remoto (TeamViewer, AnyDesk), esto es un fallo de seguridad que deja puertas traseras abiertas en la red que harían aún más vulnerable la red perimetral.

En las condiciones y el contexto planteado es urgente la necesidad de encontrar una solución al problema de la seguridad, que se adapte a los requerimientos expuestos y nos brinde numerosas ventajas como escalabilidad, actualizaciones permanentes, soporte y las propiedades de integración unificada de servicios de seguridad.

Por consiguiente, en el presente proyecto se propone implementar un Unified Threat Management (UTM) aplicando el proceso de gestión de seguridad del marco de COBIT 5, que permitirá asegurar la red perimetral de la empresa Rem Systems SAC y repeler todos los ataques y mitigar todas las vulnerabilidades y amenazas que se puedan presentar.



## II. MARCO TEÓRICO

Se ha revisado diversas publicaciones e investigaciones en diferentes bibliotecas digitales nacionales e internacionales, encontrándose los siguientes antecedentes:

### Nacional

- ❖ En el año 2018, Kenny Esleyther Ruiz Vieira y Wilson Delgado Ramos, desarrollaron el trabajo de titulación “Implementación de una solución de seguridad perimetral Open Source en la red telemática de la Universidad Nacional Pedro Ruiz Gallo” (Para obtención del título de Ingeniero de Sistemas) de la Universidad de Lambayeque.

La problemática que dio motivo al desarrollo de este proyecto, es que actualmente en la red telemática de la “Universidad Nacional Pedro Ruiz Gallo” no existe ningún dispositivo o tecnología que permita garantizar la seguridad perimetral de la red, por ello, ha sido víctima de ataques informáticos e intromisiones a la red interna ocasionando la inestabilidad de los servicios y robo de información. El tipo de investigación es de tipo aplicada experimental y descriptiva. Los resultados confirmaron que después de la puesta en producción de “PF-Sense” que es una tecnología “UTM Open Source”, ha habido un significativo descenso de las vulnerabilidades, que en promedio se tenía 113 por servicio reduciéndolo a 5.14, y el “Sistema académico” siendo el más atacado con 287 vulnerabilidades, ha disminuido a 10.

- ✓ Este antecedente permitió tener una visión más clara sobre el desempeño de las tecnologías “UTM Open Source” respecto a la protección de las redes internas dentro del ámbito de la seguridad perimetral y la ciberseguridad, adicionalmente ayudó como referencia para redactar las teorías relacionadas al tema.

- ❖ En el año 2016, Renzo Giancarlo Da Silva de Oliveira y Jony Rene Silva Ledesma, desarrollaron el trabajo de titulación “Efecto de la Implementación del sistema PF-Sense en la seguridad perimetral lógica en los servicios de la red troncal de la Universidad Nacional de la Amazonía” para obtener del título de Ingeniero de Computación y Sistemas en la Universidad Privada de la Selva Peruana.

La problemática que dio motivo al desarrollo de este proyecto, fue que se ha estado utilizando un firewall “FreeBSD v6.3” desde hace más de 10 años, y no contaba con soporte, además, se ha detectado fallos y limitaciones en su operatividad, todo lo mencionado conlleva a que existía una sobreexposición y vulnerabilidad a cualquier ataque informático. El presente estudio es una investigación pre experimental, la población ah sido conformada por la cantidad de intentos de ingreso a la red perimetral lógica durante todos los días del año. Como resultado y brindando una solución a esta problemática se implementó “PF-Sense” sin generar costos de producto por estar basado en tecnologías “Open Source”, cumpliendo con todas las expectativas de ciberseguridad y protección perimetral permitiendo reducir las vulnerabilidades identificadas de 104.6 a 3.3 vulnerabilidades por servicio.

- ✓ Este antecedente ha servido para conocer los servicios y herramientas tecnológicas asociadas al “Unified Threat Management (UTM) y el impacto positivo que ha generado al minimizar las vulnerabilidades y proteger la red perimetral a partir de su implementación.

- ❖ En el año 2017, Omar Bautista Pillaca, desarrolló el trabajo de titulación “Implementación de un servidor Linux y su influencia en la seguridad perimetral de la red local de la empresa Junefield Group S. A.” Para obtención del título de Ingeniero de Sistemas en la Universidad Cesar Vallejo.

El problema que dio motivo al desarrollo de este proyecto es la falta de seguridad perimetral en las redes de datos, ya que actualmente la empresa cuenta con escasas medidas de seguridad que no garantizan la confidencialidad, integridad y disponibilidad de los datos en la red interna. Esta investigación es de tipo aplicada bajo un enfoque cuantitativo. En este proyecto se implementó Linux Endian Firewall Community, que es una distribución “Open Source” especializada en seguridad perimetral y gestión unificada de amenazas (UTM); no tiene costo de licenciamiento y cuenta con el soporte de la comunidad. Los resultados de la implementación del proyecto evidenciaron los siguientes resultados: la confidencialidad pasó de 32.8% a un 95.7%, la integridad pasó de 69.11% a un 80.14% y finalmente la disponibilidad pasó de 90.0% un 94.6%.

- ✓ Esta tesis ha servido para demostrar la eficiencia las soluciones basadas en “UTM Open Source” como lo es “Linux Endian Firewall Community”. Finalmente, este proyecto de tesis ha servido como ejemplo para el desarrollo de la justificación institucional y la justificación económica.
  
- ❖ En el 2018, Rogelio Joseph Pacotaype, realizó la tesis titulada “Metodología integral para evaluar el rendimiento de firewalls” Para ser honrado con el título profesional de Ingeniero de sistemas en la Universidad Cesar Vallejo.

La problemática que se desarrolló en este proyecto de investigación es desarrollar una metodología para la evaluación de rendimiento de los equipos de seguridad firewalls, y aplicarla para determinar que los firewalls de tipo hardware tienen mayor desempeño y estabilidad que los firewalls de software que generalmente se implementan sobre un sistema operativo base. El diseño de la investigación fue pre experimental, el cual, los resultados obtenidos de las pruebas de

evaluación del desempeño de los firewalls dieron las siguientes conclusiones:

- a) Para esta investigación se evaluaron los Firewalls de hardware “Fortinet y Palo Alto” y los Firewalls de software “Endian y Sophos”.
  - b) Los “Firewalls de hardware” tienen mayor rendimiento en el desempeño de la red, mostrándose con un promedio de (4,4598 a 74,0398 Mbps) contra un (2,8584 a 42,0266 Mbps) de los “Firewalls de software”.
  - c) Asimismo, el indicador latencia que calcula el retardo que genera el Firewall cuando el tráfico pasa a través de él, se mostró favorable a los Firewalls de hardware, con un promedio de 10,228 s contra un promedio de 12,840 s de los Firewalls de software.
  - d) Respecto a quién tiene el mayor rendimiento en el filtrado antimalware, las pruebas se mostraron favorables con 61,6 % de un “Firewall de hardware” contra un 38,4 % de los Firewalls de software.
  - e) Después de realizar las pruebas para determinar quién consume más recursos, los resultados muestran favorable a los “Firewalls de hardware” con un promedio de 34,550% en CPU y 26,650% de RAM, en comparación a un “Firewall de Software” con un 46,050% de CPU y 34,350 % de RAM.
- ✓ La presente tesis sirvió para definir el tipo de arquitectura de “UTM” que se implementará en la empresa “Rem Systems SAC”. Tras el estudio realizado de este antecedente, se ha evidenciado y comprobado que las soluciones UTM basadas en “Appliance de Hardware” son más eficientes como los UTM de las

empresas Fortinet y Palo Alto, por ello se ha tomado la decisión de implementar en la empresa “Rem Systems SAC” la solución UTM basada en una arquitectura de “Appliance Hardware” de la empresa FORTINET.

- ❖ En el año 2018, César Renato Espinoza Chipane, desarrolló el trabajo de titulación “Propuesta de una red privada virtual para mejorar el servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A.” Para lograr titularse como Ingeniero de Sistemas en la Universidad Autónoma del Perú.

La problemática que dio motivo al desarrollo de este proyecto es que las conexiones de las tiendas Mass hacia las oficinas de Super Mercados Peruanos S.A. se establecen a través de enlaces de datos arrendados que presentan mala calidad e inestabilidad en las conexiones provocando inconvenientes en la carga de los sistemas de ventas generando colas de espera que perjudica la imagen corporativa. El desarrollo de este proyecto es de tipo aplicada pre experimental. Los resultados mostraron que tras la implementación de una “Red Privada Virtual” (VPN) redujo los tiempos de carga y conexión a los sistemas informáticos, reduciendo el tiempo de espera de un intervalo de “4 min - 7 min” a menos de 7 segundos, agilizando la atención de los clientes.

- ✓ La presente tesis sirvió para entender la importancia de una “red privada virtual” (VPN) en la interconexión de sucursales para el uso de los sistemas de información fuera de su red local. Además, ha servido como referente en el uso de tecnologías “Appliance hardware” de la empresa FORTINET, puesto que en este antecedente se implementó el UTM Fortigate-30E del cual solo se utilizó el módulo de VPN.

## Internacional

- ❖ En el año 2017, Ing. Guido Fabian Miguez Gómez, desarrolló el trabajo de titulación “Implementación de un sistema de gestión unificada de amenazas (UTM) para la empresa de Créditos Palacio del Hogar” (Para obtención del título de Magister en Seguridad Informática Aplicada) de la Escuela Superior Politécnica del Litoral de la Facultad de Ingeniería en Electricidad y Computación.

La problemática que dio motivo al desarrollo de este proyecto de tesis es brindar una solución a los problemas de seguridad perimetral, ya que la red interna no contaba con ningún dispositivo que proteja el tráfico entrante y saliente, y que impida conexiones o filtre los accesos no autorizados a los sistemas de información, a consecuencia de ello la empresa ha tenido precedentes de ataques informáticos y de robo de información. El desarrollo de esta tesis de implementación es de tipo aplicada. Como resultados de este antecedente se ha demostrado que la implementación del “UTM Endian Community” permitió mitigar todas las vulnerabilidades identificadas y aseguró el tráfico de la red perimetral, permitiendo facilitar la administración del tráfico de la red.

- ✓ De este trabajo se ha tomado se abstraído información valiosa para el marco teórico para mejorar la comprensión de las teorías relacionadas al tema en referencia al concepto de los Appliances Hardware, además contribuyó a reforzar los conocimientos sobre la importancia de las tecnologías UTM en la protección de la seguridad perimetral.
- ❖ En el año 2016, Orivaldo Kléber Lima Rios, desarrolló el trabajo de titulación “Melhores práticas para implantar política de segurança da informação e comunicação em instituições federais de ensino superior” (Para recibir el título de Master of Science Informatics) de la Universidad Federal de Pernambuco.

La problemática de este proyecto de tesis, recae en que el 65% las instituciones federales de educación superior en Brasil no tienen implementado o no adoptan políticas de seguridad de la información y las comunicaciones (PoSIC). Para la realización de este trabajo se utilizó el método inductivo y el tipo de investigación ha sido aplicada. De un estudio realizado a 104 instituciones de educación superior que reveló que solo 53 adoptan políticas de seguridad de la información y comunicaciones, pero necesitan ser actualizadas en base a las exigencias actuales. Como resultados finalmente se desarrollaron 42 prácticas diferentes que cubren todas las necesidades de las instituciones públicas y/o empresas privadas para planificar la implementación de políticas de seguridad (PoSIC) basado en guías de las mejores prácticas de ITIL v3, ISO/IEC 27002 y controles de seguridad de la información de la guía profesional de “COBIT 5 para la seguridad de la información”

- ✓ Este antecedente ha servido de aporte para la base teórica concerniente a COBIT 5, adicionalmente ayudó a comprender la importancia de implementar políticas de seguridad en las organizaciones y empresas para garantizar la seguridad de la información.
  
- ❖ En el año 2017, Sixto Geovanny Robayo Zapata y Yorvin Oswaldo Miraba Cercado, desarrollaron el trabajo de titulación “Implementación de un UTM Keiro para el control y mitigación de amenazas presentes en la red perimetral de la empresa Mindcorp S.A.” Para ser reconocido con el título de Ingeniero en Networking y Telecomunicaciones en la Universidad de Guayaquil.

Dio motivo al desarrollo de este proyecto porque desde el último semestre la empresa ha sufrido ataques malintencionados de forma concurrente a su red interna, todo ello se debe a que actualmente no cuenta con una infraestructura de seguridad adecuada para la

protección de la red interna y la red en el perímetro, adicionalmente carece de mecanismos de detección de intrusiones y cifrado de información por lo que la empresa ya ha sufrido de interceptación en sus conexiones originando el robo de información. El tipo de implementación se basa en una investigación de proyecto factible, aplicando la metodología de investigación de campo. Los resultados de la implementación de Keiro UTM de tipo Appliance en Software hizo que disminuyera el número de incidencias protegiendo a la red interna de amenazas y ataques malintencionados proporcionando una mayor efectividad en el rendimiento de la red.

- ✓ Este antecedente contribuyó en las teorías relacionadas al tema, además, brindó información muy precisa para poder comprender como sería la implementación del tipo de UTM Appliance Software que necesita no solo un servidor físico sino también un sistema operativo.
  
- ❖ En el año 2019, Andrés Mauricio Pérez Lasso y Gabriel Elias Pinto Gutiérrez, desarrolló el trabajo de titulación “Sistema de seguridad perimetral para el edificio Zeus de Arcotel basado en tecnologías UTM de código abierto” Para optar el título como Ingenieros Electrónicos en la Universidad Politécnica Salesiana sede Quito.

La problemática que dio motivo al desarrollo de este proyecto de tesis es que en “Acortel” una de las instituciones del gobierno de Ecuador, está por caducar la licencia de su Firewall “Palo Alto” que es la única medida de seguridad perimetral que tiene, adicionalmente tiene problemas de gestión de seguridad porque tiene servicios de seguridad dispersos en diversas plataformas las cuales no trabajan de manera integrada. La investigación de este proyecto de tesis es de tipo aplicada. Como resultado, se decidió migrar el Firewall “Palo Alto” a una solución “UTM Open Source” llamada “PF-Sense” que se ajustó a las necesidades de la institución y facilitó la migración del Firewall “Palo



Alto” y los servicios propietarios dispersos a un “UTM Appliance Software” que no necesita licencia y que cumple con todas las características de un UTM de nivel superior con los módulos fundamentales para establecer una sólida solución de seguridad perimetral en redes de datos.

- ✓ Este antecedente sirvió para comprender la importancia de tener integrado múltiples servicios de ciberseguridad en un solo dispositivo, además se utilizó como fuente de información para comprender el tipo de licenciamiento que tienen algunos Appliance Hardware como “Palo Alto”, finalmente evidenció el posicionamiento y preferencia de soluciones UTM de tipo “Open Source” para cuestiones de ciberseguridad.
  
- ❖ In 2020, Artem Voronkov, developed the Thesis "Usability of Firewall Configuration" (To obtain the title of Doctor Computer Science) in Karlstad University.

El objetivo principal de esta investigación es identificar brechas y problemas que no se han abordado adecuadamente en las guías de seguridad, ofreciendo a los profesionales de seguridad enfoques y procesos de configuración útiles que puedan establecer un conjunto de buenas prácticas y políticas de seguridad de nivel superior gestionada. La investigación es aplicada y los datos son recopilados utilizando métodos de investigación cuantitativos y cualitativos. La población de este proyecto de investigación estuvo conformada por 300 administradores de sistemas donde se recopilaron pensamientos, opiniones, y experiencias; todo ello basado en entrevistas y encuestas. Los resultados muestran los siguientes puntos importantes de esta investigación: Sobre la gestión de los dispositivos de seguridad, no siempre es beneficioso tener más de dos personas responsables de las medidas de seguridad. Existe una falta, o incluso ausencia de evaluación de usabilidad a la hora de elegir los dispositivos de

seguridad para la protección de la red. Finalmente, el estudio demuestra que es vital realizar un estudio y validar las capacidades del dispositivo de seguridad antes de implementarlo en un ambiente de producción.

- ✓ Este antecedente nos ha permitido entender lo importante que es la gestión de los dispositivos de seguridad en una organización y como debería delegarse la responsabilidad sobre ellos, además ayudó a concientizar la elección de dispositivos de seguridad en base a sus capacidades y a la usabilidad que se le dará para la protección de las redes en un ambiente de producción.

## **TEORÍAS RELACIONADAS AL TEMA**

Mencionaremos algunas definiciones teóricas que van a servir a la comprensión de la presente investigación en la sustentación de esta tesis.

### **Unified Threat Management (UTM)**

Según Whitman y Mattord (2016, p.536) Al Unified Threat Management (UTM) o en su traducción gestión unificada de amenazas, se le considera la nueva generación de Firewalls, viene a ser una solución híbrida que se caracteriza por integrar las capacidades actuales de seguridad informática y gestión de redes, cuentan con servicios integrados que trabajan y se administran de manera unificada bajo una sola consola de administración. Los servicios integrados que tienen por lo general los UTM son los servicios de: Firewall, IDS, IPS, VPN, Routing, Antivirus, Antispam, Antimalware, y seguridad web (HTTPS), entre otros.

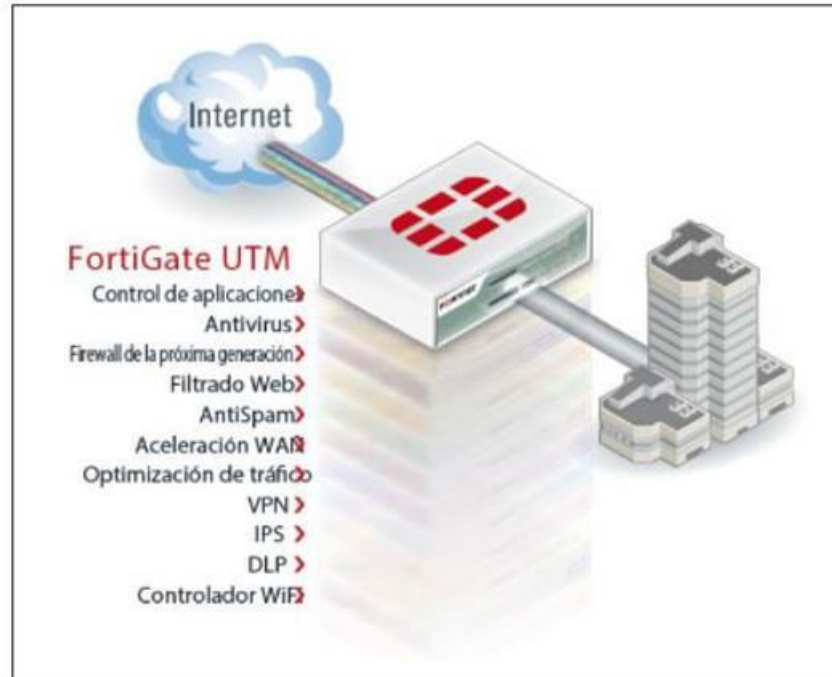


Figura 1: Unified Threat Management

## Appliances UTM

Según Barrett, Weiss y Hausman (2015, p.27) Los Appliance UTM son un conjunto de elementos (hardware, software y SO) que trabajan de manera embebida para realizar un proceso o tarea específica de forma integrada y colaborativa. Por lo general la arquitectura de los “Appliances UTM” pueden ser de tipo hardware o software. O sea: Appliances hardware y Appliances Software.

### – Appliance Hardware UTM

Es un equipo físico donde encontramos de manera embebida el software que vendría a ser los servicios o módulos y el sistema operativo, por lo general los “Appliance Hardware UTM” cuentan con una interfaz web para la administración, algunos cuentan con una Shell para realizar operaciones de administración más avanzadas por medio de comandos.

Fuente: Fortinet, 2013

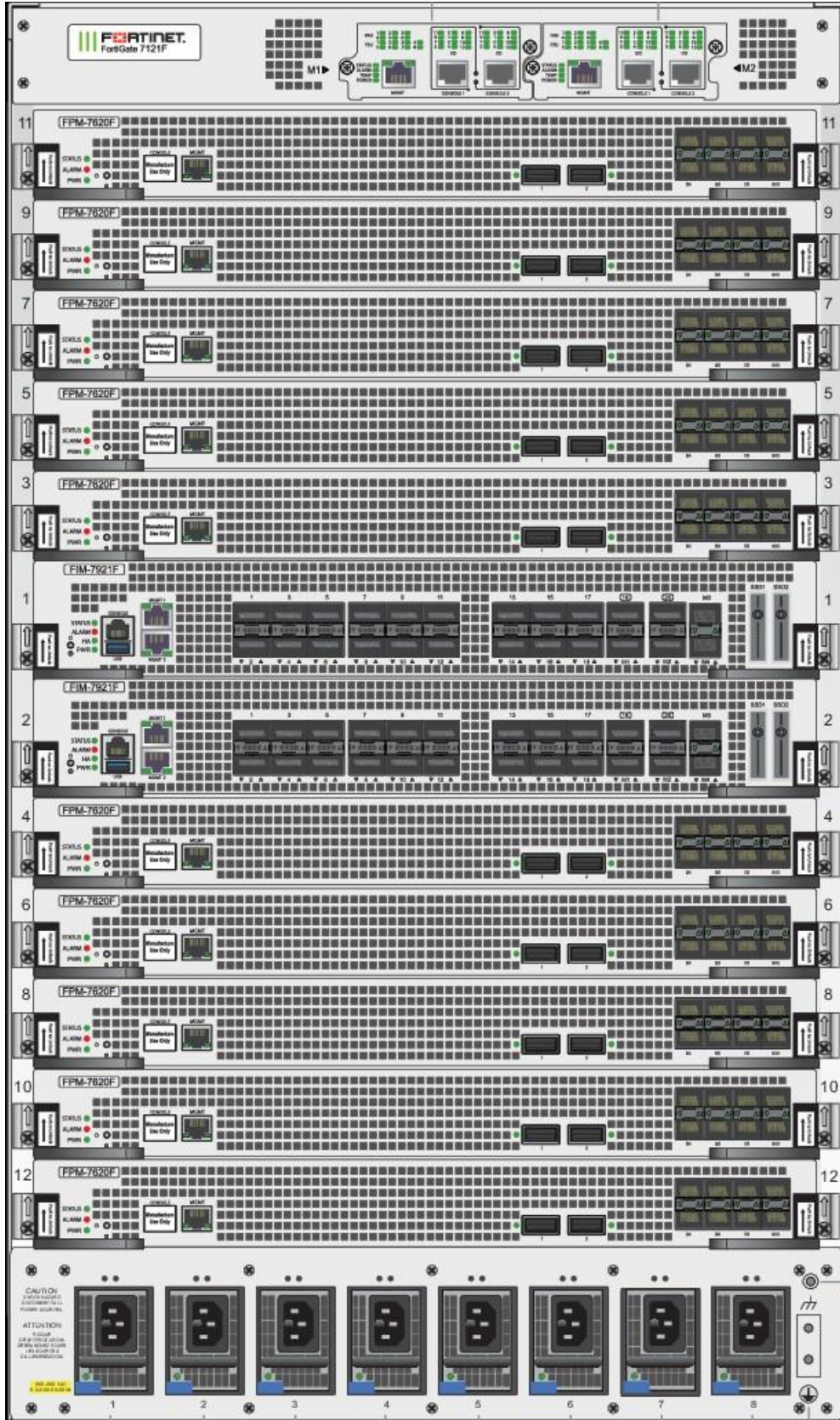


Figura 2: Appliance Hardware UTM

## - Appliance Software UTM

Están diseñados para instalarse sobre un equipo físico que por lo general es un servidor, en ese caso el “Appliance Software UTM” incluirá el sistema operativo. También existen “Appliance Software UTM” que solo son instaladores que necesitan un sistema operativo y también el equipo servidor. Su administración es por medio de un navegador web y por medio de una Shell para la administración y operaciones avanzadas por medio de comandos.

Fuente: Maggi, 2015

```
chroot: ntp done
chroot: openvpn done
chroot: pop3 done
chroot: ppp done
chroot: pppoe done
chroot: pptp done
chroot: pptpc done
chroot: quagga done
chroot: reverseproxy done
chroot: snmp done
chroot: snort done
chroot: socks done
chroot: xorp done
:: Loading CPUFreq modules (CPUFreq not supported)
:: Starting HAL daemon done
:: Starting haveged daemon done
unable to initialize libusb: -99
unable to initialize libusb: -99
:: Starting Configuration daemon done
:: Starting Confd request queuing daemon done
:: Starting Confd queue runner done
:: Starting Sysmon daemon done
:: Starting Console Support done
:: Starting Astaro User Authentication done
:: Backup restore skipped
:: Starting Postfix done
:: Starting Notification daemon done
:: Starting WebAdmin done
:: Starting rrdtool cache done
:: Starting Cron done
:: Starting service at daemon done
:: Starting PostgreSQL done
:: Starting ulogd done
:: Starting MiddleWare done
Master Resource Control: runlevel 3 has been reached
Skipped services in runlevel 3: initasg restore

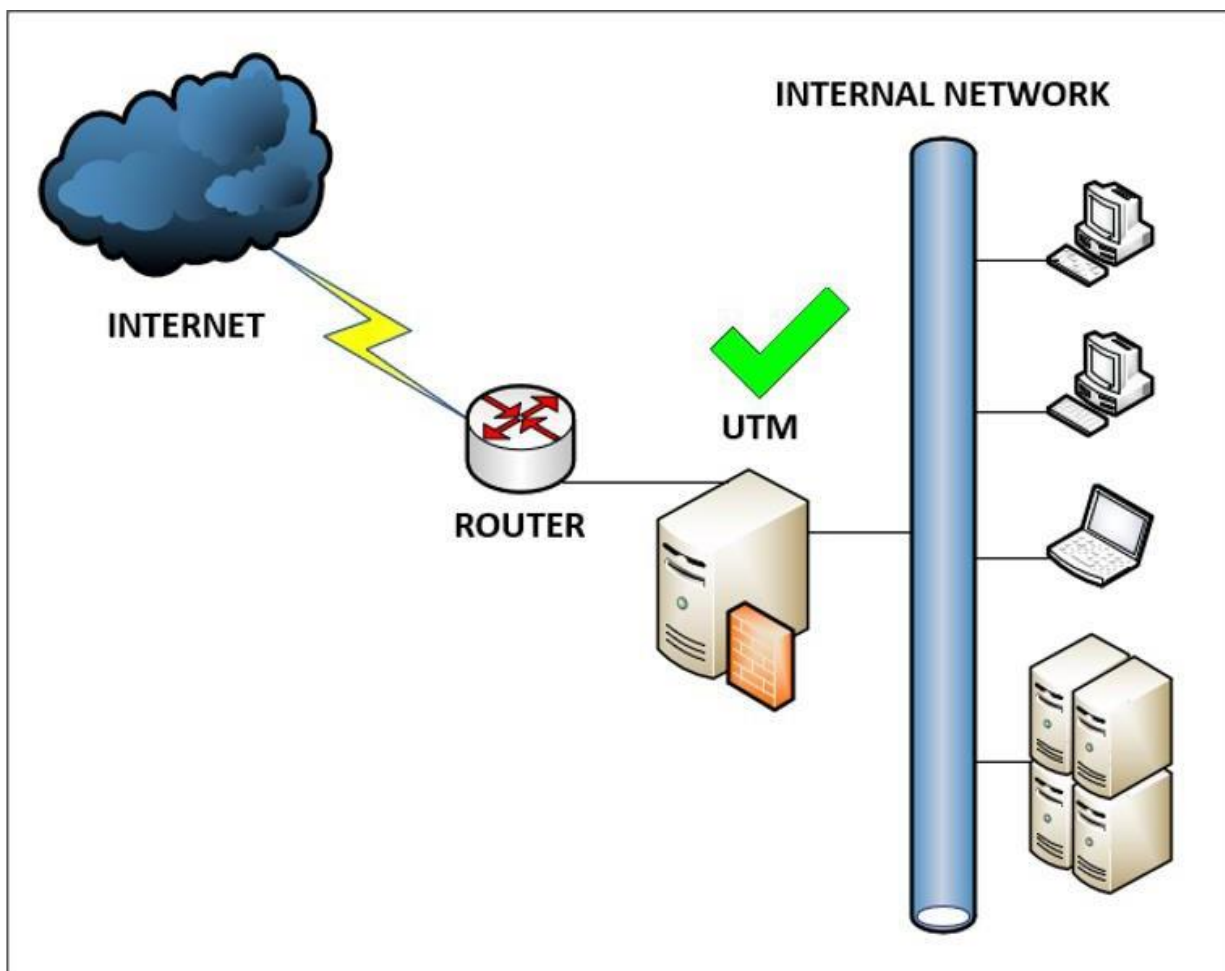
All configuration is done with WebAdmin. Go to https://10.211.55.100:4444
in your browser.

10.211.55.100
login: _
```

Figura 3: Appliance Software UTM

## Seguridad perimetral

Según Gómez (2014, p.29) Se enfocan en equipos o dispositivos que se encuentran entre la red interna y la ubicación donde se establece el tráfico con otras redes, de esa forma se controla y se administra la interconexión vigilando y analizando qué datos salen e ingresan desde el exterior para salvaguardar la integridad, disponibilidad y confidencialidad de la red interna que se desea asegurar, evitando, accesos no autorizados y todo tipo de ataques informáticos



Fuente: Elaboración propia

Figura 4: Seguridad perimetral



## COBIT 5

Según ISACA (2012, p13) COBIT 5 facilita un marco referencial e integral ayudando a los organismos y empresas a alcanzar sus objetivos en cuanto a la gobernanza y la gestión de TI, está orientado a la creación de valor desde las tecnologías de la información empresariales, manteniendo un equilibrio mediante la generación de beneficios, minimizando los riesgos y optimizando eficientemente los recursos. El marco de COBIT 5 es referencial, su aplicación puede ser transversal, y útil en organizaciones y el mundo empresarial sea cual sea su tamaño.

### Familia de productos de COBIT 5

Según ISACA (2012, p26) La familia de COBIT 5 parte desde su marco de trabajo que es la base. Además, brinda una serie de productos que son reconocidos como guías catalizadoras y guías profesionales, las cuales podemos visualizar en la siguiente imagen:

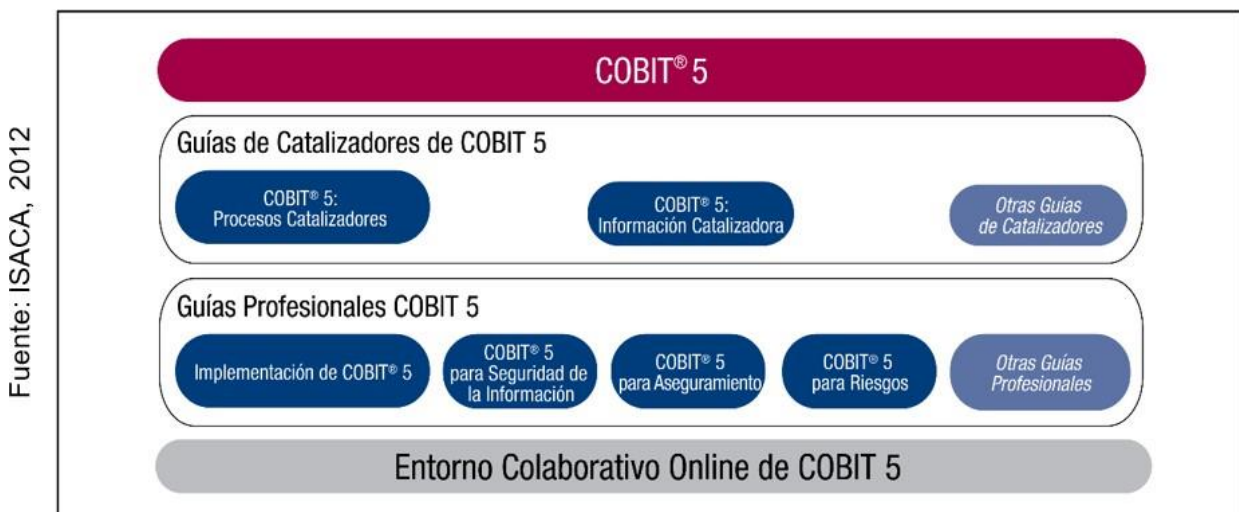


Figura 5: Familia de productos de COBIT 5

## **COBIT 5 para la seguridad de la información**

Según ISACA (2012, p16) “COBIT 5 para la seguridad de la información” es una guía profesional basado en el marco de trabajo de COBIT 5, se enfoca en la seguridad de la información y brinda un marco de trabajo muy detallado y práctico para los profesionales de la seguridad de la información como los directores de seguridad de la información (CISO), gerentes de seguridad de la información (ISM), oficiales de seguridad de la información, consultores de seguridad de la información y otros profesionales interesados.

En guía profesional de “COBIT 5 para la seguridad de la información” los procesos APO13 “*Gestionar la seguridad*”, DSS04 “*Gestionar la continuidad*”, y el proceso DSS05 “*Gestionar los servicios de seguridad*”, brindan una guía detallada basadas en prácticas de gestión y actividades específicas de seguridad, acerca de cómo definir, administrar y monitorizar un sistema para la gestión general de seguridad.

## **Modelo de referencia de Procesos de COBIT 5**

Según ISACA (2012, p33) En la práctica, las diferentes responsabilidades y roles del gobierno y gestión de la seguridad de la información se hacen visibles mediante el modelo de procesos del marco de referencia de COBIT 5.

Este marco nos presenta 5 dominios y 37 procesos que entre ellos podemos encontrar incluyen 32 procesos de gestión y 5 procesos de gobierno, cada grupo con sus propias responsabilidades, las cuales podemos encontrarlas descritas y de manera detallada en el libro de Procesos catalizadores de COBIT 5.



Fuente: ISACA, 2012

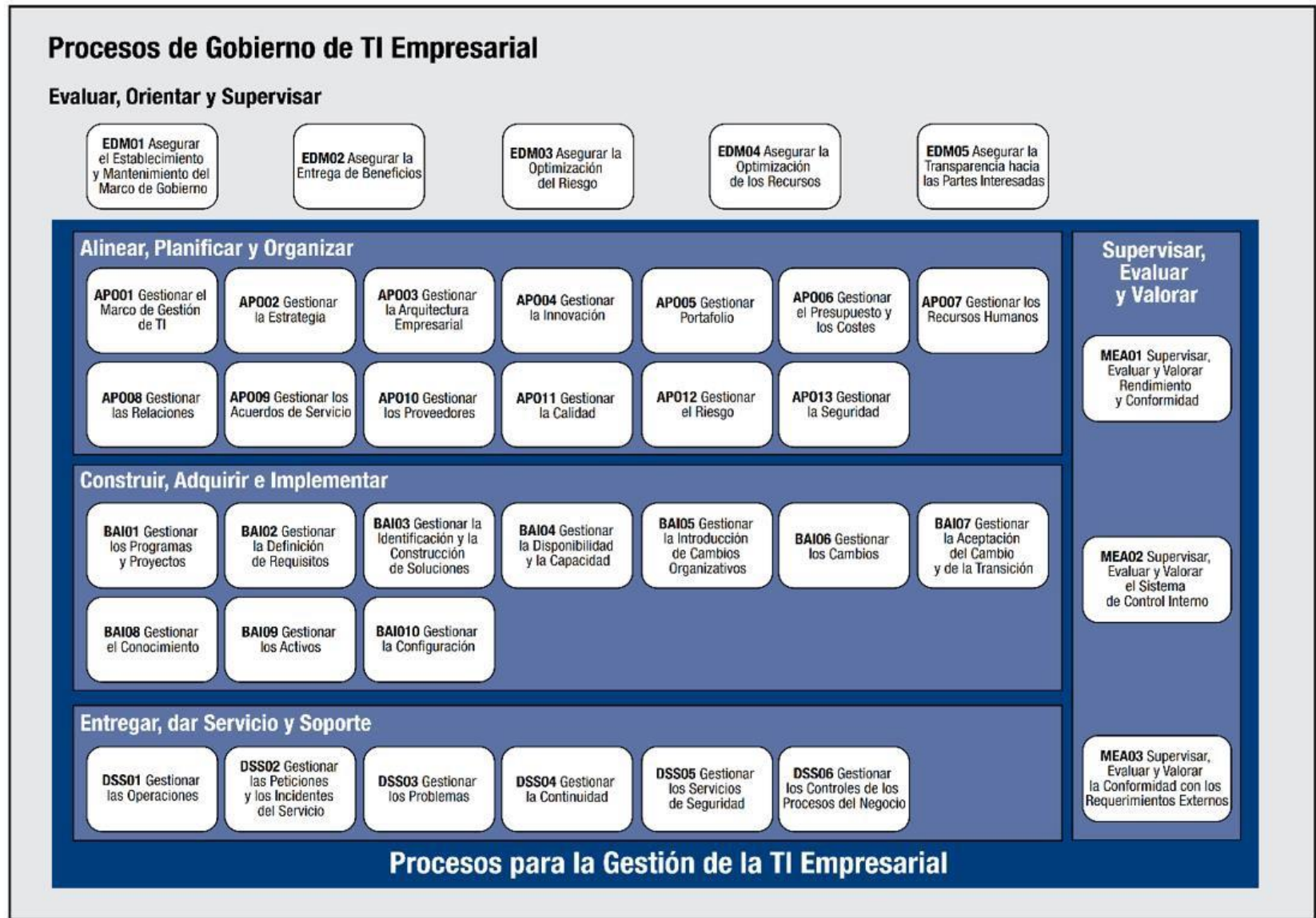


Figura 6: Modelo de referencia de procesos de COBIT 5

## Proceso DSS05: Gestión de Servicios de Seguridad

Según ISACA (2012, p191) La gestión de servicios de seguridad está asociado al proceso “DSS05 – Gestionar los servicios de seguridad” el cual manifiesta que es la intención de salvaguardar la información creada, gestionada y almacenada en la empresa y minimizar el nivel de riesgo de seguridad de la información conforme a las políticas de seguridad. Adicionalmente, recomienda instaurar y preservar los roles y privilegios de acceso, llevar a cabo la supervisión de la seguridad de manera integral en la organización.

### Métricas del Proceso DSS05

Según ISACA (2012, p191) El marco de referencia de COBIT 5 en el proceso “DSS05 Gestionar los servicios de seguridad” facilita métricas para realizar medir y recibir datos cuantitativos que le permita aterrizar sobre una realidad y sobre ella tomar acciones preventivas o correctoras.

Fuente: ISACA, 2012

Métricas
<ul style="list-style-type: none"><li>• Número de vulnerabilidades descubiertas</li><li>• Número de rupturas (<i>breaches</i>) de cortafuegos</li></ul>
<ul style="list-style-type: none"><li>• Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final</li><li>• Número de incidentes que impliquen dispositivos de usuario final</li><li>• Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno</li></ul>
<ul style="list-style-type: none"><li>• Promedio de tiempo entre los cambios y actualizaciones de cuentas</li><li>• Número de cuentas (con respecto al número de usuarios/empleados autorizados)</li></ul>
<ul style="list-style-type: none"><li>• Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno</li><li>• Clasificación media para las evaluaciones de seguridad física</li><li>• Número de incidentes relacionados con seguridad física</li></ul>
<ul style="list-style-type: none"><li>• Número de incidentes relacionados con accesos no autorizados a la información</li></ul>

Figura 7: Métricas del proceso DSS05

## Prácticas de gestión del Proceso DSS05

A continuación, presentamos la descripción de cada una de las siete prácticas de gestión que conforman el proceso “DSS05 – Gestionar los Servicios de Seguridad” del marco de referencia de COBIT 5. Este proceso se divide en siete “Prácticas de Gestión”, tal como se evidencia en la siguiente imagen:

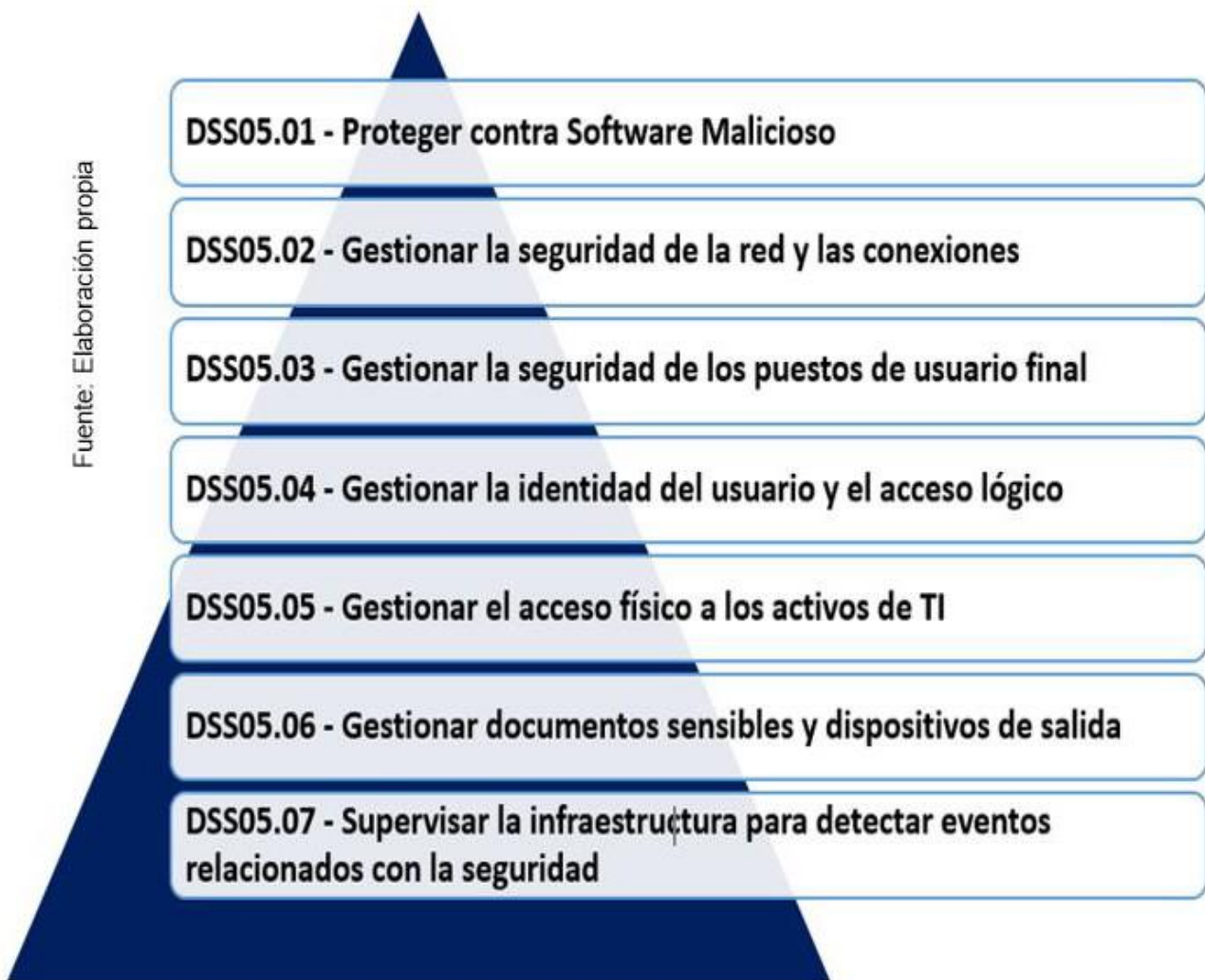


Figura 8: Prácticas de gestión del proceso DSS05 “Gestionar servicios de seguridad”

El proceso de gestión de DSS05 – Gestionar los servicios de seguridad se puede ver de manera integral en el anexo 7.

➤ **DSS05.01 – Proteger contra software malicioso**

Consiste en implementar y conservar efectivas operaciones preventivas, detectivas y correctivas en toda la compañía u organización para resguardar los sistemas de información de software mal intencionado.

➤ **DSS05.02 – Gestionar la seguridad de la red y las conexiones**

Esta práctica de control consiste en emplear medidas de seguridad y a la vez aplicar procedimientos de gestión para proteger y asegurar la información en todas las interconexiones o formas de conexión.

 **Indicador:**

Tomando en consideración COBIT 5, el indicador que me puede ayudar a medir que esta práctica de control se está realizando correctamente es:

- ✓ Número de vulnerabilidades descubiertas =  $\Sigma ((N^{\circ} \text{ de vulnerabilidades tecnológicas}) + (N^{\circ} \text{ de vulnerabilidades de configuración}) + (N^{\circ} \text{ de vulnerabilidades de política de seguridad}))$

➤ **DSS05.03 – Gestionar la seguridad de los puestos de usuario final**

Consiste en asegurar que las posiciones de los usuarios finales como los equipos portátiles, los equipos de sobremesa y otros dispositivos estén asegurados al nivel demandado o a mayor nivel del cual se tiene definido en las exigencias de seguridad de la información gestionada, resguardada o compartida.

### **Indicador:**

Tomando en consideración COBIT 5, el indicador que me puede ayudar a medir que esta práctica de control se está realizando correctamente es:

- ✓ Número de incidentes de dispositivos de usuario final =  $\Sigma * ((N^{\circ} \text{ de incidentes en Desktop}) + (N^{\circ} \text{ de incidentes en Laptop}) + (N^{\circ} \text{ de incidentes en Workstation}))$

#### ➤ **DSS05.04 – Gestionar la identidad del usuario y el acceso lógico**

Consiste en garantizar el acceso a la información a aquellos usuarios de acuerdo a los requerimientos que exija su labor en el negocio, a la vez de coordinar con los departamentos involucrados del negocio para que gestionen sus propias exigencias y derechos de acceso a los procesos del negocio.

#### ➤ **DSS05.05 – Gestionar el acceso físico a los activos de TI**

Consiste en realizar las definiciones e implementaciones para permitir, restringir o revocar el acceso a las oficinas, edificios o cualquier departamento o espacio laboral que forme parte del negocio, también se incluye espacios de emergencias. Todo acceso debe ser debidamente justificado, validado, anotado y vigilado. Todo lo mencionado se aplicará absolutamente a toda persona que pretenda ingresar a cualquier local del negocio, se incluye a los empleados.

➤ **DSS05.06 – Gestionar documentos sensibles y dispositivos de salida.**

Consiste en implantar medidas de contingencias físicas concientizadas, contables y gestionar bajo un inventario todos los activos de TI sensibles; dentro de ellos tenemos a las credenciales de seguridad como los “token”, documentos de negocio, impresoras de propósito y formularios especiales.

➤ **DSS05.07 – Supervisar la infraestructura para detectar eventos relacionados con la seguridad.**

Esta práctica de control recomienda hacer uso de herramientas para la detección de intrusiones, así como también realizar una supervisión constante a las áreas de infraestructura para prevenir acceso no autorizados; debemos asegurar que cualquier evento sea integrado con la herramienta general de eventos e incidentes.

## FOMULACIÓN DEL PROBLEMA

### 1.1.2. Problema General

**PG:** ¿De qué manera el Unified Threat Management (UTM) influye en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.?

### 1.1.3. Problemas Específicos

**PE1:** ¿De qué manera el Unified Threat Management (UTM) influye en el número de vulnerabilidades descubiertas en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.?

**PE2:** ¿De qué manera el Unified Threat Management (UTM) influye en el número de incidentes en dispositivos de usuario final en la gestión de servicios de seguridad de COBIT 5 en la empresa Rem Systems S.A.C.?

## JUSTIFICACIÓN DEL ESTUDIO

### 1.1.4. Justificación Institucional

La empresa Rem Systems S.A.C. reconociéndose como empresa privada, compite en el mercado peruano con muchas otras empresas que brindan los servicios de consultoría, proyectos y soluciones empresariales de TI. Por ello, al manejar información sensible y confidencial de sus clientes es de necesidad vital que sus tecnologías y sus redes informáticas se encuentren seguras y brinden esa imagen de confiabilidad y seguridad a sus clientes, a la sociedad y al estado peruano. Por esa razón, la realización de este proyecto contribuirá a mejorar la reputación e imagen

institucional de la empresa Rem Systems S.A.C., obteniendo ventajas competitivas en relación a confianza y seguridad ante otras empresas que brindan los mismos servicios.

#### **1.1.5. Justificación Tecnológica**

La empresa Rem Systems S.A.C. como empresa que brinda soluciones empresariales de tecnologías de la información, necesita garantizar a sus clientes los niveles más altos de seguridad, por esa razón, este proyecto se propone la implementación de un Unified Threat Management (UTM) basándose en casos de éxito de compañías y organizaciones nacionales e internacionales que aseguran que el uso de un Unified Threat Management (UTM) es la mejor opción para la protección de las redes a nivel de seguridad perimetral.

Por ello, concluimos indicando que la tecnología de Unified Threat Management (UTM) es posible implementarla en la empresa Rem Systems SAC porque en nuestro país se cuenta con el apoyo de los diversos “Partner” de tecnologías UTM que han tenido éxito al cubrir todas las necesidades de ciberseguridad en otras empresas y compañías en diversos contextos y rubros de negocio.

#### **1.1.6. Justificación Económica**

Para la empresa Rem Systems S.A.C. todos sus activos tecnológicos (computadores, redes, servidores, servicios, sistemas de información, etc.) y la información como activo más importante, son factores clave para la continuidad del negocio, por ello, mantenerlos seguros es una necesidad que, al no llegar a tomar conciencia sobre su gran importancia, podría ocasionar pérdidas económicas incalculables que podría comprometer su permanencia en el mercado u ocasionar su cierre definitivo.



Implementar un Unified Threat Management (UTM) beneficiará reduciendo horas de trabajo del departamento de TI en la administración de las aplicaciones básicas de seguridad, adicionalmente agilizará el trabajo de todos los colaboradores de la empresa porque diariamente llaman al departamento de TI por alguna razón referente a spam, virus y malware.

Finalmente, la implementación de un Unified Threat Management (UTM) beneficiará creando valor a la empresa minimizando el riesgo de sufrir ciber-ataques que podrían tener gastos de recuperación incalculables en montos de dinero, y sumado a ello la terminación de contratos por parte de los clientes originando crisis en los ingresos económicos en la empresa, y mala reputación en el mercado.

## **1.2. HIPÓTESIS**

### **1.2.1. Hipótesis General**

**HG:** El Unified Threat Management (UTM) influye significativamente en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

### **1.2.2. Hipótesis Específicos**

**H1:** El Unified Threat Management (UTM) reduce el número de vulnerabilidades descubiertas en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

**H2:** El Unified Threat Management (UTM) reduce el número de incidentes en dispositivos de usuario final en la gestión de servicios de seguridad basado en COBIT 5 en la empresa REM Systems S.A.C.

### **1.3. OBJETIVOS**

#### **1.3.1. Objetivo General**

Determinar la influencia del Unified Threat Management (UTM) en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

#### **1.3.2. Objetivos Específicos**

- Determinar la influencia del Unified Threat Management (UTM) en el número de vulnerabilidades descubiertas en la gestión de servicios de seguridad basado en COBIT 5 en la empresa REM Systems S.A.C.
- Determinar la influencia del Unified Threat Management (UTM) en el número de incidentes en dispositivos de usuario final en la gestión de servicios de seguridad basado en COBIT 5 en la empresa REM Systems SAC.

### III. METODOLOGÍA

#### Diseño de investigación

##### 3.1 Tipo y diseño de investigación: Cuantitativo

Según Hernández, Fernández y Baptista (2014, p.129) Existe una relación directa de la calidad de la investigación en medida en que pongamos en aplicación el diseño, en base a lo argumentado es importante que el diseño se ajuste en vista a posibles contingencias o si en caso la situación cambia. Aplicar el diseño es importante para el análisis de la certeza de las hipótesis que son formuladas bajo el contexto de la problemática.

##### **Diseño de Investigación: Experimental**

Según Hernández, Fernández y Baptista (2014, p.129) Nos manifiesta en relación a la investigación de tipo experimental se refiere a un estudio que de manera intencional se van a manipular desde una a muchas variables independientes para realizar un análisis sobre las consecuencias que el tratamiento ha tenido sobre una o más variables dependientes.

##### **Tipo de Diseño de Investigación: Pre-Experimental**

Según Hernández, Fernández y Baptista (2014, p.141) Se debe aplicar una evaluación al grupo de investigación antes de aplicar un estímulo o tratamiento experimental, luego, realizar una nueva evaluación y comparar con la primera, por ello se habla de un Pre-test y Post-test.

G:            Y1    →    X        →    Y2

Donde:

G            : Grupo.

X            : Tratamiento o estímulo experimental.

Y1, Y2      : Medición de actores de un grupo (pre y post prueba)

## 3.2 Variables y operacionalización

### Definición conceptual de variables

La presente investigación de tesis cuenta con dos variables y las mencionaremos a continuación:

- **Variable Independiente:** Unified Threat Management (UTM)

Según Barrett, Weiss y Hausman (2015, p.171) Las tecnologías basadas en Unified Threat Management (UTM) integran una variedad de servicios y módulos de seguridad que comúnmente se encontraban en equipos o dispositivos separados.

- **Variable Dependiente:** Gestión de servicios de Seguridad

Según ISACA (2012, p191) La gestión de servicios de seguridad está asociado al proceso “DSS05 – Gestionar los servicios de seguridad” Cuya finalidad es minimizar el impacto en el negocio a consecuencia de las vulnerabilidades e incidentes operativos de seguridad de la información

### Definición Operacional

- **Gestión de servicios de Seguridad**

La gestión de servicios de seguridad consiste en actividades de monitoreo de manera permanente de la infraestructura tecnológica de la organización con la finalidad de evitar y de detectar intrusiones no autorizadas y software malicioso identificado por del departamento de TI o reportadas por parte de las áreas usuarias.

## 2.1.2. Operacionalización de variables

Fuente: Elaboración propia

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADOR	ESCALA DE MEDICIÓN
<b>VI:</b> Unified Threat Management (UTM)	Según Barrett, Weiss y Hausman (2015, p.171) Las tecnologías basadas en Unified Threat Management (UTM) integran una variedad de servicios y módulos de seguridad que comúnmente se encontraban en equipos o dispositivos separados.				
<b>VD:</b> Gestión de servicios de Seguridad	Según ISACA (2012, p191) La gestión de servicios de seguridad está asociado al proceso “DSS05 – Gestionar los servicios de seguridad” cuya finalidad es minimizar el impacto en el negocio a consecuencia de las vulnerabilidades e incidentes operativos de seguridad en la información.	La gestión de servicios de seguridad consiste en actividades de monitoreo de manera permanente de la infraestructura tecnológica de la organización con la finalidad de evitar y de detectar intrusiones no autorizadas y software malicioso identificado por del departamento de TI o reportadas por parte de las áreas usuarias.	Gestión de servicios de Seguridad	Número de vulnerabilidades descubiertas	Razón
				Número de incidentes en dispositivos de usuario final	Razón

Tabla 1: Operacionalización de variables

## Indicadores de Variable Dependiente “Gestión de servicios de Seguridad”

Fuente: Elaboración propia

INDICADOR	DESCRIPCIÓN	TÉCNICA	INSTRUMENTO	UNIDAD DE MEDIDA	FÓRMULA
<b>Número de vulnerabilidades descubiertas</b>	Este indicador tiene por objeto evidenciar y calcular todas las vulnerabilidades o rupturas que se presentan en un día.	Fichaje	Ficha de registro	Razón	$\text{NVD} = \text{NVT} + \text{NVC} + \text{NVS}$ <p><b>Donde:</b>  <b>NVD:</b> Número de vulnerabilidades descubiertas  <b>NVT:</b> Número de vulnerabilidades tecnológicas  <b>NVC:</b> Número de vulnerabilidades de configuración  <b>NVS:</b> Número de vulnerabilidades de política de seguridad</p>
<b>Número de incidentes en dispositivos de usuario final</b>	Este indicador tiene por objeto evidenciar todos los incidentes que se han presentado en los equipos (PC, laptops, etc.) que utilizan los colaboradores en un día.	Fichaje	Ficha de registro	Razón	$\text{NIF} = \text{DSK} + \text{LAP} + \text{WRK}$ <p><b>Donde:</b>  <b>NIF:</b> Número de incidentes en dispositivos de usuarios final  <b>DSK:</b> Desktops  <b>LAP:</b> Laptops  <b>WRK:</b> Workstation</p>

Tabla 2: Indicadores de la variable dependiente

### **3.3 Población, Muestra y Muestreo**

#### **Población:**

Según Hernández, Fernández y Baptista (2014, p. 174) manifiestan que al momento en que se ha definido cuál será la unidad de muestreo o análisis, se procede a delimitar que va ser estudiada y sobre la cual se pretende generalizar los resultados. Por ello, una población es considerado el conjunto de todos los casos que concuerdan con una serie de especificaciones.

La presente investigación de tesis se identifican dos poblaciones que son las que mencionaremos a continuación:

#### **❖ Población N° 1:**

La población para el cálculo del indicador “número de vulnerabilidades descubiertas” está determinada por el número de vulnerabilidades registradas en 2 fichas de reporte.

#### **❖ Población N° 2:**

La población para el cálculo del indicador “número de incidentes en dispositivos de usuario final” está determinada por el número de vulnerabilidades registradas en 2 fichas de reporte.

#### **Muestra:**

Según Castro (2003, p.69) Manifiesta que si en caso la población obtenida es menos a cincuenta (50) individuos, la población será igual a la muestra.

Para esta investigación la muestra será igual a la población, se va a tomar el total del número de la “población N° 1” y la “población N° 2” que se han mencionado anteriormente, por consiguiente, la muestra es igual a la población.

### **3.4 Técnicas e instrumentos de recolección de datos**

#### **Técnica: Fichaje**

Según Mingrone, (2007, p.73) Manifiesta que el “Fichaje” en la investigación científica es válida y es utilizada como una técnica de tipo auxiliar; su aplicación consta en el registro de todo lo que se obtiene de los instrumentos denominados fichas de registro, estas contienen información relevante que es recopilada para una investigación.

Tomando en consideración lo indicado por el autor en la presente investigación para la recopilación de los datos relacionados en los indicadores “número promedio diario de vulnerabilidades descubiertas” y “número promedio diario de incidentes de dispositivos de usuario final” se utilizará la técnica del fichaje.

#### **Instrumento: Ficha de registro**

Según Sendra (2010. p.118) la ficha de registro hace posible llevar los datos consultados de manera ordenada y clasificada, su finalidad es evidenciar de manera cuantitativa las ocasiones que un fenómeno o un hecho ha sucedido.

- ✓ Ficha de Registro 1: Número de vulnerabilidades descubiertas. [\(ver anexo 6\)](#)
  
- ✓ Ficha de Registro 2: Número de incidentes en dispositivos de usuario final. [\(ver anexo 6\)](#)



### 3.5 Procedimientos

➤ **Validez:**

Según Hernández, Fernández y Baptista (2014, p. 200) Al referirnos a la validez es cuando hacemos referencia a la confiabilidad de un instrumento, en base a ello podremos tener la confianza en que realmente mide lo que necesitamos o busca medir. Las fichas de registro elaboradas para la presente investigación han sido validadas basándonos en el criterio de tres expertos como se evidencia en la “tabla 3”:

N°	Expertos	Grado Académico	Puntaje	
			Indicador 1	Indicador 2
			“Número de vulnerabilidades descubiertas”	“Número de incidentes en dispositivos de usuario final”
1	Bermejo Terrones, Henry Paúl	Magister	93%	93%
2	Roberto Roy Saavedra	Magister	85%	85%
3	Sinti Zárate, July Tatiana	Magister	87%	88%
TOTAL			88.33%	88.66%

Tabla 3: Validez de las fichas de registro

Una vez obtenido la validación realizada por los tres expertos se ha obtenido en el caso del “indicador 1” un valor promedio de “88.33%”; y en el caso del “indicador 2” un valor promedio de “88.66”. Demostrando la validez de los instrumentos.

➤ **Confiabilidad:**

Según Hernández, Fernández y Baptista (2014, p. 200) Cuando hablamos de que un instrumento de medición nos brinda confiabilidad nos hace referencia que si al ponerla en práctica reiteradas veces sobre la misma población nos va producir iguales resultados.

○ **Método: Pre-Test – Re-Rest**

Según Hernández, Fernández y Baptista (2014, p. 208) Este método consiste en aplicar de manera reiterativa la misma prueba para verificar la confiabilidad y estabilidad de un instrumento.

○ **Técnica: Coeficiente de correlación de Pearson**

Según Hernández, Fernández y Baptista (2014, p. 304) Es la covarianza estandarizada, lo que describe una prueba de tipo estadística que nos va a permitir el análisis de la relación de dos variables medidos en un nivel por intervalos o por razón. Para realizar el cálculo debemos tener resultados cuantificables que han sido obtenidos como muestras de las dos variables. Veamos la siguiente figura:

Fuente: Elaboración propia

Población:  $\rho_{xy} = \frac{\sigma_{xy}}{\sigma_x \cdot \sigma_y}$

Muestra:  $r_{xy} = \frac{S_{xy}}{S_x \cdot S_y}$

**p<sub>xy</sub> = Coeficiente de correlación de Pearson de la Población.**

**r<sub>xy</sub> = Coeficiente de correlación de Pearson de la Muestra.**

**$\sigma_{xy} = S_{xy}$  = Covarianza de x e y.**

**$\sigma_x = S_x$  = Desviación típica de la variable x.**

**$\sigma_y = S_y$  = Desviación típica de la variable y.**

Figura 9: Coeficiente de correlación de Pearson

Una vez obtenido el coeficiente de correlación de Pearson de acuerdo a la fórmula anterior, tiene que interpretado de acuerdo a los datos indicados en la Tabla 4:

Fuente: Elaboración propia

<b>Coeficiente</b>	<b>Interpretación</b>
+1.00	Correlación Positiva Perfecta
+0.90 hasta +0.99	Correlación Positiva Muy Alta
+0.70 hasta +0.89	Correlación Positiva Alta
+0.40 hasta +0.69	Correlación Positiva Media
+0.20 hasta +0.39	Correlación Positiva Baja
+0.01 hasta +0.19	Correlación Positiva Muy Baja
0	No existe Correlación
-0.01 hasta -0.19	Correlación Negativa Muy Baja
-0.20 hasta -0.39	Correlación Negativa Baja
-0.40 hasta -0.69	Correlación Negativa Media
-0.70 hasta -0.89	Correlación Negativa Alta
-0.90 hasta -0.99	Correlación Negativa Muy Alta
-1.00	Correlación Negativa Perfecta

Tabla 4: Grados de correlación de Pearson

Según Hernández, Fernández y Baptista (2014, p. 304) El coeficiente de relación de Pearson para su interpretación puede variar de -1.00 a +1.00, donde: -1.00 es la correlación negativa perfecta, el instrumento que evaluado no es confiable; y +1.00 es una correlación positiva perfecta, entonces se trata de un instrumento confiable que hace mediciones estables y consistentes. Un valor próximo a 0 indica ausencia o no existe correlación alguna entre las variables. A continuación, se presentan los valores calculados bajo el coeficiente de correlación de Pearson para el “indicador 1” e “Indicador 2”

Fuente: Elaboración propia

CORRELACIONES		NVD_PRE-TEST: NOV_(02-15)_2020	NVD_RE-TEST: DIC_(07-20)_2020
NVD_PRE-TEST: NOV_(02-15)_2020	Correlación de Pearson	1	.794**
	Sig. (bilateral)		<.001
	N	14	14
NVD_RE-TEST: DIC_(07-20)_2020	Correlación de Pearson	.794**	1
	Sig. (bilateral)	<.001	
	N	14	14

Tabla 5: SPSS – Número de vulnerabilidades descubiertas (NVD)

Según la tabla 5 el valor de la confiabilidad para el indicador “Número de vulnerabilidades descubiertas” dio el valor de: 0.794, concluimos, el nivel de confiabilidad del instrumento usado para medir este indicador es “Alta”.

Fuente: Elaboración propia

CORRELACIONES		NIF_PRE-TEST: NOV_(02-15)_2020	NIF_RE-TEST: DIC_(07-20)_2020
NVD_PRE-TEST: NOV_(02-15)_2020	Correlación de Pearson	1	.735**
	Sig. (bilateral)		.003
	N	14	14
NVD_RE-TEST: DIC_(07-20)_2020	Correlación de Pearson	.735**	1
	Sig. (bilateral)	.003	
	N	14	14

Tabla 6: SPSS - Número de incidentes en dispositivos de usuario final (NIF)

Según la tabla 6 el valor de la confiabilidad para el indicador “Número de incidentes en dispositivos de usuario final” fue de 0.735, concluimos, el nivel de confiabilidad del instrumento que se usó para medir este indicador es “Alta”.

### **3.6 Métodos de análisis de datos**

En la investigación se realizó en base a un análisis cuantitativo, ya que se enfocó en cuantificar la recopilación de datos de forma numérica, utilizando formulas, matrices y estadísticas para la representación y el análisis de datos para posteriormente obtener resultados medibles y cuantificables.

#### **Hipótesis Estadísticas**

Están conformadas por Nulas y Alternativas.

##### **A. Hipótesis Nula:**

Según Hernández, Fernández y Baptista (2010, p. 104) Las hipótesis nulas se muestran como inversa y contrapartida de las hipótesis planteadas en una investigación, todo ello constituye proposiciones sobre la relación entre las variables para refutar o negar lo que afirma la hipótesis de la investigación.

##### **B. Hipótesis Alternativa:**

Según Hernández, Fernández y Baptista (2010, p. 105) Las hipótesis alternativas son posibilidades diferentes ante la hipótesis nula y la hipótesis de la investigación, proporcionan otra explicación, concepto o resultante. Las Hipótesis nulas se simbolizan con "H<sub>0</sub>", y se formulan cuando existen otras posibilidades, no deben establecerse si no existen otras posibilidades.

En esta investigación se plantearon las siguientes Hipótesis:

## **Indicador 1: “Número de vulnerabilidades descubiertas”**

### **a. Hipótesis Específica 1 (HE1)**

El Unified Threat Management (UTM) reduce el número de vulnerabilidades descubiertas en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

### **b. Representación de las variables 1**

**la1:** Número de vulnerabilidades descubiertas antes el “Unified Threat Management (UTM)” en la gestión de los servicios de seguridad.

**lp1:** Número de vulnerabilidades descubiertas después el “Unified Threat Management (UTM)” en la gestión de los servicios de seguridad.

### **c. Hipótesis estadística 1**

- **Hipótesis Nula (HN01):** El Unified Threat Management (UTM) no reduce el número de vulnerabilidades descubiertas en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

$$\mathbf{HN01: la1 < lp1}$$

Se deduce que no hubo reducción del “indicador 01” al implementar el “Unified Threat Management (UTM)”.

- **Hipótesis Alternativa (HA01):** El Unified Threat Management (UTM) reduce el número de vulnerabilidades descubiertas en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

### **HA01: Ia1 > Ip1**

Se deduce que el indicador mejoró al implementar el “Unified Threat Management (UTM)”.

### **Indicador 2: “Número de incidentes en dispositivos de usuario final”**

#### **a) Hipótesis Específica 2 (HE2)**

El Unified Threat Management (UTM) reduce el número de incidentes que impliquen dispositivos de usuario final en la gestión de servicios de seguridad basado en COBIT 5 en la empresa REM Systems S.A.C.

#### **b) Representación de las variables 2**

**Ia2:** Número de incidentes que impliquen dispositivos de usuario final antes el “Unified Threat Management (UTM)” en la gestión de los servicios de seguridad

**Ip2:** Número de incidentes que impliquen dispositivos de usuario final después el “Unified Threat Management (UTM)” en la gestión de los servicios de seguridad

### c) Hipótesis estadística 2

- **Hipótesis Nula (HN02):** El Unified Threat Management (UTM) no reduce el número de incidentes que impliquen dispositivos de usuario final en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

$$\text{HN01: } I_{a1} < I_{p1}$$

Se deduce que no hubo reducción del “indicador 01” al implementar el “Unified Threat Management (UTM)”.

- **Hipótesis Alternativa (HA02):** El Unified Threat Management (UTM) reduce el número de incidentes que impliquen dispositivos de usuario final en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

$$\text{HA01: } I_{a1} > I_{p1}$$

Se deduce que el indicador mejoró al implementar el “Unified Threat Management (UTM)”.

### Nivel de significancia

Según Moncada Jiménez (2005, p. 9) Un rol muy importante en las evaluaciones de las hipótesis es el nivel de significancia, porque establece cual será el grado de error que se está dispuesto a aceptar por parte del investigador; el nivel de significancia es referido a una pequeña parte de las colas de una distribución muestral; si el valor que se está buscando se encuentra en dicha zona se concluye que el evento no concluirá al azar y se rechaza la hipótesis nula y por consecuencia se acepta la hipótesis alternativa.



Al nivel de significancia se le denomina ( $\alpha$ ). Valores  $\alpha = 0.05$  o 5%; significa que 95 de cada 100 veces, el valor que se obtenga reflejará el valor verdadero de la población, y que 5 veces de 100 no lo reflejará (habrá error).

En este proyecto de investigación se ha utilizado: ( $\alpha$ ): 0.05

Para Vivanco (2005, p.60) El nivel de confianza o también reconocido por algunos investigadores como confiabilidad, en la estimación se presenta como complementario a la probabilidad de error en la estimación:

$$1-\alpha = 0.95 = 95\%$$

Gráficamente lo podemos expresar tal cual muestra la figura N° 9:

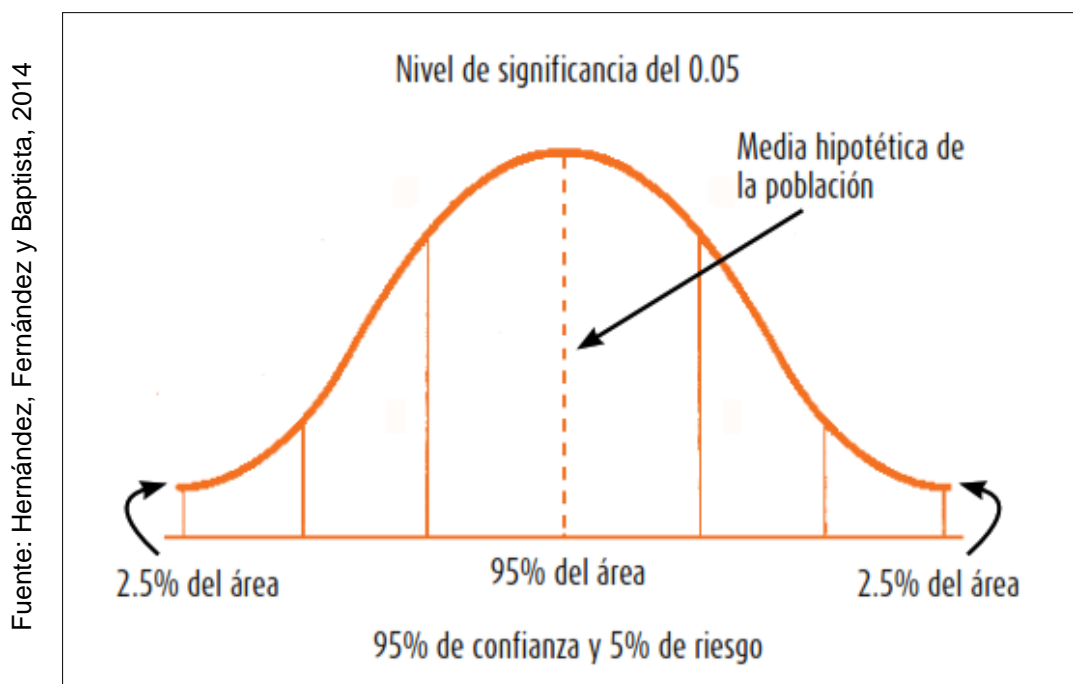


Figura 10: Nivel de significancia y confiabilidad

### **3.7 Aspectos éticos**

- ❖ Para el desarrollo del presente trabajo de investigación se ha seguido todos los lineamientos otorgados por la universidad, añadiendo que se han cumplido con todas las condiciones y criterios para realizar la investigación de la forma correcta con un diseño experimental.
  
- ❖ Se ha respetado a todos los autores de todas las teorías utilizadas en relación al tema de este trabajo de investigación, en la parte de bibliografía encontraremos los nombres de los autores y sus obras.
  
- ❖ Además, se ha contado con el apoyo de tres expertos que realizaron las validaciones de los instrumentos de medición que se han utilizado en el desarrollo de esta investigación.
  
- ❖ En referencia a la información utilizada de la empresa REM Systems S.A.C ha sido únicamente con fines académicos y se ha respetado la confidencialidad, y el código de ética. Todo ello con la finalidad de realizar el proyecto de investigación para el presente programa de titulación en ingeniería de sistemas. Se resalta que cualquier uso inapropiado del presente trabajo es rechazado y no aprobado por el investigador y la empresa.

## IV. RESULTADOS

### 3.1. Análisis descriptivo

En la presente investigación se implementó un “Unified Threat Management (UTM)” para reducir el número de vulnerabilidades descubiertas y el número de incidentes en dispositivos de usuario final. Por ello, se ha realizado un Pre-Test que nos ha permitido conocer las condiciones iniciales de los indicadores, luego se realizó un Re-Test donde corroboramos las condiciones en la que se encuentran los indicadores. Luego, se ha realizado la implementación del “Unified Threat Management (UTM)” y nuevamente se volvió a registrar el número de vulnerabilidades descubiertas y el número de incidentes en dispositivos de usuario final. Los resultados tras la evaluación del Post-Test se muestran en la siguiente tabla 7 y 8.

#### ▪ INDICADOR: Número de vulnerabilidades descubiertas

Los resultados descriptivos del número de vulnerabilidades descubiertas se pueden ver en la tabla 7:

Fuente: Elaboración propia

	N	Mínimo	Máximo	Media	Desv. Estándar
El_PreTest	14	43	114	83,14	19,09
El_PostTest	14	0,00	6,00	1,29	1,85
N válido (según lista)	14				

Tabla 7: Medidas descriptivas del indicador “número de vulnerabilidades descubiertas” antes y después de la implementación del “Unified Threat Management (UTM)”

En el caso del indicador “número de vulnerabilidades descubiertas”, al momento de realizar el Pre-Test se ha obtenido un valor de: 83.14 vulnerabilidades; y luego del Post-Test las vulnerabilidades han descendido de manera importante a valores de: 1.29. Estos resultados indican una gran diferencia entre el antes y el después de la implementación del “Unified Threat Management (UTM)”. De igual forma el número de vulnerabilidades como mínimo ha sido de: 43 vulnerabilidades antes, y después de la implementación del “Unified Threat Management (UTM)” ha sido de: 0.00; así mismo, el número de vulnerabilidades como máximo ha sido de: 114 vulnerabilidades antes, y después de la implementación del “Unified Threat Management (UTM)” ha sido de: 6.00 vulnerabilidades. Finalmente, en cuanto a la desviación estándar (dispersión) del indicador “número de vulnerabilidades descubiertas”, en el Pre-Test se tuvo variabilidad de: 19.09, y en el Post-Test se ha tenido un valor de: 1.85.

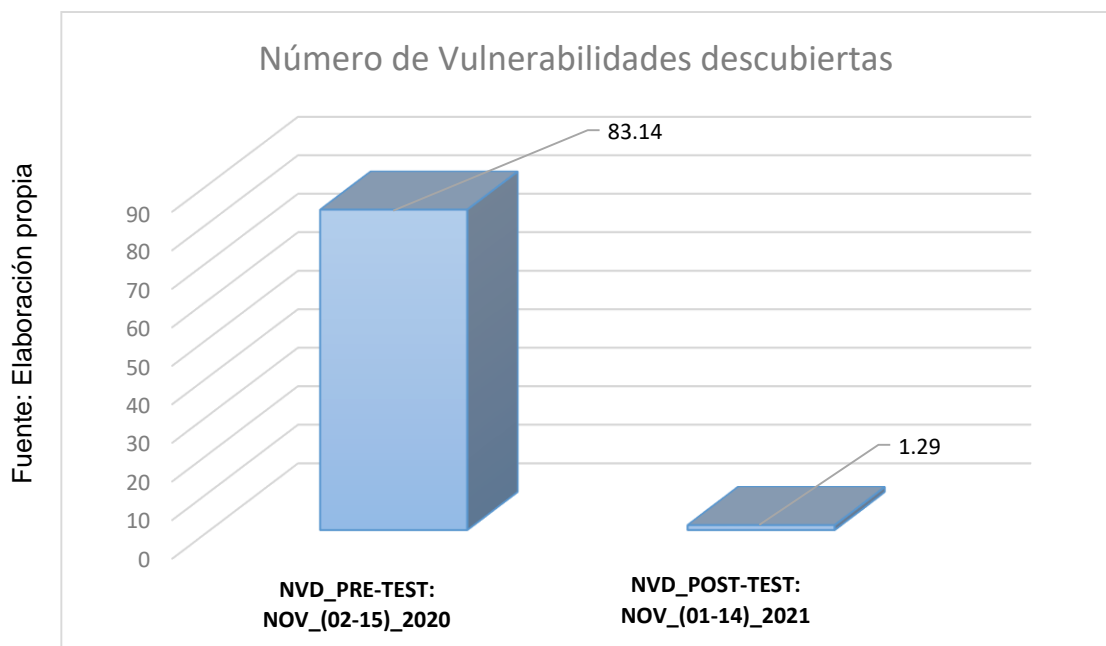


Figura 11: Número de vulnerabilidades descubiertas antes y después de implementar el “Unified Threat Management (UTM)”

▪ **INDICADOR: Número de incidentes en dispositivos de usuario final**

Los resultados descriptivos del número de vulnerabilidades descubiertas se pueden ver en la tabla 8:

	<b>N</b>	<b>Mínimo</b>	<b>Máximo</b>	<b>Media</b>	<b>Desv. Estándar</b>
El_PreTest	14	140	301	252,86	46,68
El_PostTest	14	0,00	9,00	3,86	2,79
N válido (según lista)	14				

Tabla 8: Medidas descriptivas del indicador “número de incidentes en dispositivos de usuario final” antes y después de la implementación del “Unified Threat Management (UTM)”

En el caso del indicador “número de incidentes en dispositivos de usuario final”, al momento de realizar el Pre-Test se ha obtenido un valor de: 252.86 de incidentes en dispositivos de usuario final; y luego del Post-Test los incidentes en dispositivos de usuario final han descendido de manera importante arrojando valores de: 3.86; estos resultados indican una gran diferencia entre el antes y el después de la implementación del “Unified Threat Management (UTM)”. De igual forma, los incidentes en dispositivos de usuario final como mínimo han sido de: 140, y después de la implementación del “Unified Threat Management (UTM)” ha sido de: 0.00; así mismo, los incidentes en dispositivos de usuario final como máximo ha sido de: 301 incidentes, y después de la implementación del “Unified Threat Management (UTM)” ha sido de: 9.00 incidentes en dispositivos de usuario final. Para concluir, en cuanto a la desviación estándar (dispersión) del indicador “Número de incidentes en dispositivos de usuario final”, en el Pre-Test se tuvo variabilidad de: 46,68, sin embargo, en el Post-Test se ha tenido un valor de: 2,79.

Fuente: Elaboración propia

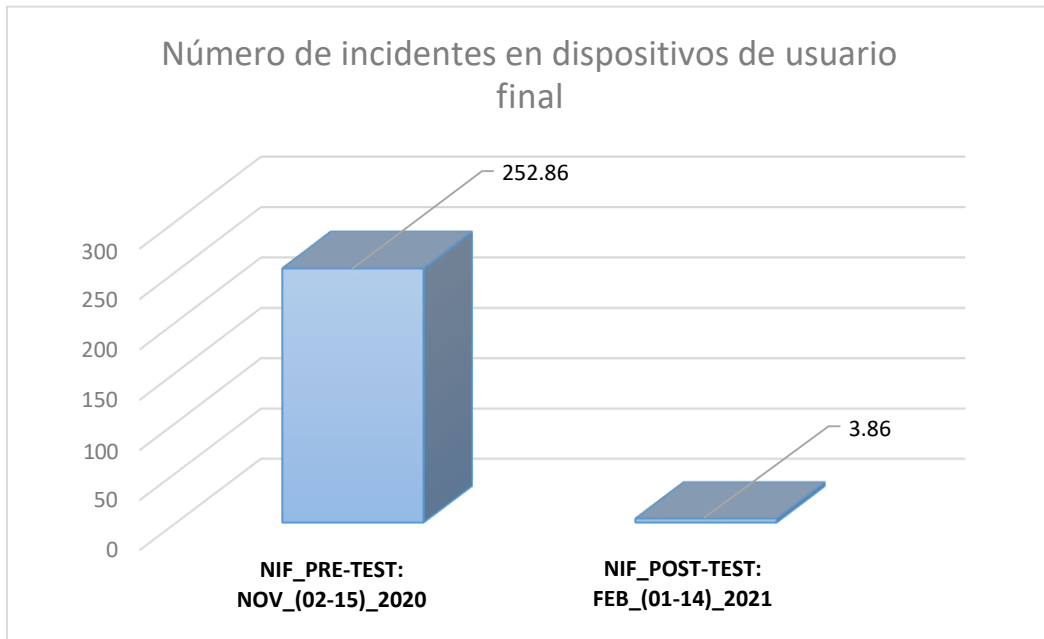


Figura 12: Número de incidentes en dispositivos de usuario final antes y después de implementar el “Unified Threat Management (UTM)”

### 3.2. Análisis inferencial

#### 3.2.1. Pruebas de normalidad

Risk (2003, p.19) señala que es vital y fundamental en la estadística cerciorarnos en la normalidad de todas nuestras muestras de estudio, ya que si las muestras resultan normales podrían aplicarse métodos estadísticos paramétricos convencionales, y si el caso es contrario los datos deben transformarse para hacer uso de otros métodos estadísticos.

Bernal Morell (2014, p.18) Manifiesta que para hacer la comprobación de un grupo de datos considerados de una distribución normal los gráficos de probabilidad lo garantizarán. Existen dos tipos de pruebas:

- ✓ **Prueba de Kolmogorov-Smirov:** Es utilizado cuando existen más de 50 unidades para el análisis.
- ✓ **Prueba de Shapiro-Wilk** Es utilizado cuando existen menos de 50 unidades para el análisis

El tamaño de la muestra del indicador “número de vulnerabilidades descubiertas” es de 14 registros, y para el indicador “número de incidentes en dispositivos de usuario final” es de 14 registros, por lo tanto, se utilizará para ambos casos el método de Shapiro-Wik.

Todas las pruebas se realizaron ingresando todos los datos de cada indicador en el Software IBM SPSS 20.0 Statistics, para un nivel de confiabilidad del 95% según las siguientes condiciones:

Si:

Sig. < 0.05: Adopta una distribución no normal

Sig. > 0.05: Adopta una distribución normal

Donde:

Sig. : p-valor o nivel crítico del contraste

❖ LOS RESULTADOS FUERON LOS SIGUIENTES:

- **INDICADOR: “Número de vulnerabilidades descubiertas”**

Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos del “número de vulnerabilidades descubiertas” contaban con distribución normal.

Fuente: Elaboración propia

	Shapiro-Wik		
	Estadístico	gl	Sig.
El_PreTest	,901	14	,117
El_PosTest	,749	14	,001

Tabla 9: Prueba de normalidad del indicador “número de vulnerabilidades descubiertas” antes y después de implementar el “Unified Threat Management (UTM)”

Tal como muestra la Tabla 9, los resultados de la prueba indican que el Sig. del “número de vulnerabilidades descubiertas” en el Pre-Test fue de: 0.117, cuyo valor es mayor a: 0.05; por lo tanto, el “número de vulnerabilidades descubiertas” se distribuye normalmente. Los resultados de la prueba del Post-Test indican que el Sig. del “número de vulnerabilidades descubiertas” fue de 0.001, cuyo valor es menor que 0.05, por lo que indica que el “número de vulnerabilidades descubiertas” se distribuye de manera no normal. Lo que confirma la distribución normal y no normal de ambos datos de la muestra, se puede visualizar en las figuras 13 y 14

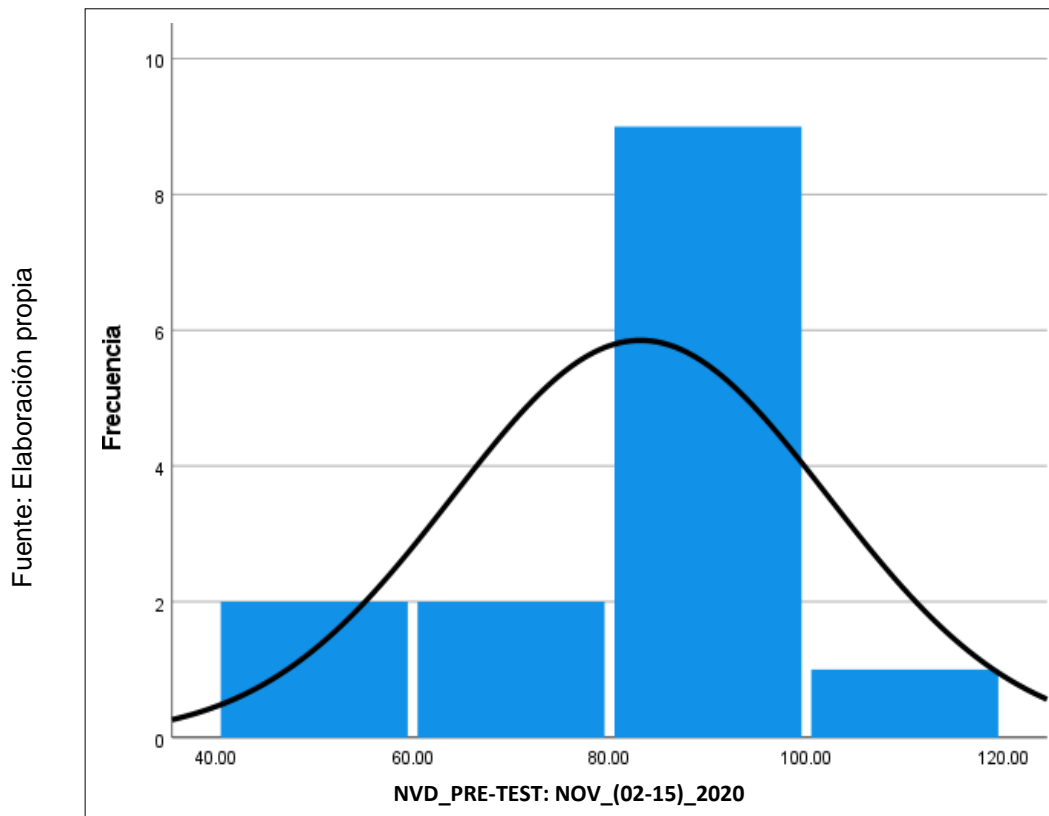


Figura 13: Prueba de normalidad del indicador número de vulnerabilidades descubiertas antes de implementar el Unified Threat Management (UTM)



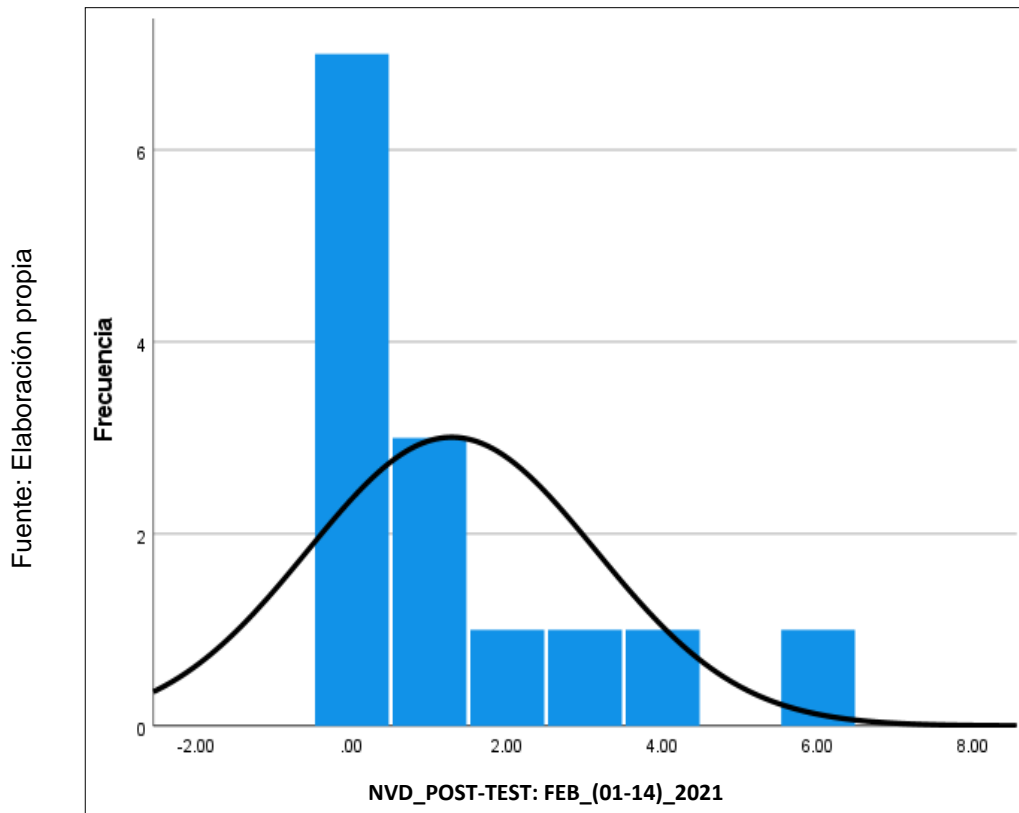


Figura 14: Prueba de normalidad del indicador número de vulnerabilidades descubiertas después de implementar el Unified Threat Management (UTM)

- INDICADOR: “número de incidentes en dispositivos de usuario final”**  
 Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos del “número de vulnerabilidades descubiertas” contaban con distribución normal.

Fuente: Elaboración propia

	Shapiro-Wik		
	Estadístico	gl	Sig.
El_PreTest	,876	14	,050
El_PosTest	,942	14	,439

Tabla 10: Prueba de normalidad del indicador “número de incidentes en dispositivos de usuario final” antes y después de implementar el “Unified Threat Management (UTM)”

Tal como muestra la Tabla 10, los resultados de la prueba indican que el Sig. del “número de incidentes en dispositivos de usuario final” en el Pre-Test fue de: 0.050, cuyo valor es mayor o igual a: 0.05; por lo tanto, el “número de incidentes en dispositivos de usuario final” se distribuye normalmente. Los resultados de la prueba del Post-Test indican que el Sig. del “número de incidentes en dispositivos de usuario final” fue de 0.439, cuyo valor es mayor que 0.05, por lo que indica que el “número de incidentes en dispositivos de usuario final” se distribuye de manera normal. Lo que confirma la distribución normal de ambos datos de la muestra, se puede visualizar en las figuras 15 y 16.

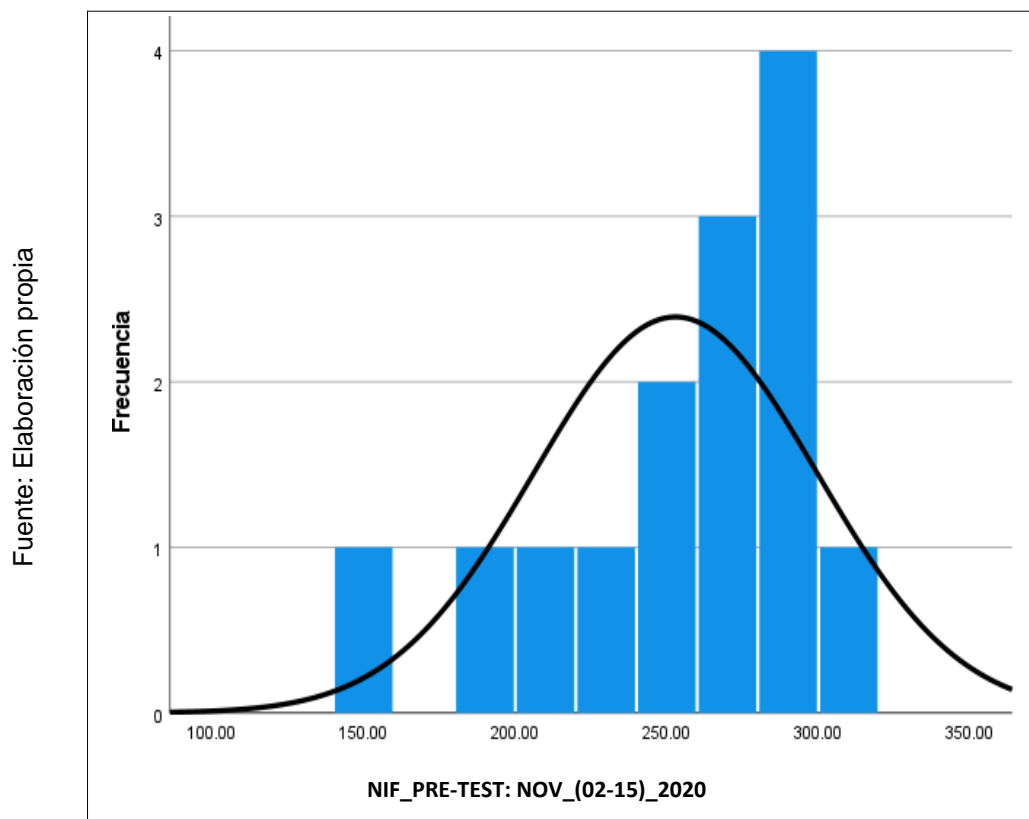


Figura 15: Prueba de normalidad del indicador número de incidentes en dispositivos de usuario antes de implementar el Unified Threat Management (UTM)

Fuente: Elaboración propia

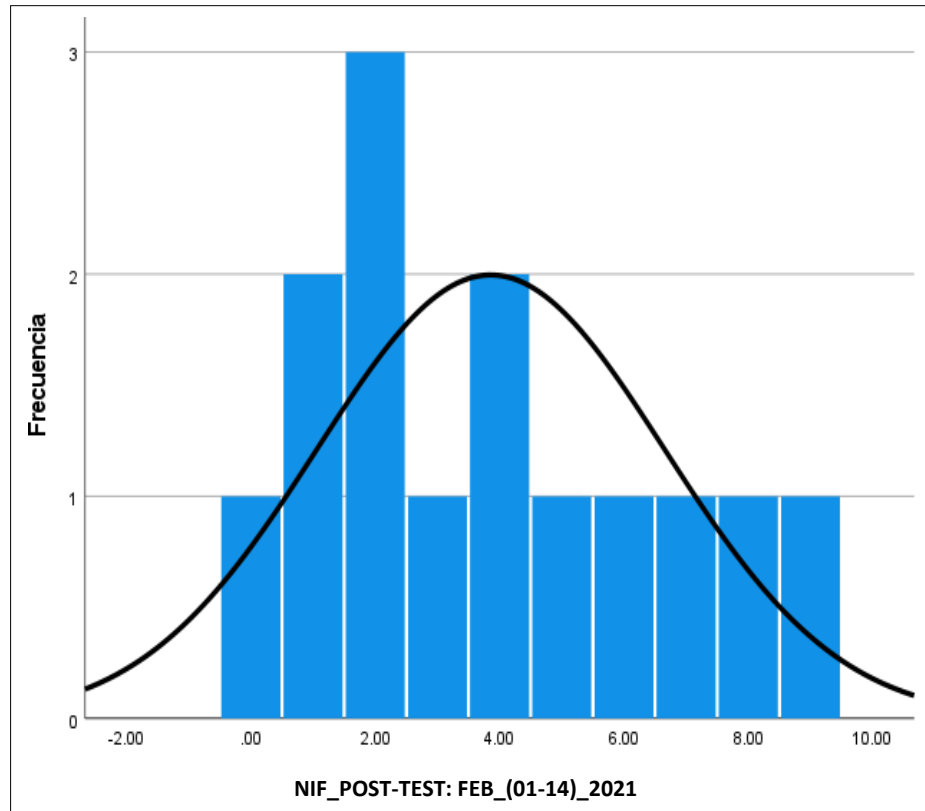


Figura 16: Prueba de normalidad del indicador número de incidentes en dispositivos de usuario después de implementar el Unified Threat Management (UTM)

### 3.3. Prueba de hipótesis

#### 3.3.1. Hipótesis de Investigación 01:

Para el indicador “Número de vulnerabilidades descubiertas”

##### a. Hipótesis de Investigación 1 (HE1)

El Unified Threat Management (UTM) reduce el número de vulnerabilidades descubiertas en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

## **b. Representación de las variables 1**

- **la1:** Número de vulnerabilidades descubiertas antes el “Unified Threat Management (UTM)” en la gestión de los servicios de seguridad
- **lp1:** Número de vulnerabilidades descubiertas después el “Unified Threat Management (UTM)” en la gestión de los servicios de seguridad

## **c. Hipótesis estadística 1**

- **Hipótesis Nula (HN01):** El Unified Threat Management (UTM) no reduce el número de vulnerabilidades descubiertas en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

$$\text{HN01: } la1 < lp1$$

Se deduce que no hubo reducción del “indicador 01” al implementar el “Unified Threat Management (UTM)”.

- **Hipótesis Alternativa (HA01):** El Unified Threat Management (UTM) reduce el número de vulnerabilidades descubiertas en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

$$\text{HA01: } la1 > lp1$$

Se deduce que el indicador mejoró al implementar el “Unified Threat Management (UTM)”.

En la siguiente figura 17, se puede verificar que el número de vulnerabilidades descubiertas (PRETEST); es de 83.14

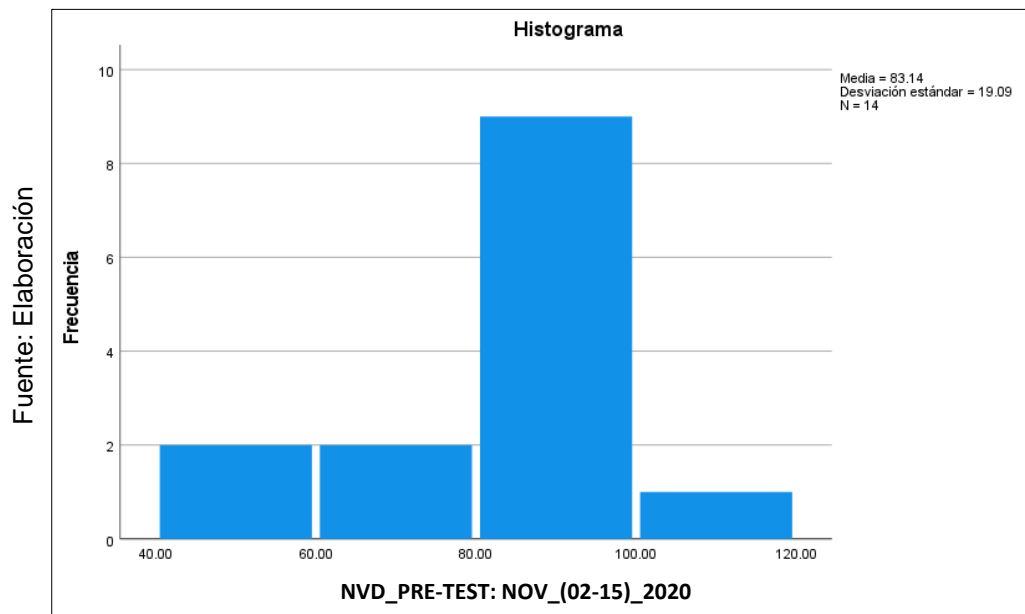


Figura 17: Número de vulnerabilidades descubiertas antes de implementar el Unified Threat Management (UTM)

En la figura 18, se puede verificar que el número de vulnerabilidades descubiertas (POSTTEST); es de 1.29

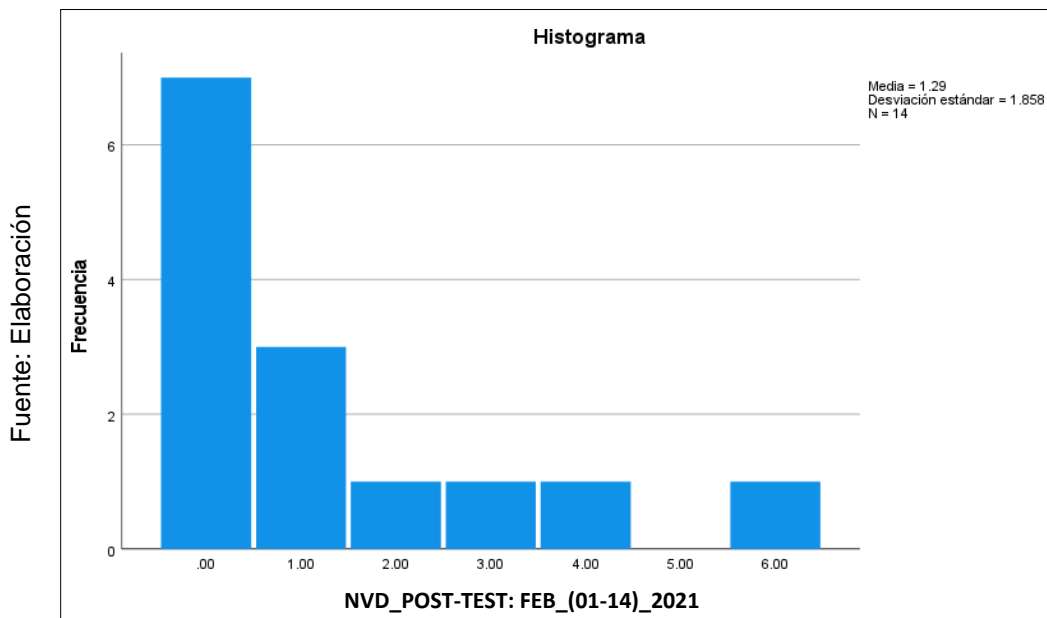


Figura 18: Número de vulnerabilidades descubiertas antes de implementar el Unified Threat Management (UTM)

En las figuras 17 y 18, se concluye que el número de vulnerabilidades descubiertas se ha reducido, podemos verificarlo al comparar el número de vulnerabilidades obtenidas en el PRETEST con 83.14 reduciéndose en el POSTTEST a 1.29; véase la figura 19.

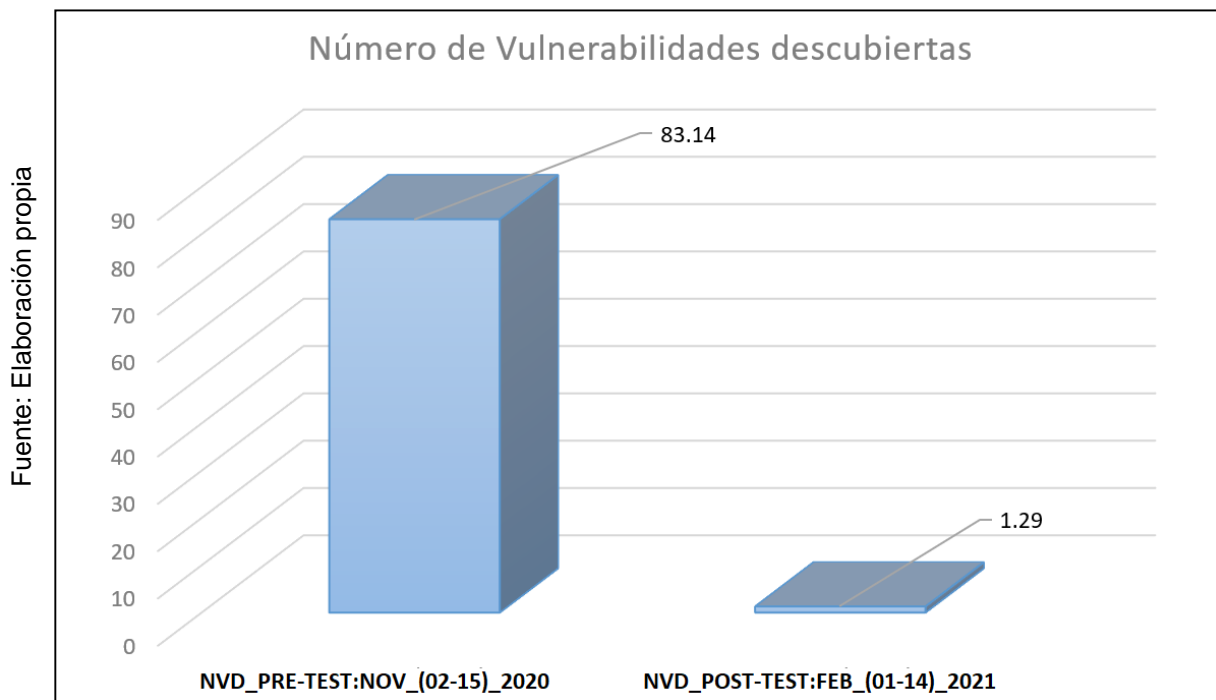


Figura 19: Número de vulnerabilidades descubiertas (Comparativa general)

### 3.3.2. Hipótesis de Investigación 02:

Para el indicador “Número de incidentes en dispositivos de usuario final”

#### a. Hipótesis Específica 2 (HE2)

El Unified Threat Management (UTM) reduce el número de incidentes en dispositivos de usuario final en la gestión de servicios de seguridad basado en COBIT 5 en la empresa REM Systems S.A.C.

#### b. Representación de las variables 2

- **Ia2:** Número de incidentes en dispositivos de usuario final antes el “Unified Threat Management (UTM)” en la gestión de los servicios de seguridad

- **Ip2:** Número de incidentes en dispositivos de usuario final después el “Unified Threat Management (UTM)” en la gestión de los servicios de seguridad

### c. Hipótesis estadística 2

- **Hipótesis Nula (HN02):** El Unified Threat Management (UTM) no reduce el número de incidentes en dispositivos de usuario final en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

**HN02:  $Ia2 < Ip2$**

Se deduce que no hubo reducción del “indicador 2” al implementar el “Unified Threat Management (UTM)”.

- **Hipótesis Alternativa (HA02):** El Unified Threat Management (UTM) reduce el número de incidentes en dispositivos de usuario final en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.

**HA02:  $Ia2 > Ip2$**

Se deduce que el “indicador 2” mejoró al implementar el “Unified Threat Management (UTM)”.

En la figura 20, el número de incidentes en dispositivos de usuario final (PRETEST); es de 252.86

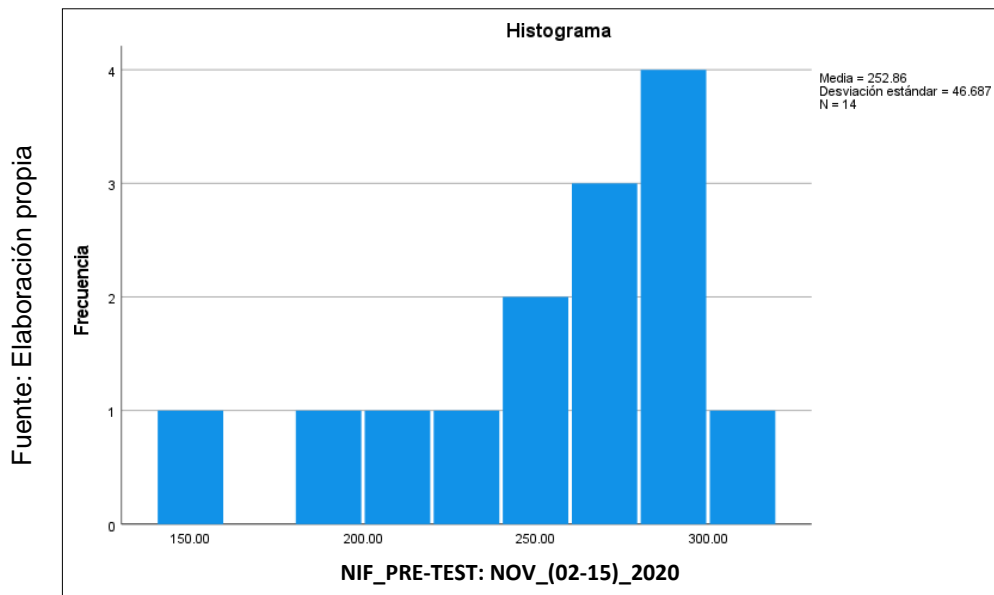


Figura 20: Número de incidentes en dispositivos de usuario final antes de implementar el Unified Threat Management (UTM)

En la figura 21, el número de número de incidentes que impliquen dispositivos de usuario final (POSTTEST); es de 3.86

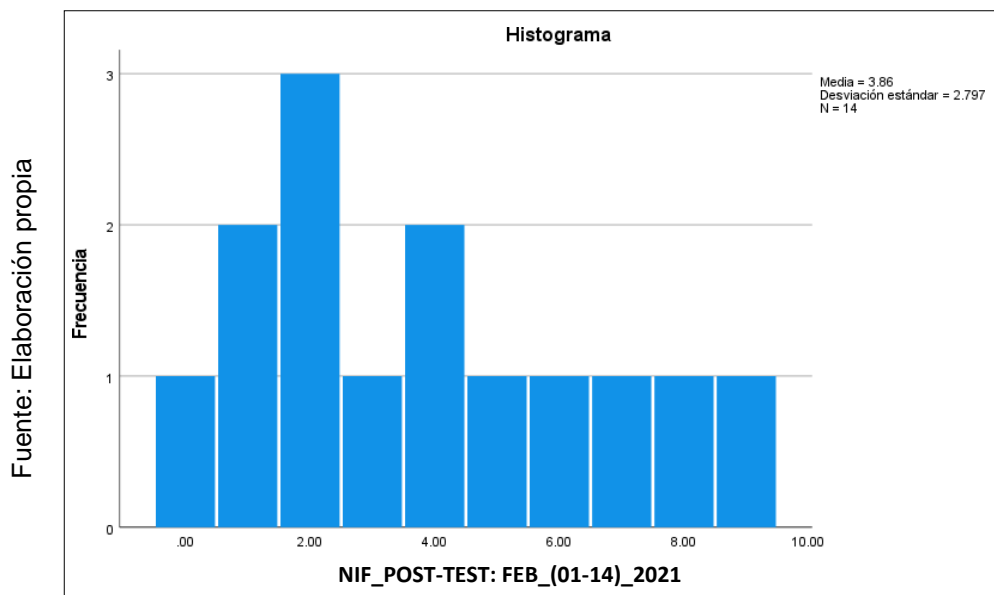


Figura 21: Número de incidentes en dispositivos de usuario final después de implementar el Unified Threat Management (UTM)



En las siguientes figuras 20 y 21, podemos concluir que el número de incidentes que impliquen dispositivos de usuario final se ha reducido, podemos verificarlo al comparar el número de vulnerabilidades obtenidas en el PRETEST con 252.86 reduciéndose en el POSTTEST a 3.86; véase la figura 22.

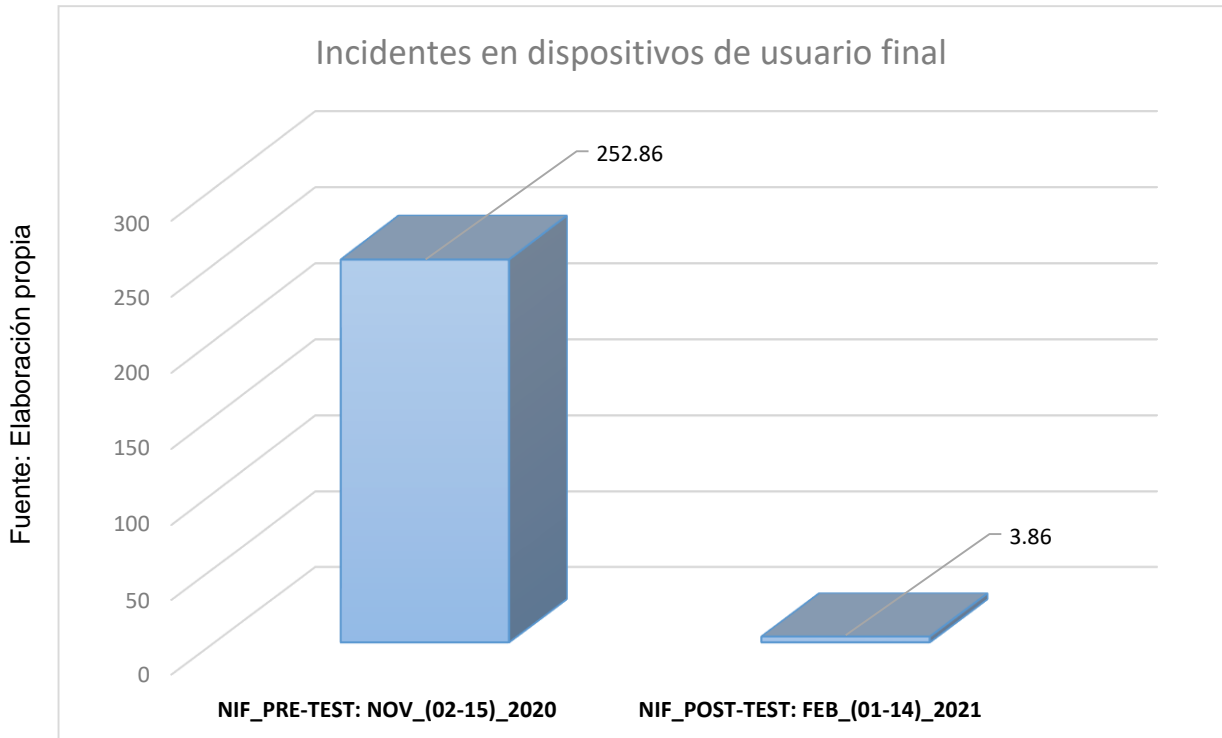


Figura 22: Número de incidentes en dispositivos de usuario final (Comparativa general)

## V. DISCUSIÓN

El presente proyecto de investigación concluye con resultados positivos luego de la implementación del Unified Threat Management (UTM), se comprobó su efectividad y reconoció gran importancia al reducir significativamente el número de vulnerabilidades descubiertas de 83.14 a 1.29. En el desarrollo de este proceso de investigación encontramos el antecedente de la investigación de Kenny Esleyther Ruiz Vierra y Wilson Delgado Ramos, en su tesis “Implementación de una solución de seguridad perimetral Open Source en la red telemática de la Universidad Nacional Pedro Ruiz Gallo”; donde concluyeron con resultados significativos en el descenso de las vulnerabilidades que en promedio se tenía 113 reduciéndolo a 5.14. Por lo tanto, se demostró que la implementación de una solución de seguridad perimetral mejoró la protección de la red interna minimizando en gran medida el número de vulnerabilidades. Del mismo modo Renzo Giancarlo Da Silva de Oliveira y Jony Rene Silva Ledesma, en su tesis “Efecto de la implementación del sistema PF-Sense en la seguridad perimetral lógica en los servicios de la red troncal de la Universidad Nacional de la Amazonía”; la implementación permitió reducir las vulnerabilidades identificadas de 104.6 a 3.3 cumpliendo todas las expectativas de ciberseguridad y protección perimetral.

Adicionalmente hemos tenido resultados de impacto positivo luego de la implementación del Unified Threat Management (UTM) en la reducción del número de incidentes que impliquen dispositivos de usuario final, reduciéndolo de 252.86 a 3.86. Esta investigación guarda una estrecha con lo que menciona Kenny Esleyther Ruiz y Wilson Delgado Ramos en su tesis “Implementación de una solución de seguridad perimetral Open Source en la red telemática de la Universidad Nacional Pedro Ruiz Gallo”; en este caso se ha reducido los incidentes de ataques mal intencionados a los dispositivos de tipo servidor disminuyendo los ataques de 287 a 10. En las investigaciones mencionadas los resultados obtenidos demuestran que la implementación de un sistema de seguridad perimetral Unified Threat

Management (UTM) genera valor en la reducción de las vulnerabilidades que conlleva a potenciales peligros de ciberseguridad. Adicionalmente los resultados que hemos obtenido de los antecedentes de las investigaciones recolectadas encontramos lo señalado por Omar Bautista Pillaca, en su tesis “Implementación de un servidor Linux y su influencia en la seguridad perimetral de la red local de la empresa Junefield Group S.A.”; demostrando resultados positivos de mejora en la confidencialidad pasando de 32.8% a 95.7%, la integridad pasando de 69.11% a 80.14% y la disponibilidad pasó de 90.0% a un 94.6%. Todas las investigaciones han servido para demostrar la eficiencia de soluciones y tecnologías basadas en Unified Threat Management (UTM).

## VI. CONCLUSIONES

Las conclusiones a las cuales hemos llegado son las siguientes:

1. Podemos concluir manifestando que la implementación del Unified Threat Management (UTM) ha reducido de una manera significativa el número de vulnerabilidades descubiertas en la empresa REM Systems S.A.C.; ya que el número de vulnerabilidades descubiertas antes de la implementación del Unified Threat Management (UTM) era de un promedio de 83.14 vulnerabilidades diarias; y después de la implementación del Unified Threat Management (UTM) el número promedio de vulnerabilidades descubiertas se ha reducido a 1.29 vulnerabilidades diarias; lo que demuestra que las vulnerabilidades se han reducido en un 98.45% en la empresa REM Systems S.A.C.
2. Podemos concluir manifestando que la implementación del Unified Threat Management (UTM) ha reducido de una manera significativa el número de incidentes en dispositivos de usuario final en la empresa REM Systems S.A.C.; ya que el número de incidentes en dispositivos de usuario final antes de la implementación del Unified Threat Management (UTM) era de un promedio de 252.86 incidentes diarios; y después de la implementación del Unified Threat Management (UTM) el número promedio de incidentes en dispositivos de usuario final se ha reducido a 3.86 incidentes diarios; lo que demuestra que el número de incidentes que impliquen dispositivos de usuario final se ha reducido en un 98.47% en la empresa REM Systems S.A.C.
3. Para concluir, luego de haber obtenido resultados muy satisfactorios del presente estudio podemos concluir que la implementación de tecnologías basadas en Unified Threat Management (UTM) garantiza una eficaz medida de contención frente a vulnerabilidades y amenazas de ciberseguridad en la empresa REM Systems S.A.C.

## VII. RECOMENDACIONES

1. El Perú hasta el día de hoy no cuenta con ninguna estrategia nacional de ciberseguridad o seguridad cibernética, y según la agencia peruana de noticias “Andina” es el segundo país con menos ciberseguridad en América Latina; por ello, se recomienda aplicar el presente estudio en otras instituciones, organizaciones y empresas sin distinción del rubro o al tamaño de ellas ya que la tecnología actualmente es una necesidad en los negocios y la protección de la misma aporta valor para el desarrollo y el éxito de las mismas.
2. El presente proyecto de tesis complementó la investigación del trabajo de tesis titulado “Metodología integral para evaluar el rendimiento de Firewalls” el cual concluyó demostrando que los dispositivos de seguridad perimetral basados en Hardware tienen mayor desempeño y estabilidad que los que son basados en software, por ello y por otras razones como la guía del cuadrante de Garner se decidió que la implementación del Unified Threat Management (UTM) en la empresa REM System S.A.C. sea basado en hardware utilizando la tecnología de FORTINET. Se recomienda continuar la presente investigación utilizando e implementando tecnologías como los llamados: “NGFW”.
3. A los responsables de la ciberseguridad se les recomienda que todo Unified Threat Management (UTM) basado en Hardware o Software sea constantemente administrado con una óptica de mejora continua, ya que diariamente aparecen nuevos riesgos y nuevas vulnerabilidades en cuestiones de ciberseguridad, todo ello hace de que los administradores de sistemas despierten conciencia y apliquen mejoras a sus dispositivos de seguridad perimetral basados como mínimo en Unified Threat Management (UTM) o “NGFW”.

## REFERENCIAS

- (2012). En D. Kosutic, *Ciberseguridad en 9 pasos* (pág. 14). EPPSServicesLtd, Zagreb.
- Barrett, D., Weiss, M., & Hausman, K. (2015). Appliance Unified Threat Management. En *CompTIA Security+, II* (pág. 27). Indiana, USA: Pearson Education Inc.
- Barrett, D., Weiss, M., & Hausman, K. (2015). Unified Threat Management (UTM). En *CompTIA Security+, II* (pág. 171). Indiana, USA: Pearson Education Inc.
- Bautista Pillaca, O. (2017). *Implementación de un servidor Linux y su influencia en la seguridad perimetral de la red local de la empresa Junefield Group S.A.* Tesis de titulación, Universidad Cesar Vallejo, Lima - Perú.
- Bernal Morell, E. (2014). Los gráficos de probabilidad normal. En *Bioestadística básica para investigadores con SPSS* (pág. 18). España: Bubok Publishing S.L.
- Castro, F. (2003). Muestra. En *El proyecto de investigación y su esquema de elaboración* (pág. 69). Caracas, Venezuela: Uyapar.
- Da Silva de Oliveira, R. G., & Silva Ledesma, J. R. (2016). *Efecto de la Implementación del sistema PF-Sense en la seguridad perimetral lógica en los servicios de la red troncal de la Universidad Nacional de la Amazonía.* Tesis de titulación, Universidad Privada de la Selva Peruana, Iquitos - Perú.
- Enrique Javier Santiago, J. S. (2017). <https://revistas.uax.es>. Obtenido de [https://revistas.uax.es/index.php/tec\\_des/article/download/1174/964](https://revistas.uax.es/index.php/tec_des/article/download/1174/964)
- Espinoza Chipane, C. R. (2018). *Propuesta de una red privada virtual para mejorar el servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A.* Tesis de titulación, Universidad Autónoma del Perú, Lima - Perú.

Felipa, P. B. (20 de Octubre de 2017). *Marketing+Internet=e-commerce: oportunidades y desafíos*. Obtenido de <https://www.redalyc.org/https://www.redalyc.org/pdf/3235/323549941003.pdf>

Fortinet. (2021). <https://www.fortinet.com/>. Obtenido de <https://www.fortinet.com/lat/products/smallbusiness/utm>

Gómez Vieites, Á. (2014). Principio de Defensa en profundidad. En *Seguridad en equipos informáticos* (pág. 29). Madrid, España: RA-MA.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2010). Métodos de análisis de datos. En *Metodología de la investigación, VI* (pág. 260). Distrito Federal (DF), México: McGRAW-HILL / Interamericana Editores S.A.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). Coeficiente de correlación de Pearson. En *Metodología de la investigación, VI* (pág. 304). Distrito Federal (DF), México: McGRAW-HILL / Interamericana Editores S.A.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). Confiabilidad. En *Metodología de la investigación, VI* (pág. 200). Distrito Federal (DF), México: McGRAW-HILL / Interamericana Editores S.A.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). Diseños experimentales. En *Metodología de la investigación, VI* (pág. 129). Distrito Federal (DF), México: McGRAW-HILL / Interamericana Editores S.A.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). En el proceso cuantitativo. En *Metodología de la investigación, VI* (pág. 129). Distrito Federal (DF), México: McGRAW-HILL / Interamericana Editores S.A.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). Grdos de correlación de Pearson. En *Metodología de la investigación, VI* (pág. 304). Distrito Federal (DF), México: McGRAW-HILL / Interamericana Editores S.A.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). Hipótesis alternativa. En *Metodología de la investigación, VI* (pág. 105). Distrito Federal (DF), México: McGRAW-HILL / Interamericana Editores S.A.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). Hipótesis Nula. En *Metodología de la investigación, VI* (pág. 104). Distrito Federal (DF), México: McGRAW-HILL / Interamericana Editores S.A.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). Población. En *Metodología de la investigación, VI* (pág. 174). Distrito Federal (DF), México: McGRAW-HILL / Interamericana Editores S.A.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). Preexperimentos. En *Metodología de la investigación, VI* (pág. 141). Distrito Federal (DF), México: McGRAW-HILL / Interamericana Editores S.A.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). Pre-test / Re-Test. En Castro, *Metodología de la investigación, VI* (pág. 208). Distrito Federal (DF), México: McGRAW-HILL / Interamericana Editores S.A.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). Validez. En *Metodología de la investigación, VI* (pág. 200). Distrito Federal (DF), México: McGRAW-HILL / Interamericana Editores S.A.

ISACA. (2012). COBIT 5 para la seguridad de la información - Público Objetivo. En *COBIT 5 para la seguridad de la información* (pág. 16). Illinois, USA: ISACA.

ISACA. (2012). DSS05 - Gestión de servicios de seguridad. En *Procesos Catalizadores* (pág. 191). Illinois, USA: ISACA.

ISACA. (2012). Familia de productos de COBIT 5. En *Un Marco de negocio para el Gobierno y la Gestión de las TI de la empresa* (pág. 26). Illinois, USA: ISACA.



ISACA. (2012). Modelo de referencia de procesos de COBIT 5. En *Un Marco de negocio para el Gobierno y la Gestión de las TI de la empresa* (pág. 33). Illinois, USA: ISACA.

ISACA. (2012). Principio 1 - Satisfacer las necesidades de las partes interesadas. En *COBIT 5 para la seguridad de la Información* (pág. 21). Illinois, USA: ISACA.

ISACA. (2012). Resumen ejecutivo. En *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa* (pág. 13). Illinois, USA: ISACA.

Lima Rios, O. K. (2016). *Melhores práticas para implantar política de segurança da informação e comunicação em instituições federais de ensino superior*. Tesis de Maestría, Universidade Federal de Pernambuco , Recife - Brasil.

Méndez Álvarez, C. E. (2011). Identificación de la investigación. En *Metodología* (pág. 92). Bogotá, Colombia: McGraw Hill.

Miguez Gómez, G. F. (2017). *Implementación de un sistema de gestión unificada de amenazas (UTM) para la empresa de Créditos Palacio del Hogar*. Tesis de Maestría, Escuela Superior Politécnica del Litoral de la Facultad de Ingeniería en Electricidad y Computación, Guayaquil - Ecuador.

Mingrone de Camarota, P. L. (2007). La técnica del fichaje. En *Metodología del estudio eficaz* (pág. 73). Buenos aires, Argentina.

Moncada Jiménez, J. (2005). Nivel de significancia. En *Estadística para las ciencias del movimiento humano, I* (pág. 9).

Pacotaype Huaman, R. J. (2018). *Metodología integral para evaluar el rendimiento de firewalls*. Tesis de titulación, Universidad Cesar Vallejo, Lima - Perú.

Pérez Lasso, A. M., & Pinto Gutiérrez, G. E. (2019). *Sistema de seguridad perimetral para el edificio Zeus de Arcotel basado en tecnologías UTM de código abierto*. Universidad Politécnica Salesiana. Quito - Ecuador.

Pérez, M. y. (4 de Junio de 2021). <https://idconline.mx/>. Obtenido de <https://idconline.mx/corporativo/2021/06/04/aumentaron-ciberataques-dirigidos-a-fuerza-laboral-remota>

Risk, M. (2003). Pruebas de normalidad de una muestra. En *Cartas sobre Estadística de la Revista Argentina de Bioingeniería*, v1.1 (pág. 19). Buenos Aires, Argentina.

Robayo Zapata, S. G., & Miraba Cercado, Y. O. (2017). *Implementación de un UTM Keiro para el control y mitigación de amenazas presentes en la red perimetral de la empresa Mindcorp S.A.* Tesis de Titulación, Universidad de Guayaquil, Guayaquil - Ecuador.

Ruiz Vieira, K. E., & Delgado Ramos, W. (2018). *Implementación de una solución de seguridad perimetral Open Source en la red telemática de la Universidad Nacional Pedro Ruiz Gallo.* Tesis de titulación, Universidad de Lambayeque, Chiclayo - Perú.

Sendra, J. (2010). Fichas de registro. En *Atención y apoyo psicosocial domiciliario* (pág. 118). España: IdeasPropias.

Voronkov, A. (2020). *Usability of Firewall Configuration.* Tesis de Doctorado, Karlstad University, Karlstad - Suecia.

Whitman, M., & Herbert, M. (2016). Unified Threat Management (UTM). En *Management of Information Security*. V (pág. 536). Boston - USA: Cengage.

Zambrano, F. (30 de Octubre de 2015). <https://andina.pe/>. Obtenido de <https://andina.pe/agencia/noticia.aspx?id=582288>

## ANEXO 1: MATRIZ DE CONSISTENCIA

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLE	VARIABLE DEPENDIENTE			MÉTODOS
Principal	General	General	Independiente				
<p><b>PG:</b> ¿De qué manera el Unified Threat Management (UTM) influye en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems SAC?</p>	<p><b>OG:</b> Determinar la influencia del Unified Threat Management (UTM) en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems SAC.</p>	<p><b>HG:</b> El Unified Threat Management (UTM) influye significativamente en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems SAC.</p>	<p><b>Unified Threat Management (UTM)</b></p>				<p><b>Tipo de investigación:</b> Cuantitativo - Aplicada</p>
Específicos	Específicos	Específicos	Dependiente	Dimensión	Indicadores	Instrumentos	Fórmula
<p><b>PE1:</b> ¿De qué manera el Unified Threat Management (UTM) influye en el número de vulnerabilidades descubiertas en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems SAC?</p>	<p><b>OE1:</b> Determinar la influencia del Unified Threat Management (UTM) en el número de vulnerabilidades descubiertas en la gestión de servicios de seguridad basado en COBIT 5 en la empresa REM Systems SAC.</p>	<p><b>HE1:</b> El Unified Threat Management (UTM) reduce el número de vulnerabilidades descubiertas en la gestión de servicios de seguridad basado en COBIT 5 en la empresa Rem Systems SAC.</p>	<p><b>Gestión de servicios de seguridad</b></p>		Número de vulnerabilidades descubiertas	Ficha de registro	$NVD = NVT + NVC + NVS$
<p><b>PE2:</b> ¿De qué manera el Unified Threat Management (UTM) influye en el número de incidentes que impliquen dispositivos de usuario final en la gestión de servicios de seguridad de COBIT 5 en la empresa Rem Systems SAC?</p>	<p><b>OE2:</b> Determinar la influencia del Unified Threat Management (UTM) en el número de incidentes que impliquen dispositivos de usuario final en la gestión de servicios de seguridad basado en COBIT 5 en la empresa REM Systems SAC.</p>	<p><b>HE2:</b> El Unified Threat Management (UTM) reduce el número de incidentes que impliquen dispositivos de usuario final en la gestión de servicios de seguridad basado en COBIT 5 en la empresa REM Systems SAC.</p>			Número de incidentes en dispositivos de usuario final	Ficha de registro	$NIF = DSK + LAP + WRK$
							<p><b>Población:</b> 12 fichas de registro semanal</p> <p><b>Técnicas e instrumentos:</b></p> <ul style="list-style-type: none"> <li>- Fichaje</li> <li>- Ficha de registro</li> </ul>

## ANEXO 2: AUTORIZACIÓN DE LA EMPRESA



### AUTORIZACIÓN (EMPRESA)

Lima, 07 de enero del 2021

Señores

Universidad Cesar Vallejo

Escuela académico profesional de ingeniería de sistemas – UCV Filial Lima

Presente. -

De nuestra consideración:

Por medio de la presente, tenemos el agrado de dirigirnos a ustedes, a fin de informarles sobre la solicitud para el uso de información no confidencial de mi representado, requerido por vuestro alumno del proceso de titulación **Sr. LUIS ARNALDO GODOY FUENTES**, identificado con el DNI: 44733139, para el desarrollo de su tesis titulada: **“UNIFIED THREAT MANAGEMENT (UTM) PARA LA GESTIÓN DE LOS SERVICIOS DE SEGURIDAD BASADO EN COBIT 5 EN LA EMPRESA REM SYSTEMS S.A.C.”**

Al respecto, de manera expresa autorizamos que la información no confidencial recogida de la presente investigación pase a ser de carácter público dentro de los fines académicos que son propios de la naturaleza de este tipo de trabajos, entre los cuales está su publicación en el repositorio de la Universidad, una vez concluido el mismo.

Sin otro particular, nos despedimos de ustedes expresándole las muestras de nuestra mayor consideración.

Atentamente,

  
\_\_\_\_\_  
**REM SYSTEMS S.A.C.**  
**ADRIAN MARTIN ALCANTARA CORTEZ**  
Adrian Alcantara Cortez  
Gerente General  
**GERENTE GENERAL**

Jr. Ernesto Mora 475 Piso 2, San Martin de Porres, Lima – Perú

Teléfono: (511) 701 – 3625

[www.remsystems.pe](http://www.remsystems.pe)

## ANEXO 3: COMPROMISO DE CONFIDENCIALIDAD




### COMPROMISO DE CONFIDENCIALIDAD

Yo, LUIS ARNALDO GODOY FUENTES, estudiante de Ingeniería de Sistemas de la Universidad César Vallejo, identificado con DNI N° 44733139, con la tesis titulada “**UNIFIED THREAT MANAGEMENT (UTM) PARA LA GESTIÓN DE LOS SERVICIOS DE SEGURIDAD BASADO EN COBIT 5 EN LA EMPRESA REM SYSTEMS S.A.C.**”

Me comprometo a que los datos brindados por la empresa Rem Systems S.A.C. han sido utilizados únicamente con fines académicos, se ha respetado la ética y el acuerdo de confidencialidad establecido por la empresa la cual detalla la protección de los datos personales de sus clientes.

En caso de no cumplir con este compromiso de confidencialidad, asumiré las sanciones disciplinarias designadas por la empresa y me pondré a disposición de las autoridades.

Suscrito, en la ciudad de Lima, el 07 de Enero del 2021

  
LUIS ARNALDO GODOY FUENTES  
BACHILLER

  
ADRIAN MARTIN ALCANTARA CORTEZ  
**REM SYSTEMS S.A.C.**  
Adrian Alcantara Cortez  
Gerente General

Jr. Ernesto Mora 475 Piso 2, San Martin de Porres, Lima – Perú  
Teléfono: (511) 701 – 3625  
[www.remsystems.pe](http://www.remsystems.pe)

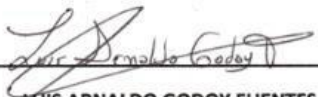
## ANEXO 4: CONSTANCIA DE ASISTENCIA A ENTREVISTA Y ENCUESTA




### CONSTANCIA DE ASISTENCIA A ENTREVISTA Y ENCUESTA

Yo, Luis Arnaldo Godoy Fuentes, estudiante de Ingeniería de Sistemas de la Universidad César Vallejo, por medio de la presente se deja constancia de haber realizado la entrevista y encuesta que forma parte del trabajo de investigación titulado: **“UNIFIED THREAT MANAGEMENT (UTM) PARA LA GESTIÓN DE LOS SERVICIOS DE SEGURIDAD BASADO EN COBIT 5 EN LA EMPRESA REM SYSTEMS S.A.C.”** para obtener el título de Ingeniero de Sistemas.

Suscrito, en la ciudad de Lima, el 11 de Enero del 2021

  
\_\_\_\_\_  
**LUIS ARNALDO GODOY FUENTES**  
ENTREVISTADOR

  
\_\_\_\_\_  
**ADRIAN MARTIN ALCANTARA CORTEZ**  
**REM SYSTEMS S.A.C.**  
Adrian Alcantara **GERENTE GENERAL**  
Gerente General

Jr. Ernesto Mora 475 Piso 2, San Martin de Porres, Lima – Perú

Teléfono: (511) 701 – 3625

[www.remsystems.pe](http://www.remsystems.pe)

## **ANEXO 5: CONTENIDO DE ENTREVISTA Y ENCUESTA**

**NOMBRE Y APELLIDO:** Adrián Martín Alcántara Cortez

**EMPRESA:** REM Systems S.A.C.

**PUESTO:** Gerente General

### **PREGUNTAS:**

#### **1. ¿A QUÉ SE DEDICA LA EMPRESA?**

RPTA: Servicios, proyectos y consultoría de soluciones tecnológicas empresariales

#### **2. ¿CUÁL ES EL CARGO QUE TIENE EN LA EMPRESA?**

RPTA: Gerente General

#### **3. ¿CUÁLES SON LOS PROBLEMAS QUE ACTUALMENTE TIENE LA EMPRESA?**

RPTA: Los problemas que actualmente tenemos son de seguridad informática porque desde los inicios de la empresa hemos tenido antecedentes de ataques y vulnerabilidades a nuestra red interna. Sumado a ello a consecuencia de la pandemia y el confinamiento los servicios de mesa de ayuda de la empresa han tenido que gestionarse remotamente desde la casa de nuestros colaboradores, para ello hemos tenido que utilizar aplicaciones de escritorio remoto comerciales, pero a raíz de esto también hemos tenido problemas y tenemos conocimiento que utilizar este tipo de aplicaciones no es lo mejor cuando se habla de seguridad informática.

#### **4. ¿QUÉ TIPO DE HERRAMIENTAS DE ACCESO REMOTO UTILIZA LA EMPRESA?**

RPTA: Anydesk o TeamViewer

**5. ¿LA EMPRESA ACTUALMENTE CUENTA CON ALGÚN DE SOLUCIÓN TECNOLÓGICA PARA MITIGAR ESTOS PROBLEMAS?**

RPTA: Tenemos implementadas herramientas de estaciones finales como antivirus, Antispyware y un routerOS Mikrotik que es del proveedor de acceso a internet (ISP) que solo funciona como router, sabemos que dicho equipo cuenta con ciertas características que nos podrían ser muy útiles como VPN, pero el proveedor solo lo configura para acceso a internet y no nos permite habilitar otro servicio, la administración total la tienen ellos.

**6. ¿DISPONEN DE ALGUNA TECNOLOGÍA BASADA EN TECNOLOGÍAS UNIFICADAS PARA LA PROTECCIÓN Y SEGURIDAD DE LA RED PERIMETRAL?**

RPTA: De ese tipo, por ahora no.

**7. ¿TIENEN IMPLEMENTADA ALGUNA MEDIDA DE ADMINISTRACIÓN PARA EL USO DE INTERNET? (Restricciones, política, controles de acceso, etc.)**

RPTA: Por ahora no.

**8. ¿TIENEN IMPLEMENTADA ALGUNA SOLUCIÓN QUE BRINDE SEGURIDAD AL TRÁFICO DE CORREOS ELECTRÓNICOS ENTRANTES Y SALIENTES?**

RPTA: Tenemos los antivirus que nos han ayudado mucho, pero en algunas circunstancias no han sido tan eficaces por lo que hemos tenido infecciones por medio del correo electrónico.

**9. ¿HAN TENIDO ATAQUES QUE HAN SIDO DE GRAN IMPACTO?**

RPTA: Los más críticos fueron cuando fuimos atacados con Ransomware en 3 ocasiones, comprometiendo varias estaciones de trabajo y el servidor de archivos. Pero recuperamos gracias a que tenemos un buen plan de gestión de riesgos, realizamos Backus diarios, perdimos horas hombre de trabajo.



## ANEXO 6: VALIDACIÓN DE EXPERTOS PARA LAS METODOLOGÍAS

 <b>UCV</b> UNIVERSIDAD CÉSAR VALLEJO	<b>VALIDACIÓN DE INSTRUMENTO</b>
<b>Título de tesis:</b>	Unified Threat Management (UTM) para la gestión de los servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.
<b>Autor:</b>	Godoy Fuentes, Luis Arnaldo
<b>Nombre del instrumento de evaluación:</b>	Ficha de Registro
<b>Indicador:</b>	Número de vulnerabilidades descubiertas
<b>DATOS DEL EXPERTO</b>	
<b>Apellidos y Nombres:</b>	Sinti Zárate, July Tatiana
<b>Título y/o Grado:</b>	Magister
<b>Fecha:</b>	08/04/2021

INDICADORES	CRITERIO	DEFICIENTE 1% - 20%	REGULAR 21% - 40%	BUENO 41% - 60%	MUY BUENO 61% - 80%	EXCELENTE 81% - 100%	
Claridad	Está formado por lenguaje apropiado					85%	
Objetividad	Esta expresado en conducta observable					85%	
Actualidad	Es adecuado al avance de la ciencia y tecnología					85%	
Organización	Existe una organización lógica					90%	
Suficiencia	Comprende los aspectos de cantidad y calidad					85%	
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico					85%	
Consistencia	Está basado en aspectos teóricos y científicos					85%	
Coherencia	Entre los índices e indicadores					90%	
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr					90%	
Pertenencia	El instrumento es adecuado al tipo de investigación					90%	
<b>PROMEDIO</b>							<b>87%</b>

### Aplicabilidad:

- El instrumento puede ser aplicado  
 El instrumento debe ser mejorado



Firma del Experto

**VALIDACIÓN DE INSTRUMENTO**

<b>Título de tesis:</b>	<b>Unified Threat Management (UTM) para la gestión de los servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.</b>
<b>Autor:</b>	Godoy Fuentes, Luis Arnaldo
<b>Nombre del instrumento de evaluación:</b>	Ficha de Registro
<b>Indicador:</b>	Número de vulnerabilidades descubiertas
<b>DATOS DEL EXPERTO</b>	
<b>Apellidos y Nombres:</b>	<b>SAAVEDRA JIMENEZ ROBERT ROY</b>
<b>Título y/o Grado:</b>	<b>MAGISTER EN DIRECCION Y GESTION DE EMPRESAS</b>
<b>Fecha:</b>	<b>20/03/2021</b>

INDICADORES	CRITERIO	DEFICIENTE 1% - 20%	REGULAR 21% - 40%	BUENO 41% - 60%	MUY BUENO 61% - 80%	EXCELENTE 81% - 100%
Claridad	Está formado por lenguaje apropiado					<b>85%</b>
Objetividad	Esta expresado en conducta observable					<b>85%</b>
Actualidad	Es adecuado al avance de la ciencia y tecnología					<b>85%</b>
Organización	Existe una organización lógica					<b>85%</b>
Suficiencia	Comprende los aspectos de cantidad y calidad					<b>85%</b>
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico					<b>85%</b>
Consistencia	Está basado en aspectos teóricos y científicos					<b>85%</b>
Coherencia	Entre los índices e indicadores					<b>85%</b>
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr					<b>85%</b>
Pertenencia	El instrumento es adecuado al tipo de investigación					<b>85%</b>
<b>PROMEDIO</b>		<b>85%</b>				

**Aplicabilidad:**
 El instrumento puede ser aplicado

 El instrumento debe ser mejorado



Firma del Experto

**VALIDACIÓN DE INSTRUMENTO**

<b>Título de tesis:</b>	<b>Unified Threat Management (UTM) para la gestión de los servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.</b>
<b>Autor:</b>	Godoy Fuentes, Luis Arnaldo
<b>Nombre del instrumento de evaluación:</b>	Ficha de Registro
<b>Indicador:</b>	Número de vulnerabilidades descubiertas
<b>DATOS DEL EXPERTO</b>	
<b>Apellidos y Nombres:</b>	<b>Bermejo Terrones Henry Paúl</b>
<b>Título y/o Grado:</b>	Maestro en Ingeniería de Sistemas con mención en TI
<b>Fecha:</b>	10/04/2021

INDICADORES	CRITERIO	DEFICIENTE	REGULAR	BUENO	MUY BUENO	EXCELENTE
		1% - 20%	21% - 40%	41% - 60%	61% - 80%	81% - 100%
Claridad	Está formado por lenguaje apropiado					<b>95%</b>
Objetividad	Esta expresado en conducta observable					<b>90%</b>
Actualidad	Es adecuado al avance de la ciencia y tecnología					<b>95%</b>
Organización	Existe una organización lógica					<b>95%</b>
Suficiencia	Comprende los aspectos de cantidad y calidad					<b>95%</b>
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico					<b>95%</b>
Consistencia	Está basado en aspectos teóricos y científicos					<b>90%</b>
Coherencia	Entre los índices e indicadores					<b>90%</b>
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr					<b>90%</b>
Pertenencia	El instrumento es adecuado al tipo de investigación					<b>95%</b>
<b>PROMEDIO</b>		<b>93%</b>				

**Aplicabilidad:**

- El instrumento puede ser aplicado  
 El instrumento debe ser mejorado



Firma del Experto

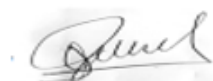
**VALIDACIÓN DE INSTRUMENTO**

<b>Título de tesis:</b>	<b>Unified Threat Management (UTM) para la gestión de los servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.</b>
<b>Autor:</b>	Godoy Fuentes, Luis Arnaldo
<b>Nombre del instrumento de evaluación:</b>	Ficha de Registro
<b>Indicador:</b>	Número de incidentes en dispositivos de usuario final
<b>DATOS DEL EXPERTO</b>	
<b>Apellidos y Nombres:</b>	<b>SAAVEDRA JIMENEZ ROBERT ROY</b>
<b>Título y/o Grado:</b>	<b>MAGISTER EN DIRECCION Y GESTION DE EMPRESAS</b>
<b>Fecha:</b>	<b>20/03/2021</b>

INDICADORES	CRITERIO	DEFICIENTE 1% - 20%	REGULAR 21% - 40%	BUENO 41% - 60%	MUY BUENO 61% - 80%	EXCELENTE 81% - 100%
Claridad	Está formado por lenguaje apropiado					<b>85%</b>
Objetividad	Esta expresado en conducta observable					<b>85%</b>
Actualidad	Es adecuado al avance de la ciencia y tecnología					<b>85%</b>
Organización	Existe una organización lógica					<b>85%</b>
Suficiencia	Comprende los aspectos de cantidad y calidad					<b>85%</b>
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico					<b>85%</b>
Consistencia	Está basado en aspectos teóricos y científicos					<b>85%</b>
Coherencia	Entre los índices e indicadores					<b>85%</b>
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr					<b>85%</b>
Pertenencia	El instrumento es adecuado al tipo de investigación					<b>85%</b>
<b>PROMEDIO</b>		<b>85%</b>				

**Aplicabilidad:**
 El instrumento puede ser aplicado

 El instrumento debe ser mejorado



Firma del Experto

## VALIDACIÓN DE INSTRUMENTO

<b>Título de tesis:</b>	<b>Unified Threat Management (UTM) para la gestión de los servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.</b>
<b>Autor:</b>	Godoy Fuentes, Luis Arnaldo
<b>Nombre del instrumento de evaluación:</b>	Ficha de Registro
<b>Indicador:</b>	Número de incidentes en dispositivos de usuario final
<b>DATOS DEL EXPERTO</b>	
<b>Apellidos y Nombres:</b>	<b>Bermejo Terrones Henry Paúl</b>
<b>Título y/o Grado:</b>	Maestro en Ingeniería de Sistemas con mención en TI
<b>Fecha:</b>	10/04/2021

INDICADORES	CRITERIO	DEFICIENTE 1% - 20%	REGULAR 21% - 40%	BUENO 41% - 60%	MUY BUENO 61% - 80%	EXCELENTE 81% - 100%
Claridad	Está formado por lenguaje apropiado					<b>95%</b>
Objetividad	Esta expresado en conducta observable					<b>90%</b>
Actualidad	Es adecuado al avance de la ciencia y tecnología					<b>95%</b>
Organización	Existe una organización lógica					<b>95%</b>
Suficiencia	Comprende los aspectos de cantidad y calidad					<b>95%</b>
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico					<b>95%</b>
Consistencia	Está basado en aspectos teóricos y científicos					<b>90%</b>
Coherencia	Entre los índices e indicadores					<b>90%</b>
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr					<b>90%</b>
Pertenencia	El instrumento es adecuado al tipo de investigación					<b>95%</b>
<b>PROMEDIO</b>		<b>93%</b>				

**Aplicabilidad:**

- El instrumento puede ser aplicado
- El instrumento debe ser mejorado



Firma del Experto

 <b>UCV</b> UNIVERSIDAD CÉSAR VALLEJO	<b>VALIDACIÓN DE INSTRUMENTO</b>
<b>Título de tesis:</b>	Unified Threat Management (UTM) para la gestión de los servicios de seguridad basado en COBIT 5 en la empresa Rem Systems S.A.C.
<b>Autor:</b>	Godoy Fuentes, Luis Arnaldo
<b>Nombre del instrumento de evaluación:</b>	Ficha de Registro
<b>Indicador:</b>	Número de incidentes en dispositivos de usuario final
<b>DATOS DEL EXPERTO</b>	
<b>Apellidos y Nombres:</b>	Sinti Zárate, July Tatiana
<b>Título y/o Grado:</b>	Magister
<b>Fecha:</b>	08/04/2021

INDICADORES	CRITERIO	DEFICIENTE 1% - 20%	REGULAR 21% - 40%	BUENO 41% - 60%	MUY BUENO 61% - 80%	EXCELENTE 81% - 100%
Claridad	Está formado por lenguaje apropiado					90%
Objetividad	Esta expresado en conducta observable					90%
Actualidad	Es adecuado al avance de la ciencia y tecnología					85%
Organización	Existe una organización lógica					90%
Suficiencia	Comprende los aspectos de cantidad y calidad					85%
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico					85%
Consistencia	Está basado en aspectos teóricos y científicos					85%
Coherencia	Entre los índices e indicadores					90%
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr					90%
Pertenencia	El instrumento es adecuado al tipo de investigación					90%
<b>PROMEDIO</b>		<b>88%</b>				

**Aplicabilidad:**

- El instrumento puede ser aplicado  
 El instrumento debe ser mejorado



Firma del Experto

FICHA DE REGISTRO			
<b>Investigador:</b>	Godoy Fuentes, Luis Arnaldo	<b>Tipo de Prueba:</b>	PRE-TEST
<b>Empresa Investigada:</b>	Rem Systems S.A.C.		
<b>Motivo de Investigación:</b>	Tesis de Pre-Grado		
<b>Fecha de Inicio:</b>	02/11/2020	<b>Fecha Final:</b>	15/11/2020

Variable	Indicador	Simbología de la Fórmula	Fórmula
Gestión de servicios de Seguridad	Número de vulnerabilidades descubiertas	<p><b>NVD:</b> Número de vulnerabilidades descubiertas.</p> <p><b>NVT:</b> Número de vulnerabilidades tecnológicas.</p> <p><b>NVC:</b> Número de vulnerabilidades de configuración.</p> <p><b>NVS:</b> Número de vulnerabilidades de política de seguridad.</p>	$NVD = NVT + NVC + NVS$

Item	Fecha	NVT	NVC	NVS	NVD
1	02-11-2020	37	24	17	78
2	03-11-2020	52	28	14	94
3	04-11-2020	34	19	20	73
4	05-11-2020	43	30	18	91
5	06-11-2020	57	17	13	87
6	07-11-2020	48	22	10	80
7	08-11-2020	26	11	6	43
8	09-11-2020	64	25	10	99
9	10-11-2020	51	18	12	81
10	11-11-2020	39	31	26	96
11	12-11-2020	43	29	17	89
12	13-11-2020	55	23	14	92
13	14-11-2020	71	33	10	114
14	15-11-2020	30	13	4	47
<b>Σ (NVD)</b>					1164
<b>Promedio:</b>					83.14



FICHA DE REGISTRO			
<b>Investigador:</b>	Godoy Fuentes, Luis Arnaldo	<b>Tipo de Prueba:</b>	RE-TEST
<b>Empresa Investigada:</b>	Rem Systems S.A.C.		
<b>Motivo de Investigación:</b>	Tesis de Pre-Grado		
<b>Fecha de Inicio:</b>	07/12/2020	<b>Fecha Final:</b>	20/12/2020

Variable	Indicador	Simbología de la Fórmula	Fórmula
Gestión de servicios de Seguridad	Número de vulnerabilidades descubiertas	<p><b>NVD:</b> Número de vulnerabilidades descubiertas.</p> <p><b>NVT:</b> Número de vulnerabilidades tecnológicas.</p> <p><b>NVC:</b> Número de vulnerabilidades de configuración.</p> <p><b>NVS:</b> Número de vulnerabilidades de política de seguridad.</p>	$NVD = NVT + NVC + NVS$

Item	Fecha	NVT	NVC	NVS	NVD
1	07-12-2020	43	25	14	82
2	08-12-2020	56	23	11	90
3	09-12-2020	39	28	18	85
4	10-12-2020	61	33	8	102
5	11-12-2020	68	35	16	119
6	12-12-2020	54	29	15	98
7	13-12-2020	26	20	11	57
8	14-12-2020	59	31	13	103
9	15-12-2020	95	38	12	145
10	16-12-2020	72	36	15	123
11	17-12-2020	51	40	16	107
12	18-12-2020	87	27	25	139
13	19-12-2020	103	41	13	157
14	20-12-2020	29	15	10	54
<b>Σ (NVD)</b>					1461
<b>Promedio:</b>					104.36



FICHA DE REGISTRO			
<b>Investigador:</b>	Godoy Fuentes, Luis Arnaldo	<b>Tipo de Prueba:</b>	POS-TEST
<b>Empresa Investigada:</b>	Rem Systems S.A.C.		
<b>Motivo de Investigación:</b>	Tesis de Pre-Grado		
<b>Fecha de Inicio:</b>	01/02/2021	<b>Fecha Final:</b>	14/02/2021

Variable	Indicador	Simbología de la Fórmula	Fórmula
Gestión de servicios de Seguridad	Número de vulnerabilidades descubiertas	<p><b>NVD:</b> Número de vulnerabilidades descubiertas.</p> <p><b>NVT:</b> Número de vulnerabilidades tecnológicas.</p> <p><b>NVC:</b> Número de vulnerabilidades de configuración.</p> <p><b>NVS:</b> Número de vulnerabilidades de política de seguridad.</p>	$NVD = NVT + NVC + NVS$

Item	Fecha	NVT	NVC	NVS	NVD
1	01-02-2021	0	1	2	3
2	02-02-2021	0	0	0	0
3	03-02-2021	0	0	1	1
4	04-02-2021	0	0	0	0
5	05-02-2021	0	1	1	2
6	06-02-2021	0	0	0	0
7	07-02-2021	0	0	0	0
8	08-02-2021	0	0	0	0
9	09-02-2021	0	0	4	4
10	10-02-2021	0	1	0	1
11	11-02-2021	0	0	0	0
12	12-02-2021	0	1	0	1
13	13-02-2021	0	2	4	6
14	14-02-2021	0	0	0	0
<b><math>\Sigma</math> (NVD)</b>					18
<b>Promedio:</b>					1.29

<b>FICHA DE REGISTRO</b>			
<b>Investigador:</b>	Godoy Fuentes, Luis Arnaldo	<b>Tipo de Prueba:</b>	<b>PRE-TEST</b>
<b>Empresa Investigada:</b>	Rem Systems S.A.C.		
<b>Motivo de Investigación:</b>	Tesis de Pre-Grado		
<b>Fecha de Inicio:</b>	02/11/2020	<b>Fecha Final:</b>	15/11/2020

<b>Variable</b>	<b>Indicador</b>	<b>Simbología de la Fórmula</b>	<b>Fórmula</b>
Gestión de servicios de Seguridad	Número de incidentes en dispositivos de usuario final	<b>NIF:</b> Número de incidentes en dispositivos de usuario final <b>DSK:</b> Desktop <b>LAP:</b> Laptops <b>WRK:</b> Workstation	<b>NIF = DSK + LAP + WRK</b>

<b>Item</b>	<b>Fecha</b>	<b>DSK</b>	<b>LAP</b>	<b>WRK</b>	<b>NIF</b>
1	02-11-2020	244	8	2	254
2	03-11-2020	260	3	0	263
3	04-11-2020	269	7	0	276
4	05-11-2020	228	1	0	229
5	06-11-2020	206	4	1	211
6	07-11-2020	267	2	0	269
7	08-11-2020	186	0	0	186
8	09-11-2020	299	0	2	301
9	10-11-2020	291	3	0	294
10	11-11-2020	276	1	5	282
11	12-11-2020	297	0	0	297
12	13-11-2020	244	5	3	252
13	14-11-2020	264	15	7	286
14	15-11-2020	140	0	0	140
<b>Σ (NVD)</b>					3540
<b>Promedio:</b>					252.86

FICHA DE REGISTRO			
<b>Investigador:</b>	Godoy Fuentes, Luis Arnaldo	<b>Tipo de Prueba:</b>	RE-TEST
<b>Empresa Investigada:</b>	Rem Systems S.A.C.		
<b>Motivo de Investigación:</b>	Tesis de Pre-Grado		
<b>Fecha de Inicio:</b>	07/12/2020	<b>Fecha Final:</b>	20/12/2020

Variable	Indicador	Simbología de la Fórmula	Fórmula
Gestión de servicios de Seguridad	Número de incidentes en dispositivos de usuario final	<p><b>NIF:</b> Número de incidentes en dispositivos de usuario final</p> <p><b>DSK:</b> Desktop</p> <p><b>LAP:</b> Laptops</p> <p><b>WRK:</b> Workstation</p>	<b>NIF = DSK + LAP + WRK</b>

Item	Fecha	DSK	LAP	WRK	NIF
1	07-12-2020	281	4	2	287
2	08-12-2020	236	7	0	243
3	09-12-2020	284	0	1	285
4	10-12-2020	255	3	0	258
5	11-12-2020	248	1	0	249
6	12-12-2020	276	3	4	283
7	13-12-2020	193	0	1	194
8	14-12-2020	285	2	1	288
9	15-12-2020	288	0	1	289
10	16-12-2020	367	4	0	371
11	17-12-2020	373	8	5	386
12	18-12-2020	362	5	2	369
13	19-12-2020	375	3	0	378
14	20-12-2020	191	0	0	191
<b>Σ (NVD)</b>					4071
<b>Promedio:</b>					290.79

FICHA DE REGISTRO			
<b>Investigador:</b>	Godoy Fuentes, Luis Arnaldo	<b>Tipo de Prueba:</b>	POST-TEST
<b>Empresa Investigada:</b>	Rem Systems S.A.C.		
<b>Motivo de Investigación:</b>	Tesis de Pre-Grado		
<b>Fecha de Inicio:</b>	01/02/2021	<b>Fecha Final:</b>	14/02/2021

Variable	Indicador	Simbología de la Fórmula	Fórmula
Gestión de servicios de Seguridad	Número de incidentes en dispositivos de usuario final	<p><b>NIF:</b> Número de incidentes en dispositivos de usuario final</p> <p><b>DSK:</b> Desktop</p> <p><b>LAP:</b> Laptops</p> <p><b>WRK:</b> Workstation</p>	$NIF = DSK + LAP + WRK$

Item	Fecha	DSK	LAP	WRK	NIF
1	01-02-2021	6	1	0	7
2	02-02-2021	2	0	0	2
3	03-02-2021	7	0	2	9
4	04-02-2021	5	0	0	5
5	05-02-2021	2	0	0	2
6	06-02-2021	0	4	0	4
7	07-02-2021	0	0	0	0
8	08-02-2021	1	0	0	1
9	09-02-2021	4	1	1	6
10	10-02-2021	2	0	0	2
11	11-02-2021	7	0	1	8
12	12-02-2021	4	0	0	4
13	13-02-2021	2	1	0	3
14	14-02-2021	1	0	0	1
<b><math>\Sigma</math> (NVD)</b>					54
<b>Promedio:</b>					3.86

**ANEXO 7: PROCESO DE GESTIÓN DE DSS05 - GESTIONAR LOS SERVICIOS DE SEGURIDAD**



Se utilizaron las métricas relacionadas con la meta del proceso:

- Número de vulnerabilidades descubiertas
- Número de incidentes que impliquen dispositivos de usuario final

DSS05 Gestionar Servicios de Seguridad		Área: Gestión Dominio: Entrega, Servicio y Soporte
<b>Descripción del Proceso</b> Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.		
<b>Declaración del Propósito del Proceso</b> Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.		
<b>El proceso apoya la consecución de un conjunto de principales metas TI:</b>		
Meta TI	Métricas Relacionadas	
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	<ul style="list-style-type: none"> <li>• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación</li> <li>• Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos</li> <li>• Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI</li> <li>• Cobertura de las evaluaciones de conformidad</li> </ul>	
04 Riesgos de negocio relacionados con las TI gestionados	<ul style="list-style-type: none"> <li>• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos</li> <li>• Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos</li> <li>• Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI</li> <li>• Frecuencia de actualización del perfil de riesgo</li> </ul>	
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	<ul style="list-style-type: none"> <li>• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública</li> <li>• Número de servicios de TI con los requisitos de seguridad pendientes</li> <li>• Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados</li> <li>• Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías</li> </ul>	
<b>Objetivos y Métricas del Proceso</b>		
Meta del Proceso	Métricas Relacionadas	
1. La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio.	<ul style="list-style-type: none"> <li>• Número de vulnerabilidades descubiertas</li> <li>• Número de rupturas (<i>breaches</i>) de cortafuegos</li> </ul>	
2. La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida.	<ul style="list-style-type: none"> <li>• Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final</li> <li>• Número de incidentes que impliquen dispositivos de usuario final</li> <li>• Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno</li> </ul>	
3. Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio.	<ul style="list-style-type: none"> <li>• Promedio de tiempo entre los cambios y actualizaciones de cuentas</li> <li>• Número de cuentas (con respecto al número de usuarios/empleados autorizados)</li> </ul>	
4. Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida.	<ul style="list-style-type: none"> <li>• Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno</li> <li>• Clasificación media para las evaluaciones de seguridad física</li> <li>• Número de incidentes relacionados con seguridad física</li> </ul>	
5. La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida.	<ul style="list-style-type: none"> <li>• Número de incidentes relacionados con accesos no autorizados a la información</li> </ul>	

Se aplicó la práctica de gestión: DSS05.02 – Gestionar la seguridad de la red y las conexiones. Así mismo se realizó el despliegue de sus actividades propuestas.

Matriz RACI DSS05																										
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CSO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la Información
<b>DSS05.01</b> Proteger contra software malicioso ( <i>malware</i> ).						R	I				C	A			R	C	C	C	I	R	R		I	R		
<b>DSS05.02</b> Gestionar la seguridad de la red y las conexiones.						I					C	A				C	C	C	I	R	R		I	R		
<b>DSS05.03</b> Gestionar la seguridad de los puestos de usuario final.						I					C	A				C	C	C	I	R	R		I	R		
<b>DSS05.04</b> Gestionar la identidad del usuario y el acceso lógico.						R					C	A			I	C	C	C	I	C	R		I	R		C
<b>DSS05.05</b> Gestionar el acceso físico a los activos de TI.						I					C	A				C	C	C	I	C	R		I	R	I	
<b>DSS05.06</b> Gestionar documentos sensibles y dispositivos de salida.											I					C	C	A			R					
<b>DSS05.07</b> Supervisar la infraestructura para detectar eventos relacionados con la seguridad.				I	C						I	A				C	C	C	I	C	R		I	R	I	I

DSS05 Prácticas, Entradas/Salidas y Actividades del Proceso (cont.)				
Prácticas de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
<b>DSS05.02 Gestionar la seguridad de la red y las conexiones.</b> Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.	APO01.06	Guías de clasificación de la información	Política de seguridad en la conectividad	APO01.04
	APO09.03	ANSs	Resultados de las pruebas de intrusión	MEA02.08
<b>Actividades</b>				
1. Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.				
2. Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.				
3. Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.				
4. Cifrar la información en tránsito de acuerdo con su clasificación.				
5. Aplicar los protocolos de seguridad aprobados a las conexiones de red.				
6. Configurar los equipamientos de red de forma segura.				
7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.				
8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.				
9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.				

## ANEXO 8: CUADRANTE DE GARTNER PARA FIREWALLS DE RED 2020

Para tomar la decisión de elegir la tecnología UTM a implementar en este proyecto de tesis nos hemos basado en el ranking del cuadrante de Gartner:

### Magic Quadrant for Network Firewalls



Source: Gartner (November 2020)

Por ello se tomó la decisión de utilizar la tecnología UTM de Fortinet.



## ANEXO 9: FORTIGATE 500D

**FORTINET**

**FortiGate® 500D**



The Fortinet Enterprise Firewall Solution delivers end-to-end network security with one platform, one network security operating system and unified policy management with a single pane of glass — for **the industry's best protection against the most advanced security threats and targeted attacks.**



### Security Fabric Integration

FortiGate appliances, interconnected with the Fortinet Security Fabric, form the backbone of the Fortinet Enterprise Solution.



**16 Gbps**  
Firewall

**6 Million**  
Concurrent Sessions



**3.5 Gbps**  
IPS



**2.5 Gbps**  
NGFW



**2 Gbps**  
Threat Protection



Multiple GE RJ45 and GE SFP slots



### Deployment Modes

Next Generation Firewall  
Internal Segmentation Firewall



### Hardware Acceleration

SPU NP6 and CP8



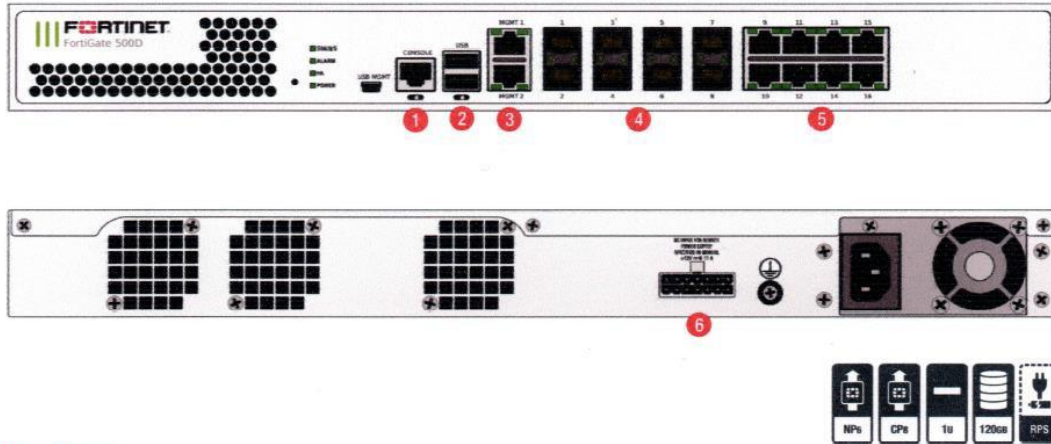
### Third-Party Certifications



DATA SHEET

## HARDWARE

### FortiGate 500D



### Interfaces

- |                                |                     |
|--------------------------------|---------------------|
| 1. Console Port (RJ45)         | 4. 8x GE SFP Slots  |
| 2. 2x USB Ports                | 5. 8x GE RJ45 Ports |
| 3. 2x GE RJ45 Management Ports | 6. FRPS Connector   |

### Powered by SPU



- Custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck

### Network Processor

Fortinet's new, breakthrough SPU NP6 network processor works inline with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency down to 2 microseconds
- VPN, CAPWAP and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload and packet defragmentation
- Traffic shaping and priority queuing

### Content Processor

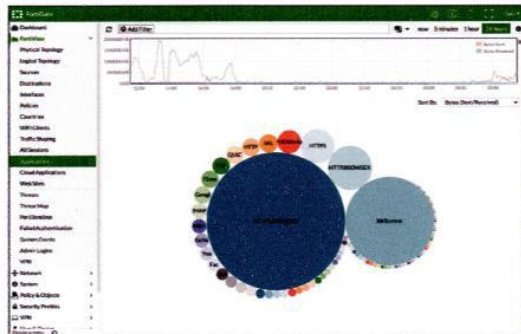
The SPU CP8 content processor works outside of the direct flow of traffic, providing high-speed cryptography and content inspection services including:

- Signature-based content inspection acceleration
- Encryption and decryption offloading

## SOFTWARE

### FortiOS

Control all the security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce operating expenses and save time with a truly consolidated next generation security platform.



- A truly consolidated platform with one OS for all security and networking services for all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives and ICSA validated security and performance.
- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings.
- Detect, contain and block advanced attacks automatically in minutes with integrated advanced threat protection framework.
- Solve your networking needs with extensive routing, switching, WiFi, LAN and WAN capabilities.
- Activate all the SPU-boosted capabilities you need on the fastest firewall platform available.



For more information, please refer to the FortiOS data sheet available at [www.fortinet.com](http://www.fortinet.com)

## SERVICES

### FortiGuard™ Security Services

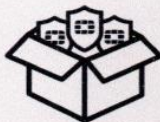
FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations, other network and security vendors, as well as law enforcement agencies:

- **Real-time Updates** — 24x7x365 Global Operations research security intelligence, distributed via Fortinet Distributed Network to all Fortinet platforms.
- **Security Research** — FortiGuard Labs have discovered over 170 unique zero-day vulnerabilities to date, totaling millions of automated signature updates monthly.
- **Validated Security Intelligence** — Based on FortiGuard intelligence, Fortinet's network security platform is tested and validated by the world's leading third-party testing labs and customers globally.

### FortiCare™ Support Services

Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East and Asia, FortiCare offers services to meet the needs of enterprises of all sizes:

- **Enhanced Support** — For customers who need support during local business hours only.
- **Comprehensive Support** — For customers who need around-the-clock mission critical support, including advanced exchange hardware replacement.
- **Advanced Services** — For global or regional customers who need an assigned Technical Account Manager, enhanced service level agreements, extended software support, priority escalation, on-site visits and more.
- **Professional Services** — For customers with more complex security implementations that require architecture and design services, implementation and deployment services, operational services and more.



#### Enterprise Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with the FortiGuard Enterprise Bundle. This bundle contains the full set of FortiGuard security services plus FortiCare service and support offering the most flexibility and broadest range of protection all in one package.



## SPECIFICATIONS

FORTIGATE 500D	
<b>Interfaces and Modules</b>	
GE RJ45 Interfaces	8
GE SFP Slots	8
GE RJ45 Management Ports	2
USB (Client / Server)	1 / 2
RJ45 Console Port	1
Local Storage	120 GB SSD
Included Transceivers	2x SFP (SX 1 GE)
<b>System Performance and Capacity</b>	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	16 / 16 / 16 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Packet per Second)	24 Mpps
Concurrent Sessions (TCP)	6 Million
New Sessions/Second (TCP)	250,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte)	14 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	10,000
SSL-VPN Throughput	400 Mpps
Concurrent SSL-VPN Users (Recommended Maximum)	500
IPS Throughput (HTTP / Enterprise Mix) <sup>1</sup>	5.7 / 3.5 Gbps
SSL Inspection Throughput <sup>2</sup>	3 Gbps
Application Control Throughput <sup>3</sup>	4 Gbps
NGFW Throughput <sup>4</sup>	2.5 Gbps
Threat Protection Throughput <sup>5</sup>	2 Gbps
CAPWAP Throughput <sup>6</sup>	10 Gbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of FortiAPs (Total / Tunnel)	512 / 256
Maximum Number of FortiTokens	1,000
Maximum Number of Registered Endpoints	2,000
High Availability Configurations	Active-Active, Active-Passive, Clustering

FORTIGATE 500D	
<b>Dimensions and Power</b>	
Height x Width x Length (inches)	1.73 x 17 x 12.68
Height x Width x Length (mm)	44 x 432 x 322
Weight	10.8 lbs (4.9 kg)
Form Factor	1 RU
Power Consumption (Average / Maximum)	113 W / 202 W
Power Source	100–240V AC, 60–50Hz
Current (Maximum)	110V/4A, 220V/2A
Heat Dissipation	690 BTU/h
<b>Operating Environment and Certifications</b>	
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	31–168°F (-35–70°C)
Humidity	20–90% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL / cUL, CB
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USG/IPv6

Note: All performance values are "up to" and vary depending on system configuration. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1. 1. IPS performance is measured using 1 Mbyte HTTP and Enterprise Traffic Mix. 2. SSL inspection is measured with IPS enabled and HTTP traffic using TLS v1.2 with AES256-SHA. 3. Application Control performance is measured with 64 Kbytes HTTP traffic. 4. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix. 5. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix. 6. CAPWAP performance is based on 1444 byte UDP packets.

For complete, up-to-date and detailed feature set, please refer to the Administration Handbook and FortiOS Datasheet.

## ORDER INFORMATION

Product	SKU	Description
FortiGate 500D	FG-500D	10x GE RJ45 ports, 8x GE SFP slots, SPU NP6 and CPB hardware accelerated, 120 GB onboard SSD storage.
<b>Optional Accessories</b>		
External Redundant AC Power Supply	FRPS-100	External redundant AC power supply for up to 4 units: FG-300C, FG-310B, FS-348B and FS-448B. Up to 2 units: FG-200B, FG-200D, FG-240D and FG-300D, FG-400D, FG-500D, FG-600D, FHV-500D, FDD-200B, FDD-400B, FDD-600B and FDD-800B.
1 GE SFP LX Transceiver Module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FG-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.



GLOBAL HEADQUARTERS  
Fortinet Inc.  
899 KIFER ROAD  
Sunnyvale, CA 94086  
United States  
Tel: +1.408.235.7700  
www.fortinet.com/sales

EMEA SALES OFFICE  
905 rue Albert Einstein  
06560 Valbonne  
France  
Tel: +33.4.8967.0500

APAC SALES OFFICE  
300 Beach Road 20-01  
The Concourse  
Singapore 199655  
Tel: +65.6395.2788

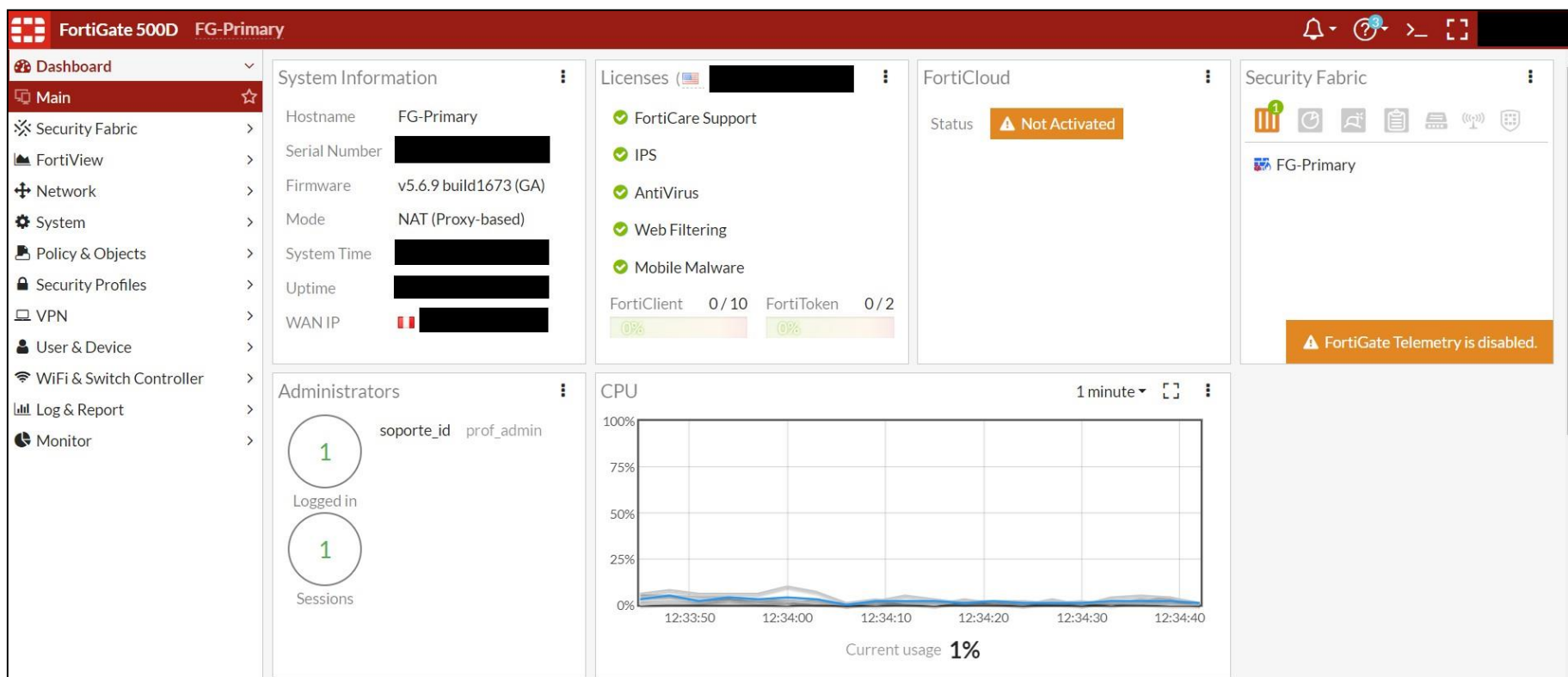
LATIN AMERICA SALES OFFICE  
Sawgrass Lakes Center  
13450 W. Sunrise Blvd., Suite 430  
Sunrise, FL 33323  
United States  
Tel: +1.954.368.9990

Copyright © 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCloud®, and FortiGuard® and certain other marks are registered trademarks of Fortinet, Inc. in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were analyzed in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event shall Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any contracts, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

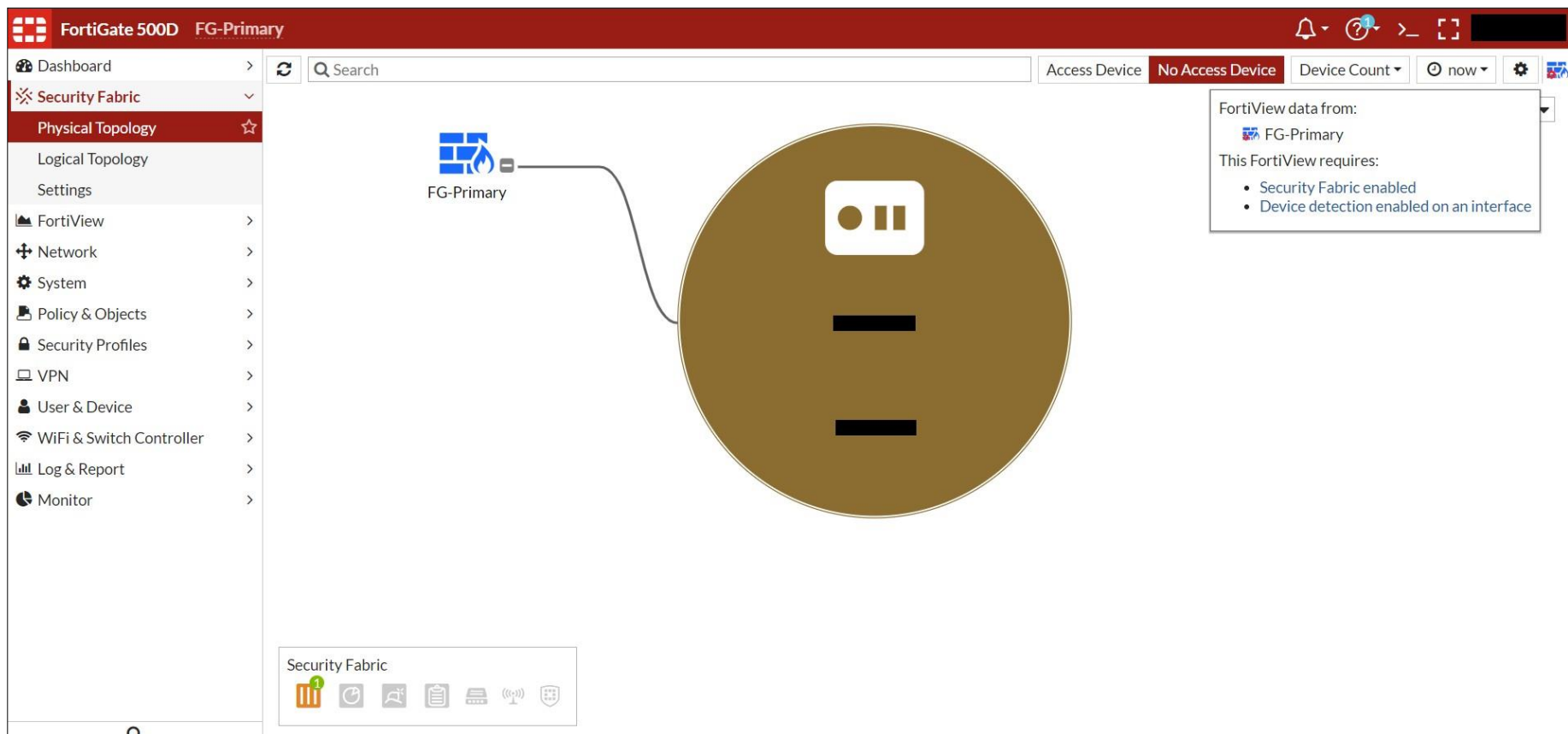
FST-PROD-DS-GT3H

FG-500D-DAT-FB-201704

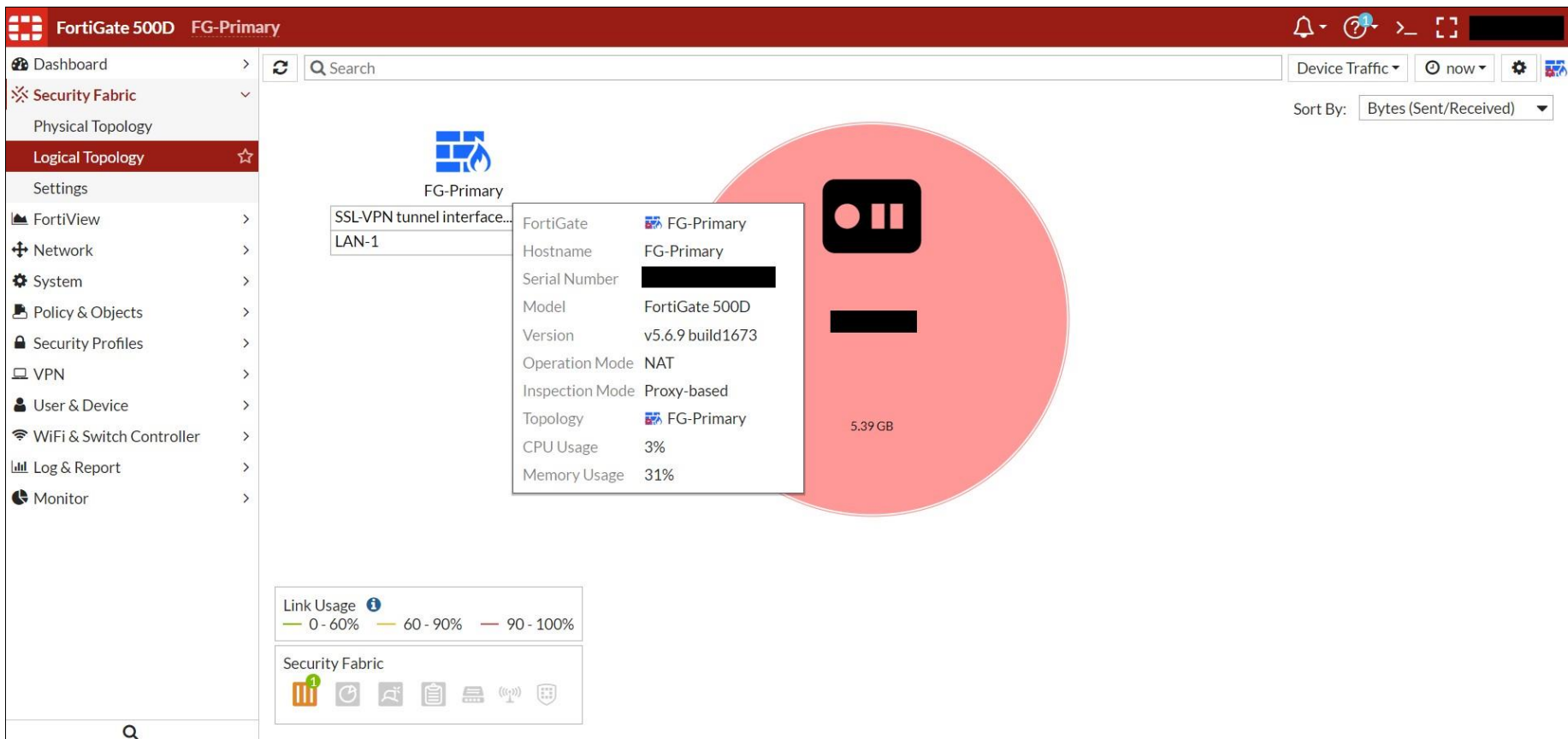
## ANEXO 10: DESPLIEGUE DE FORTIGATE 500D



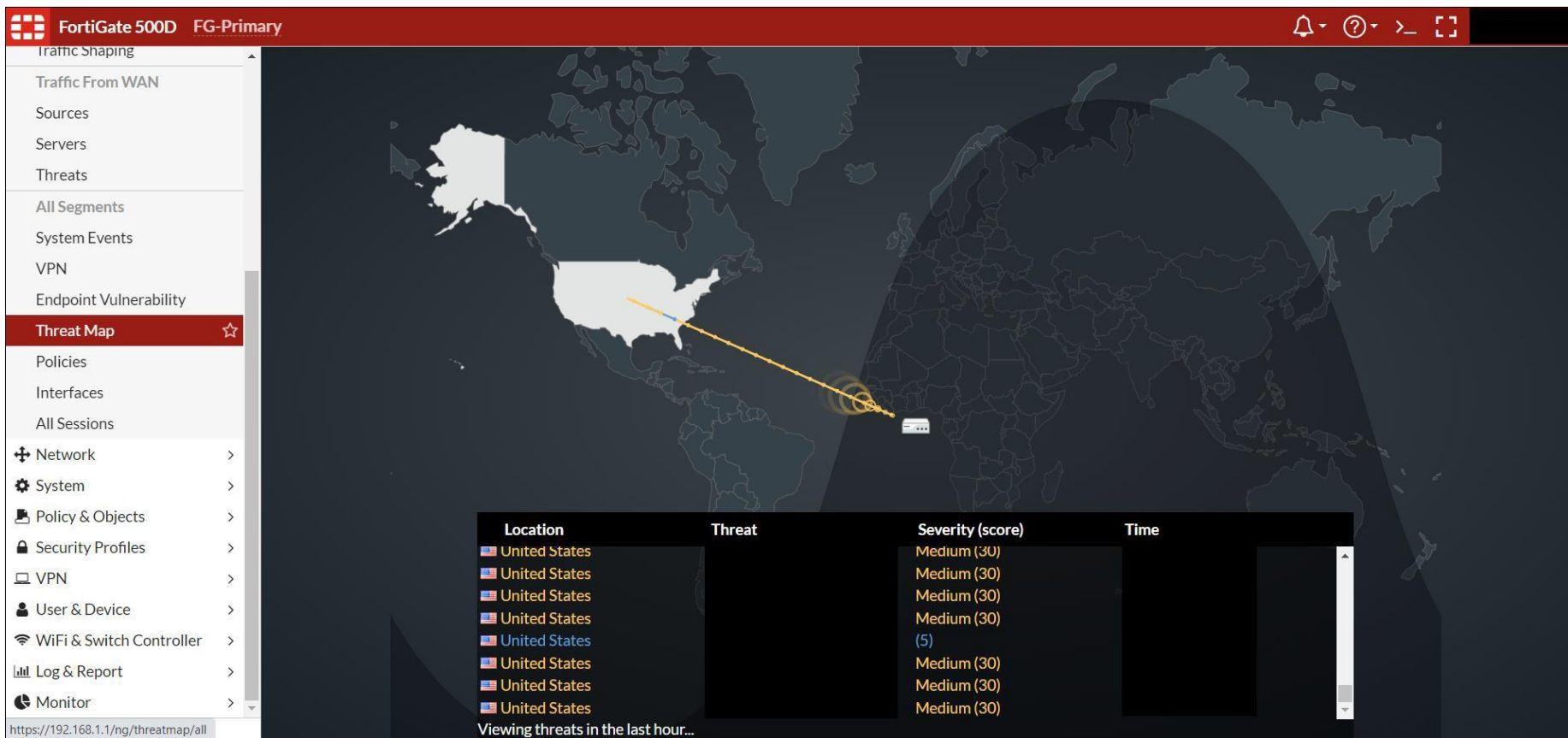
Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.



Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.

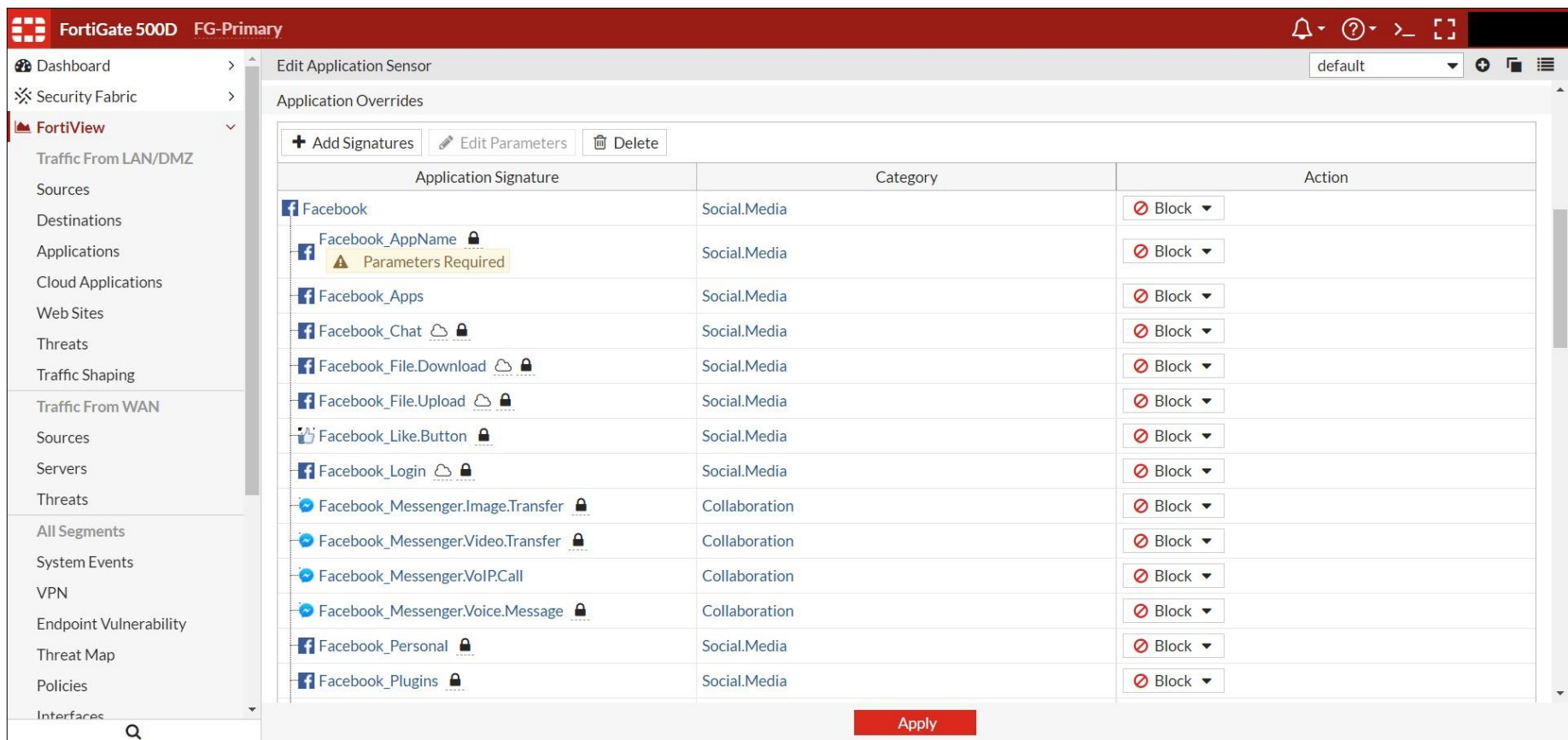


Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.

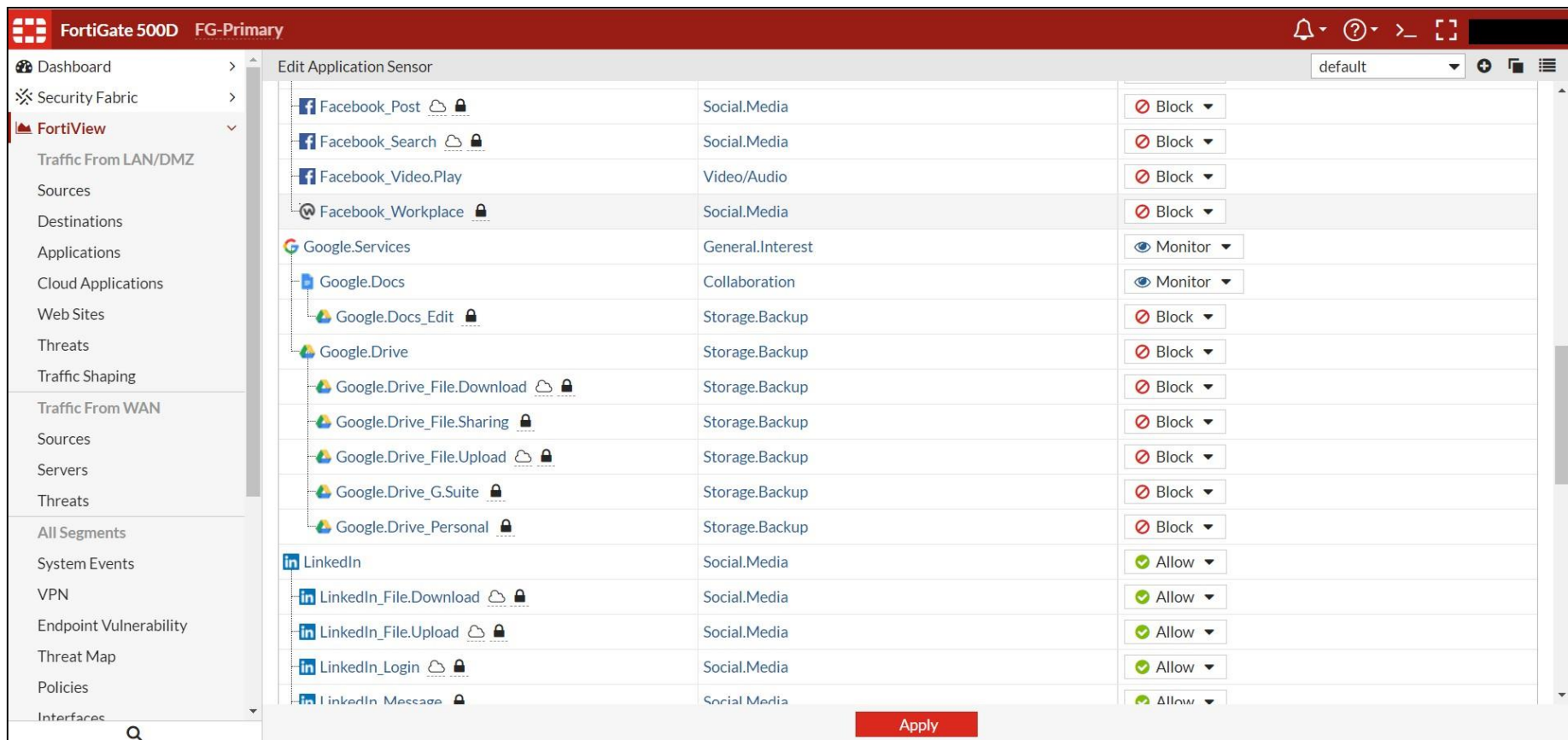


Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.

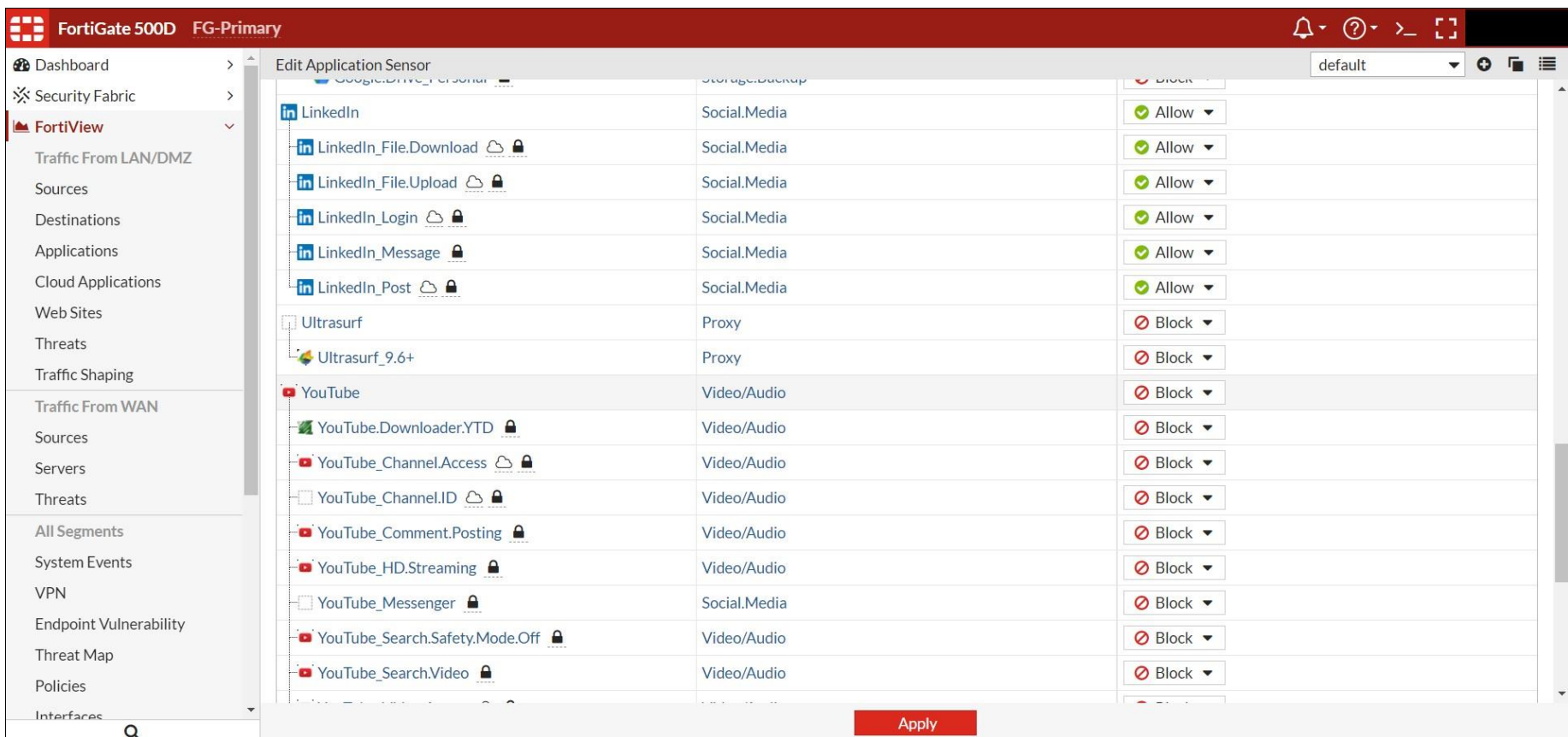




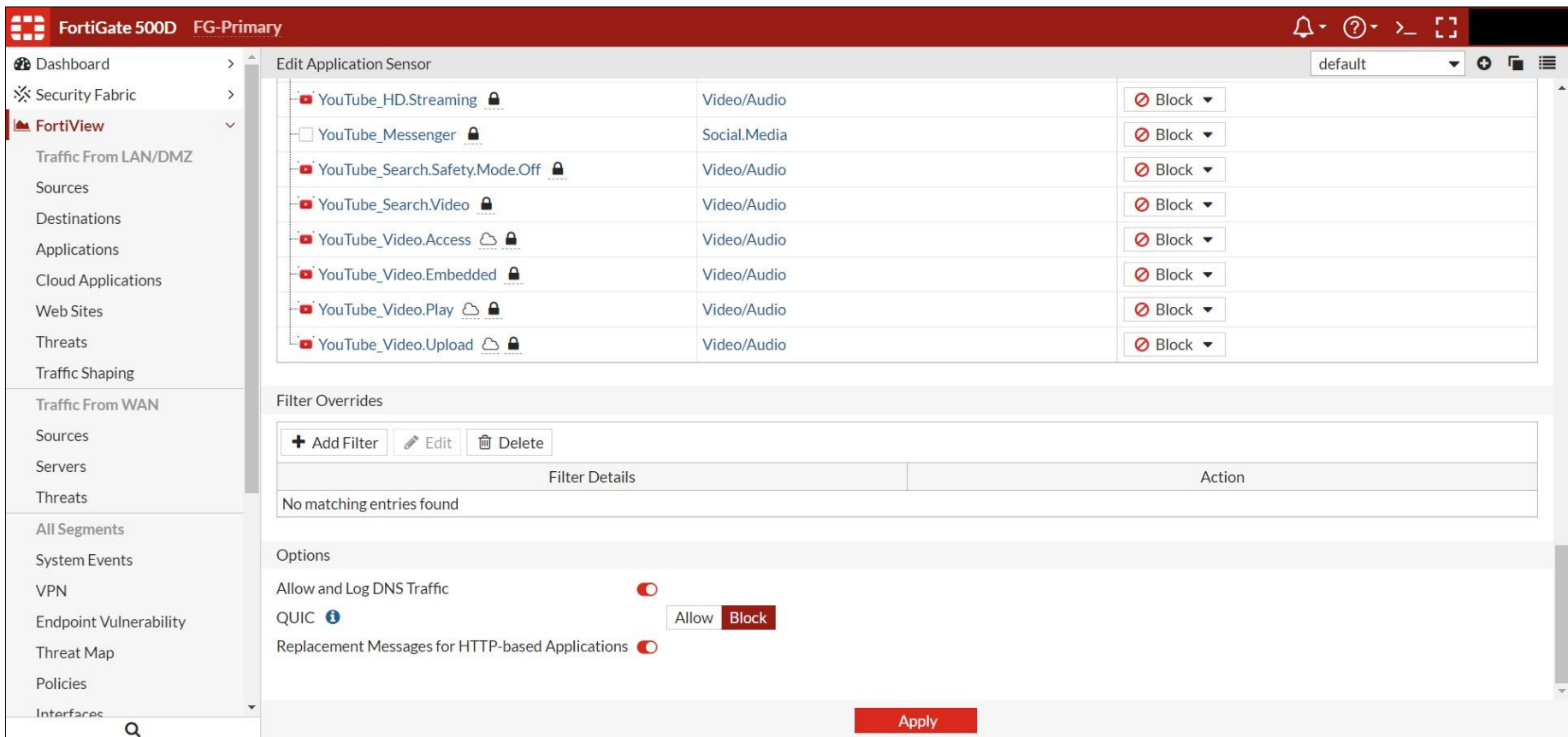
Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.



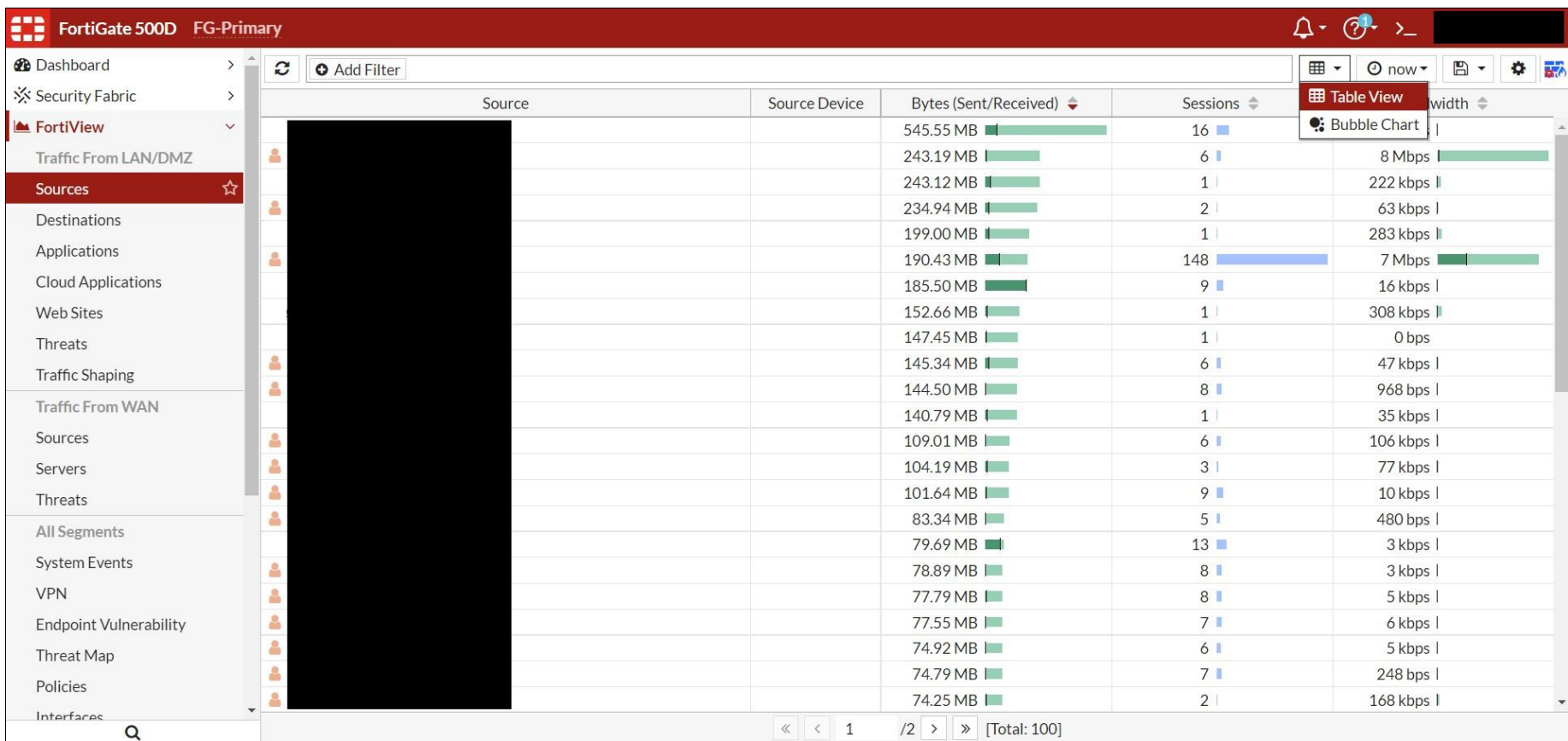
Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.



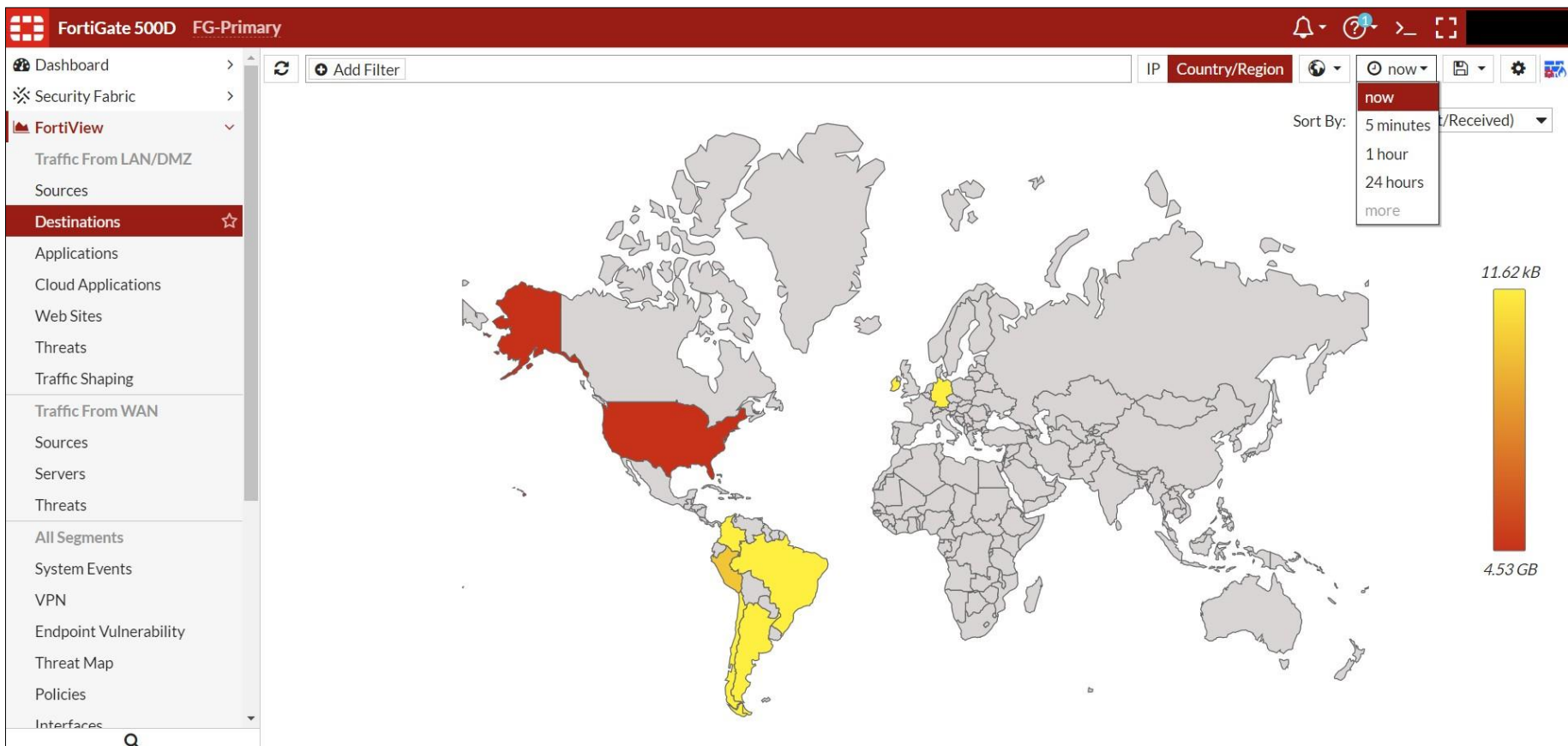
Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.



Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.

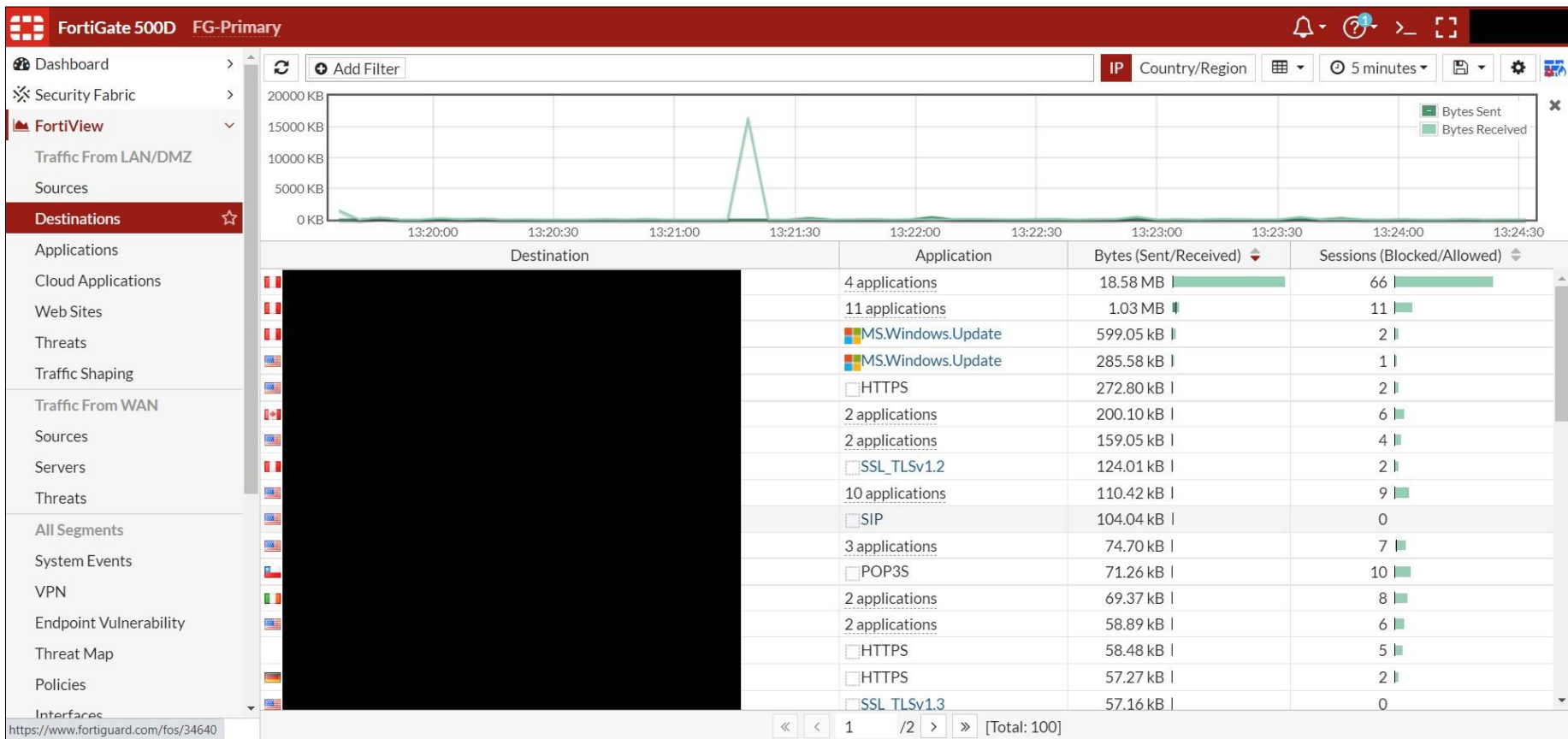


Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.

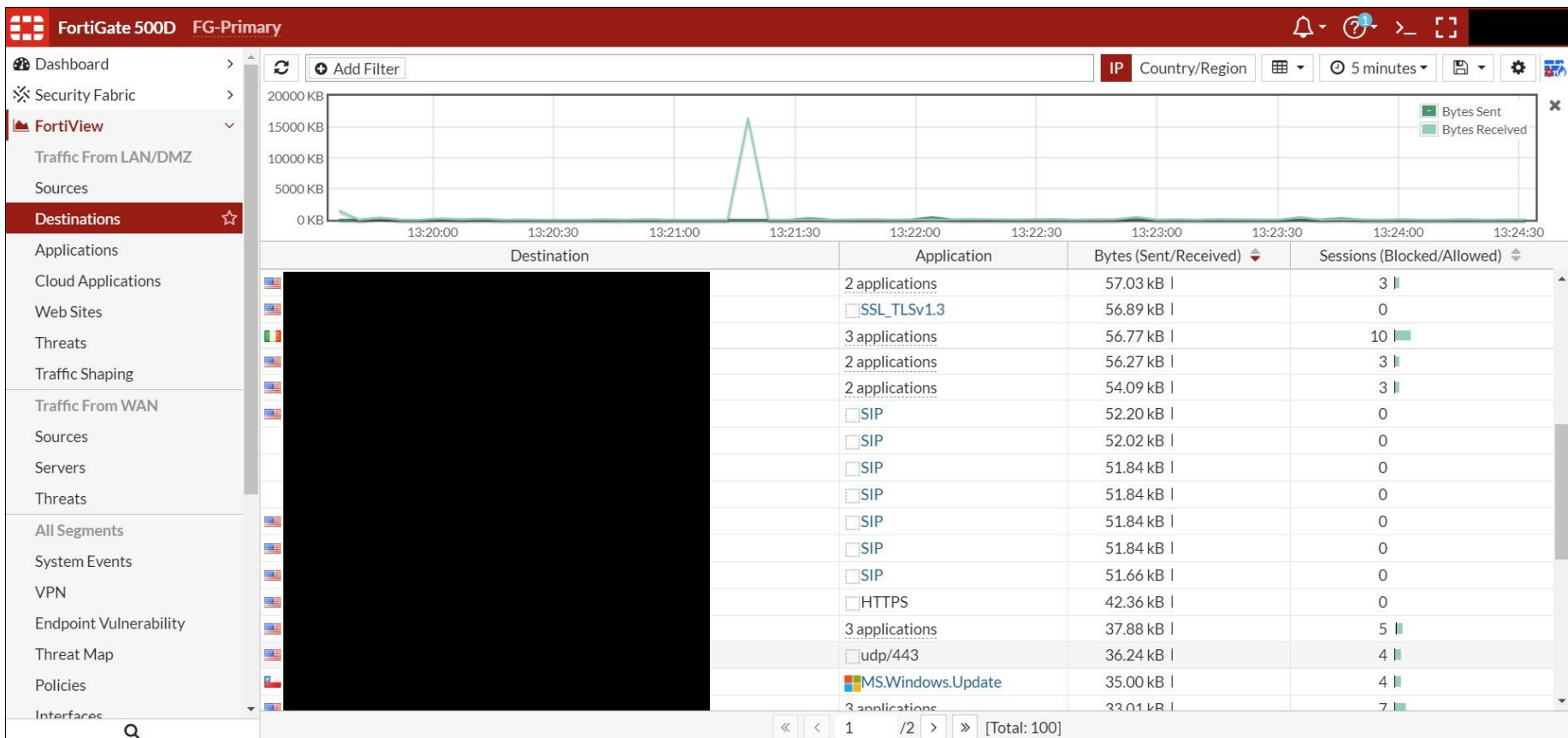


Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.



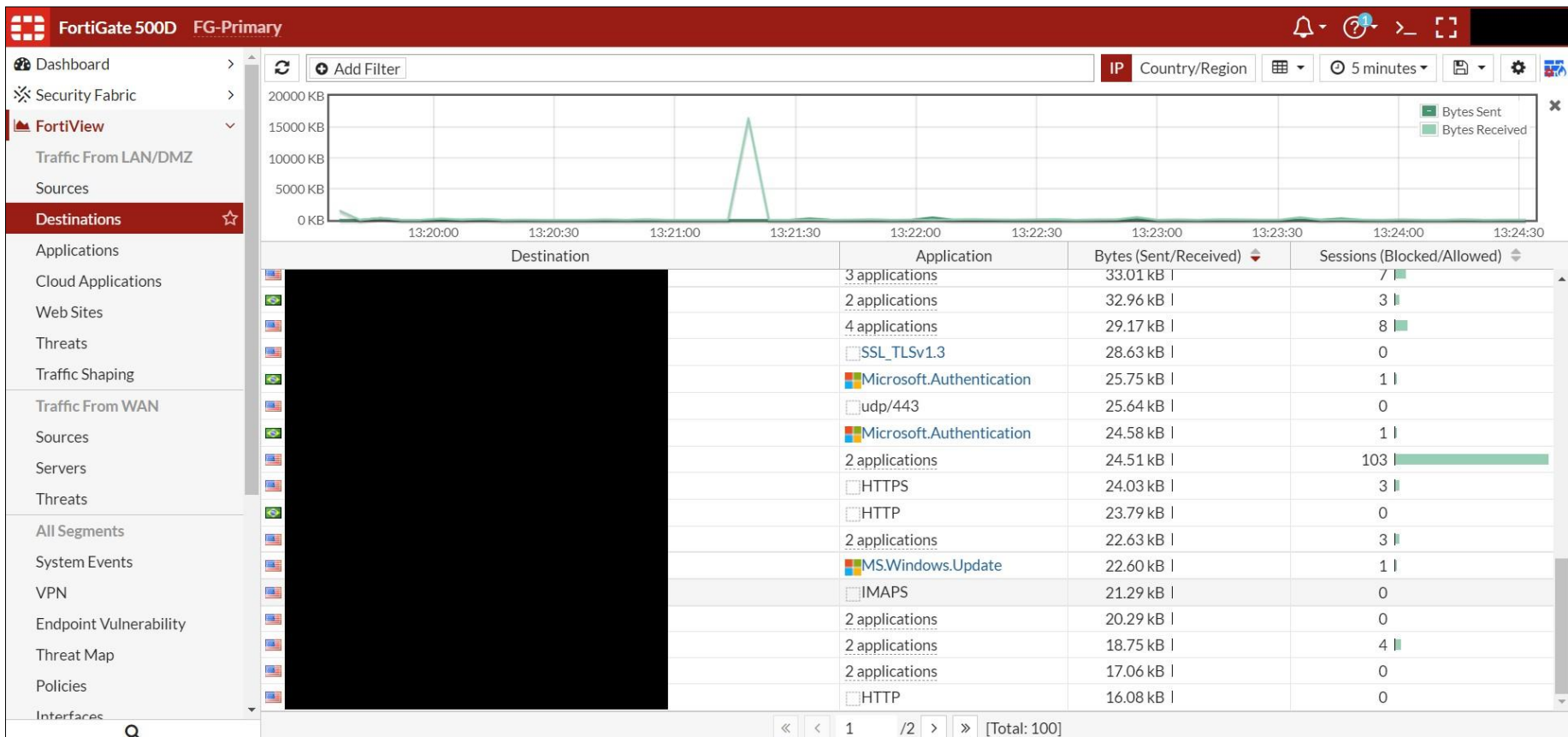


Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.

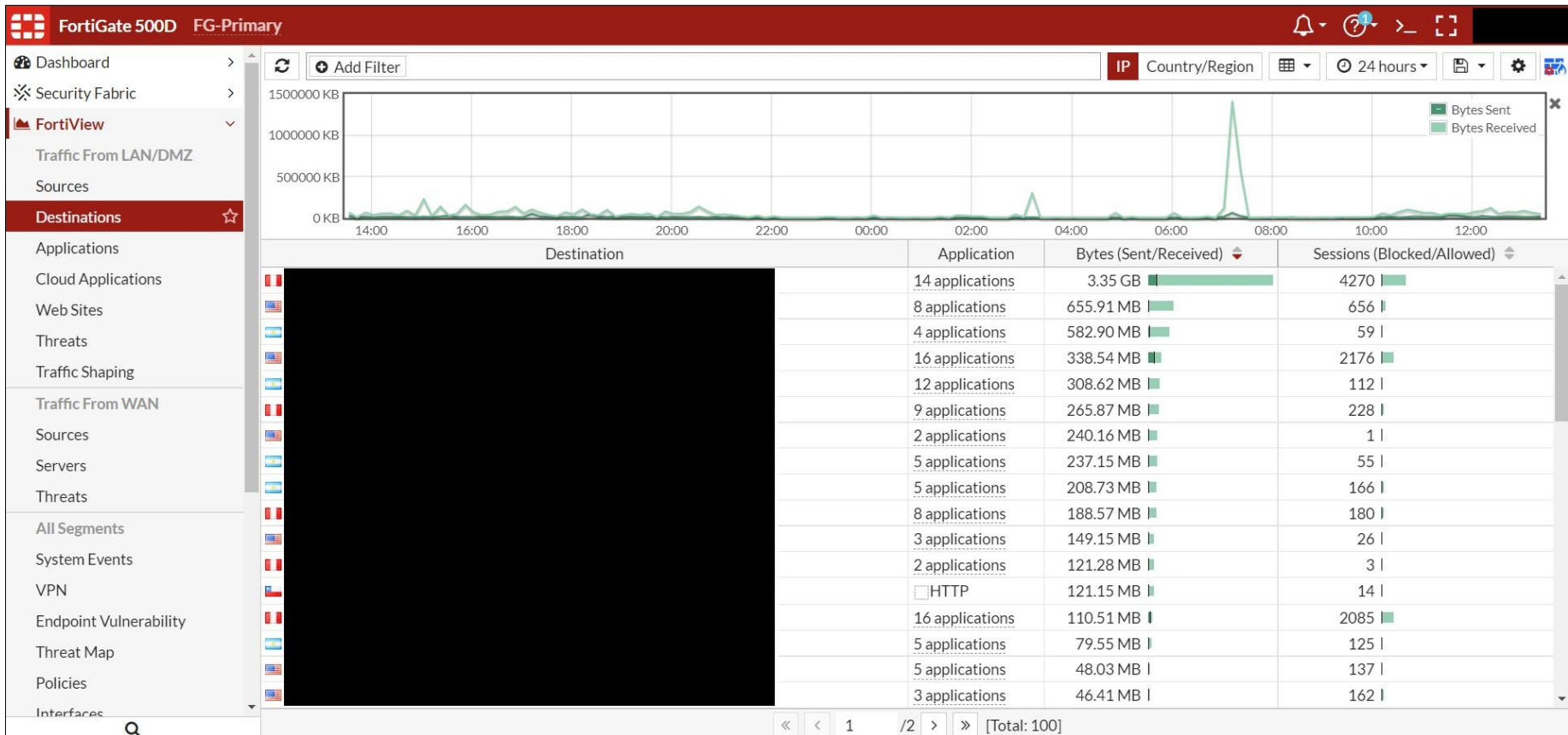


Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.

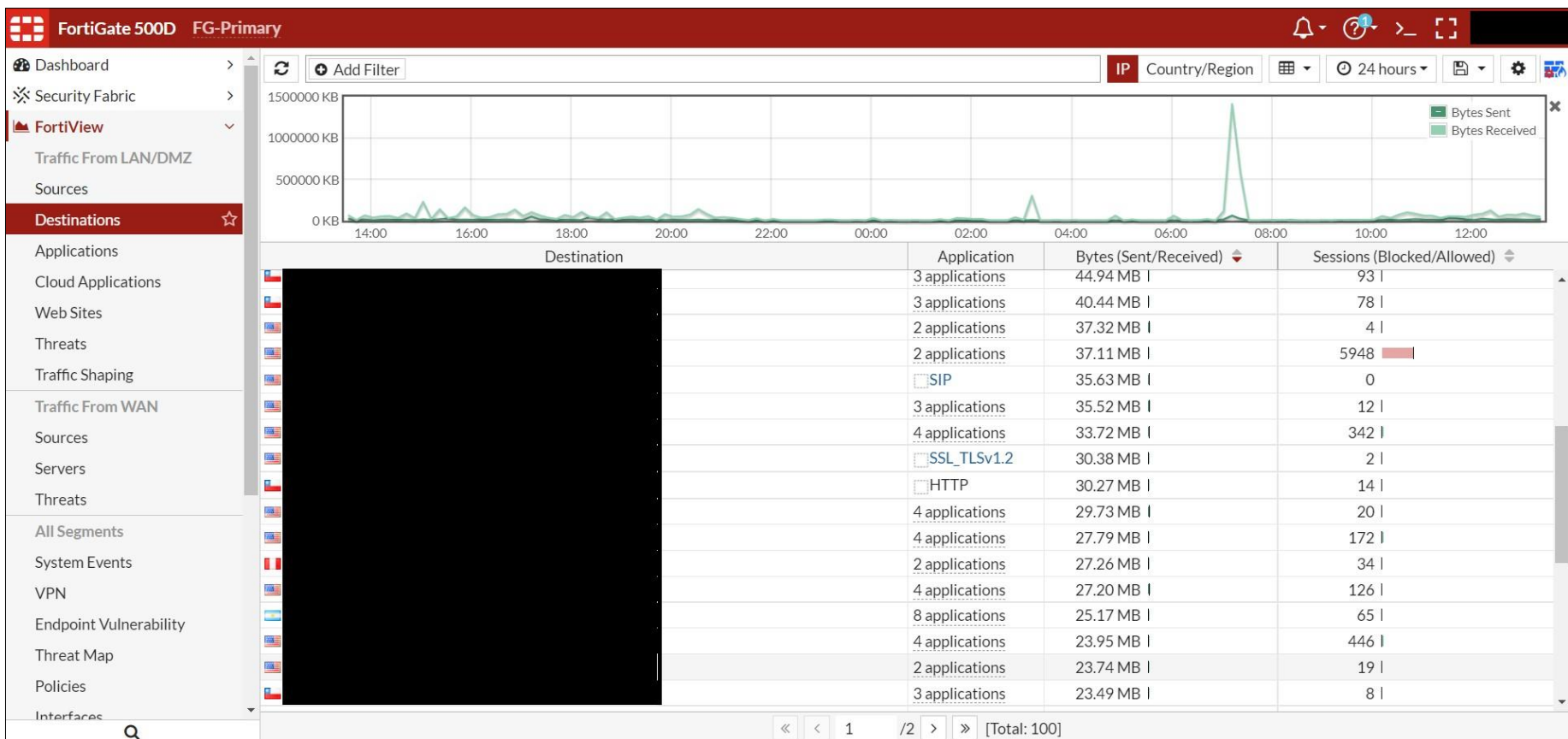




Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.

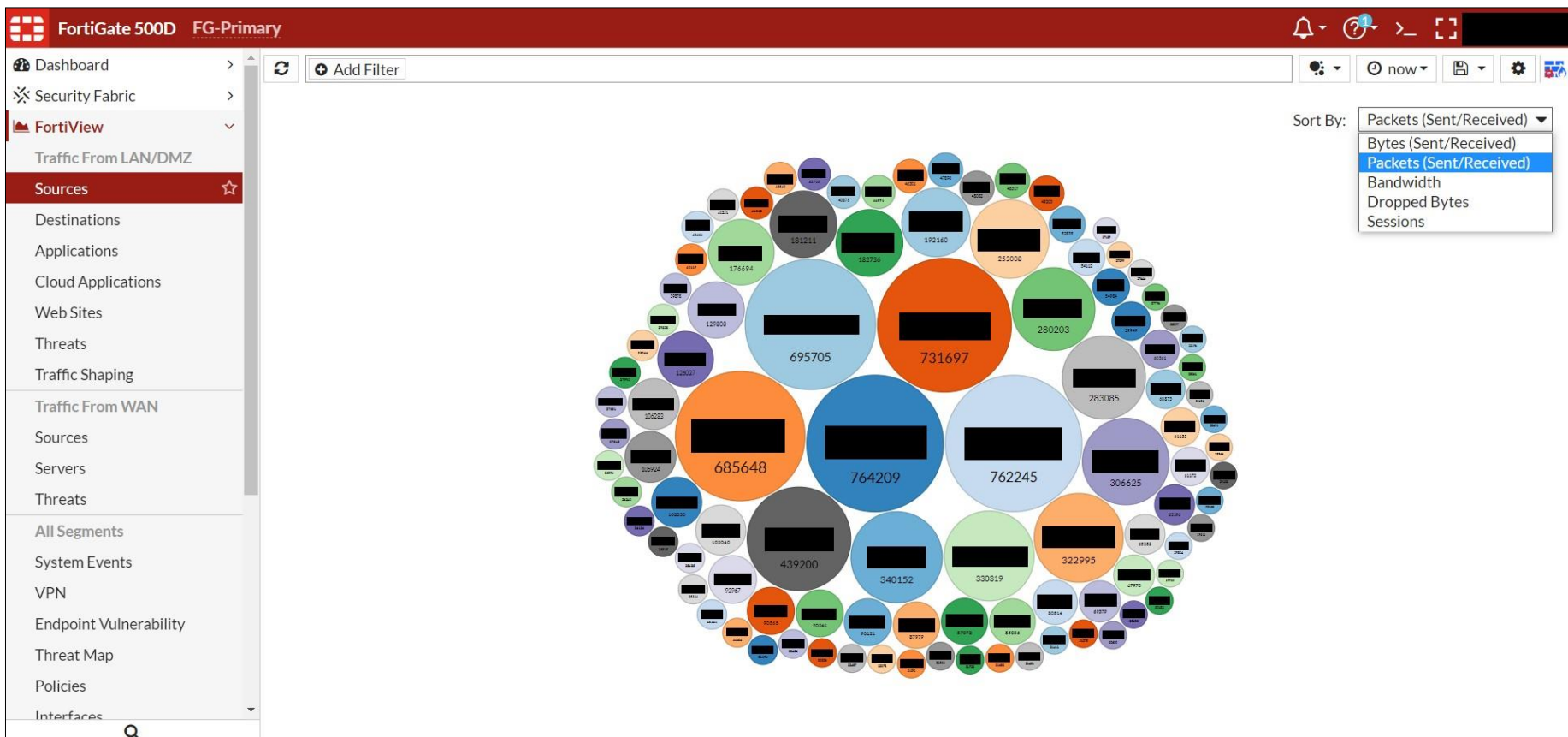


Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.



Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.

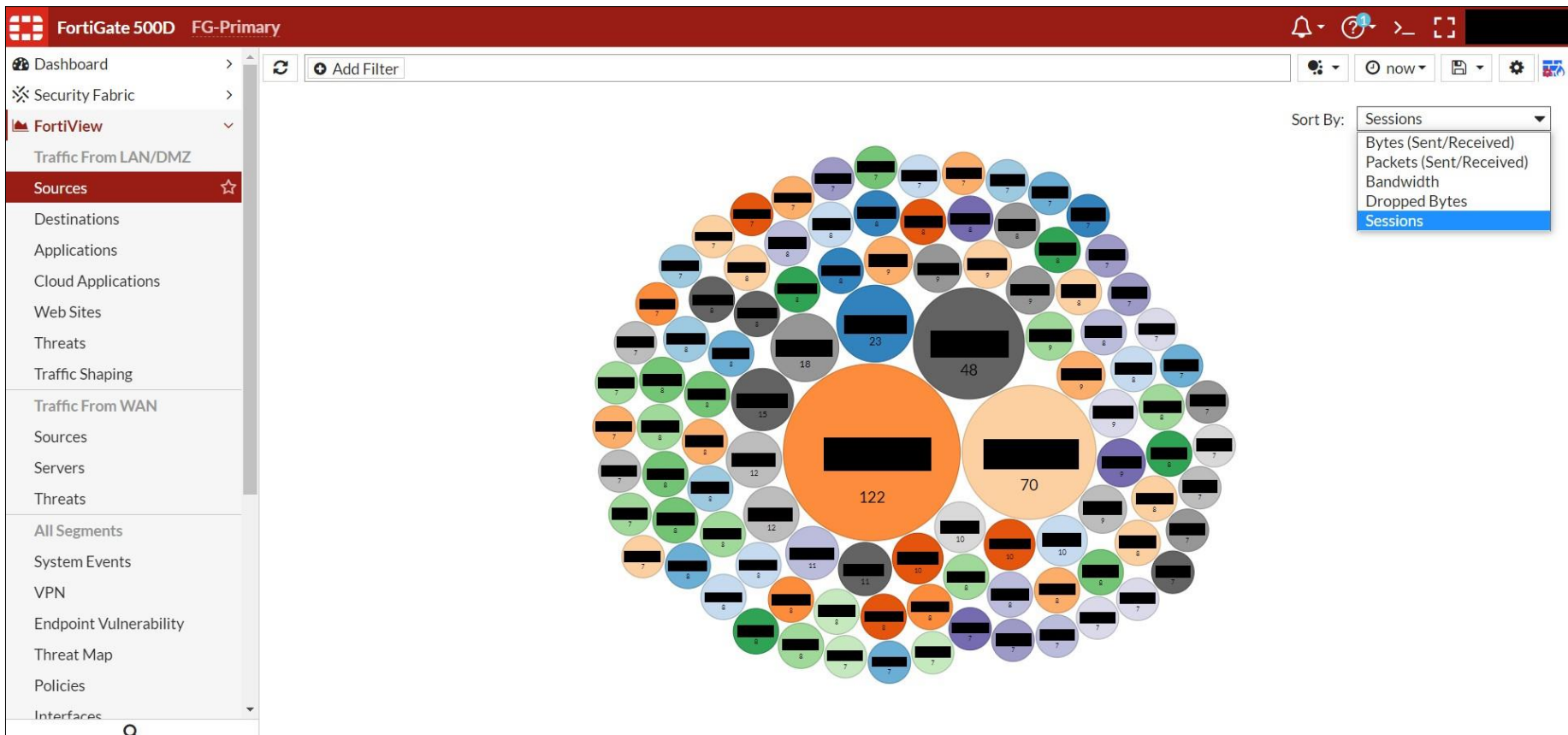




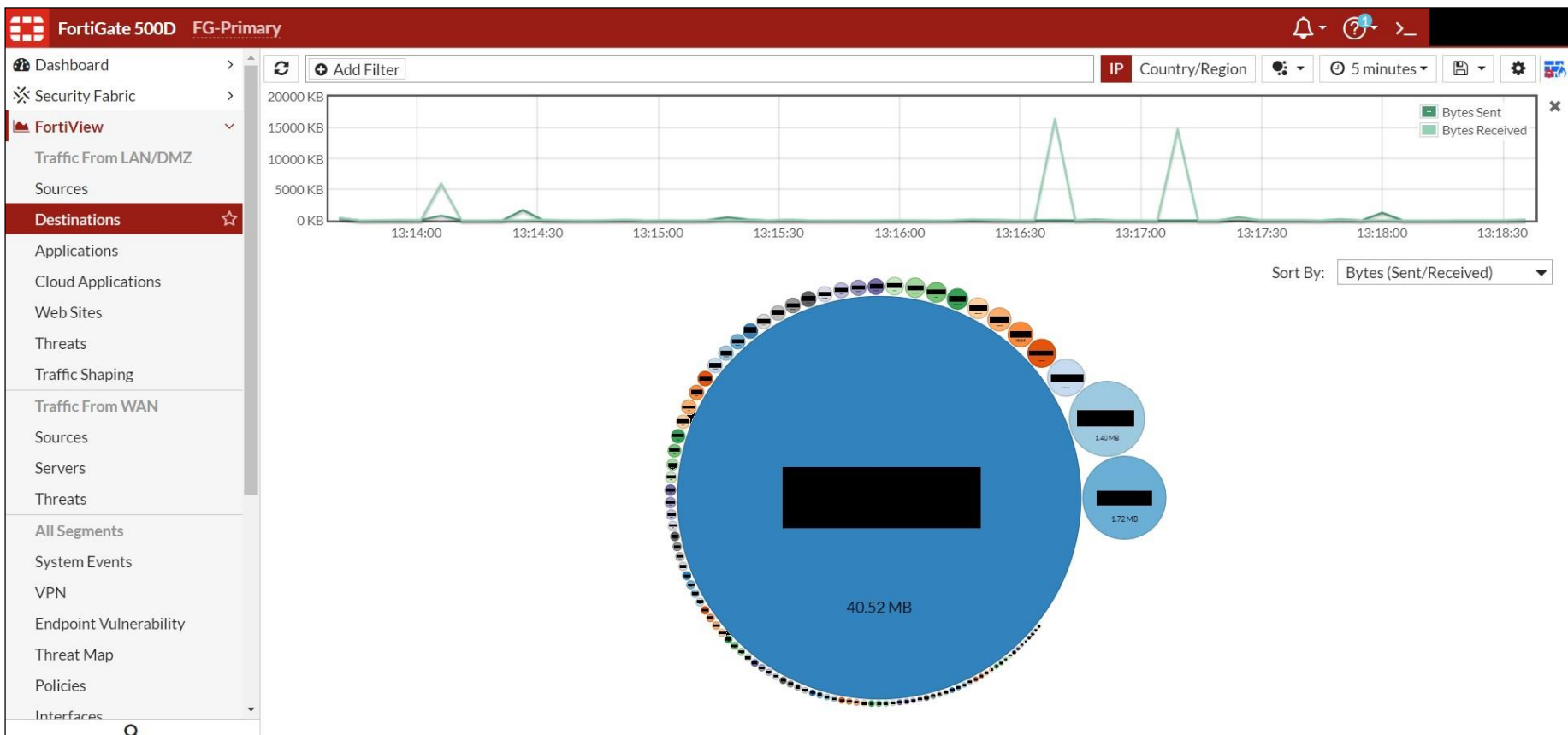
Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.





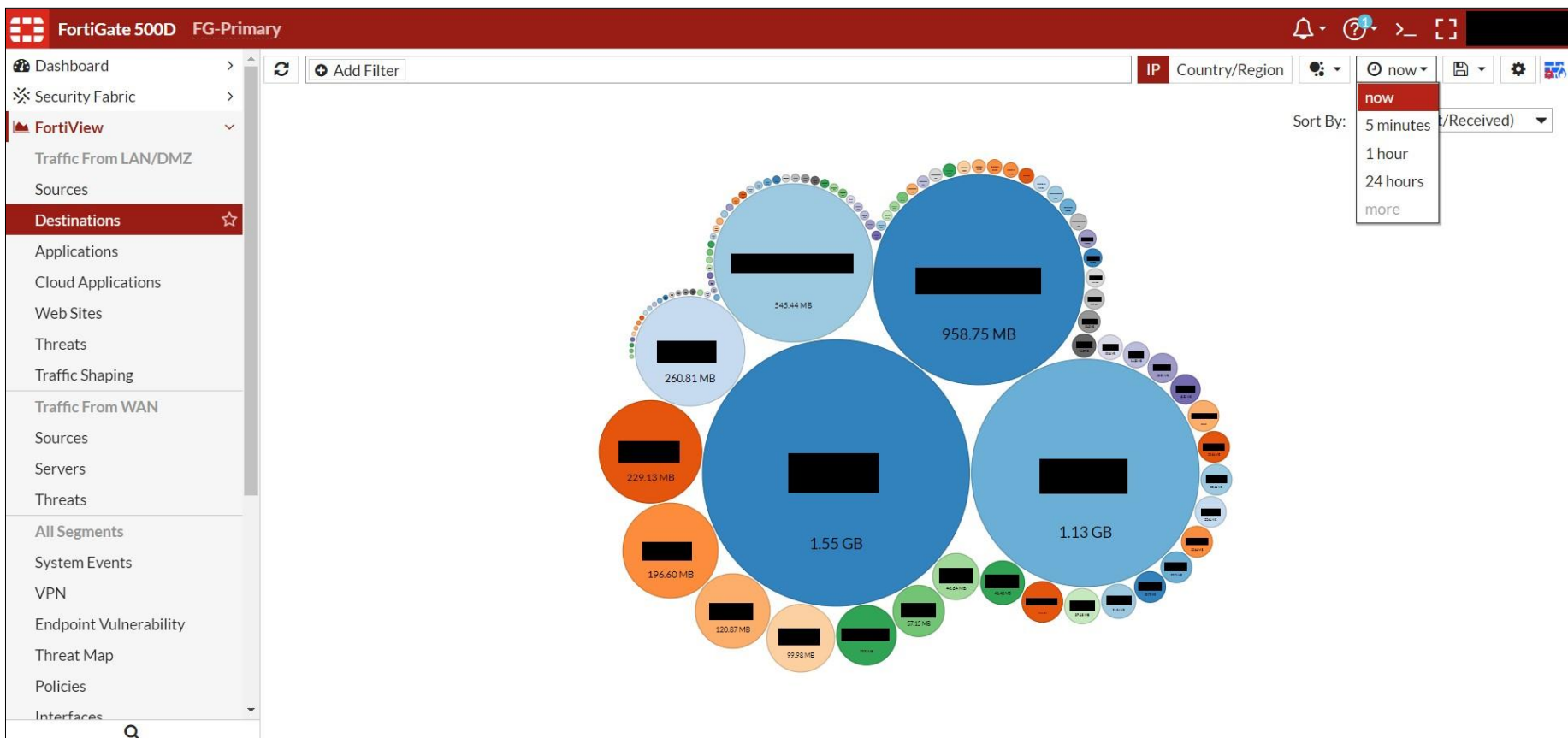


Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.

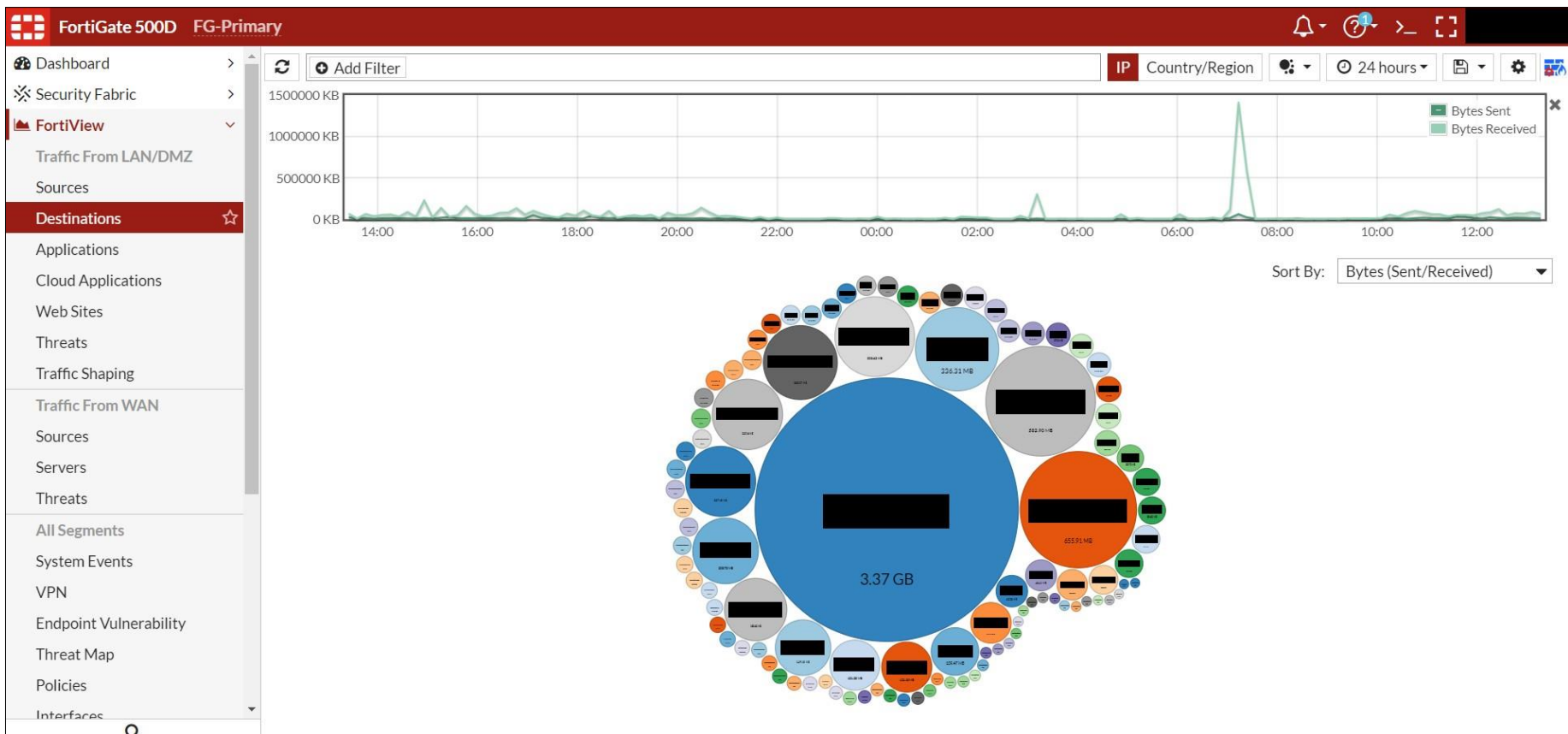


Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.

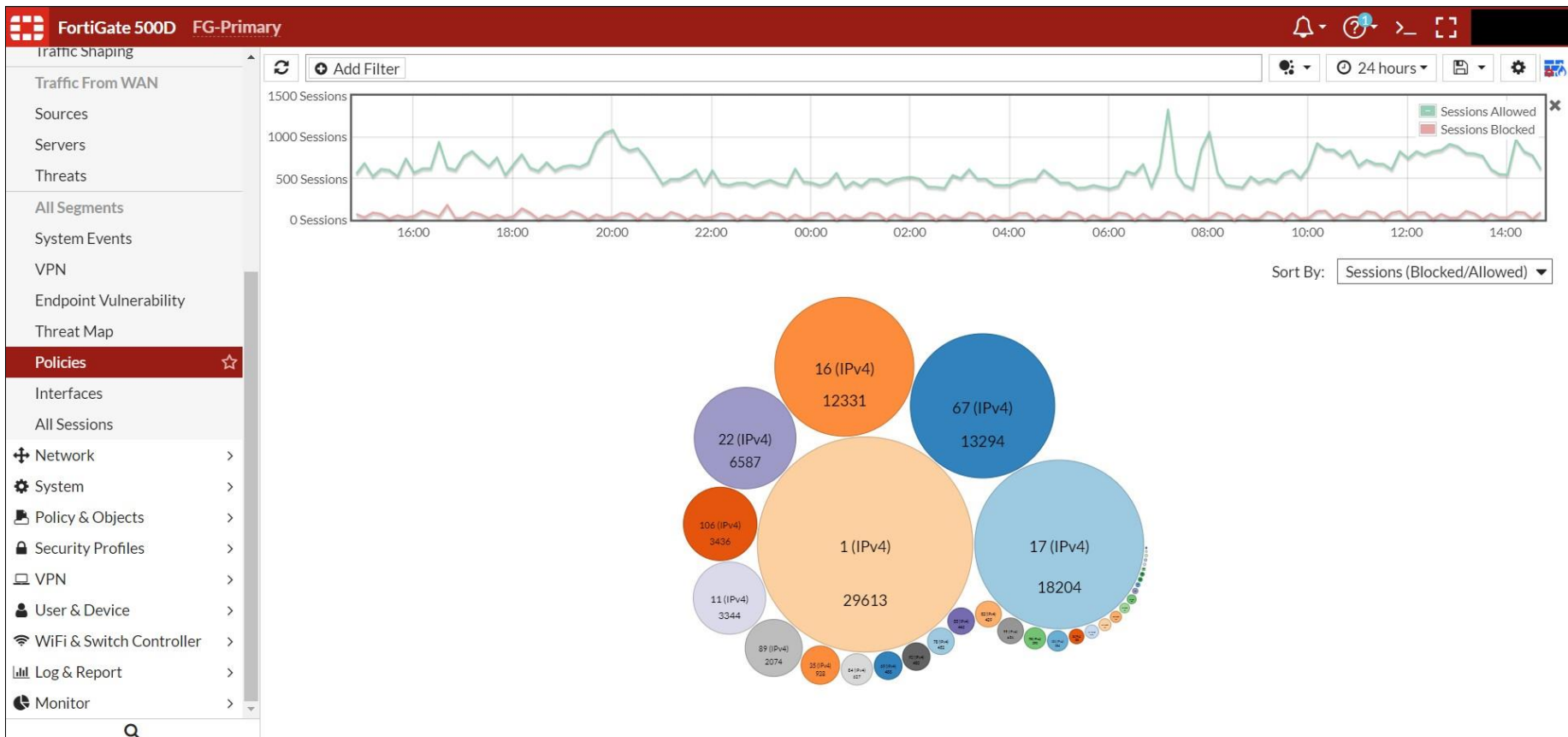




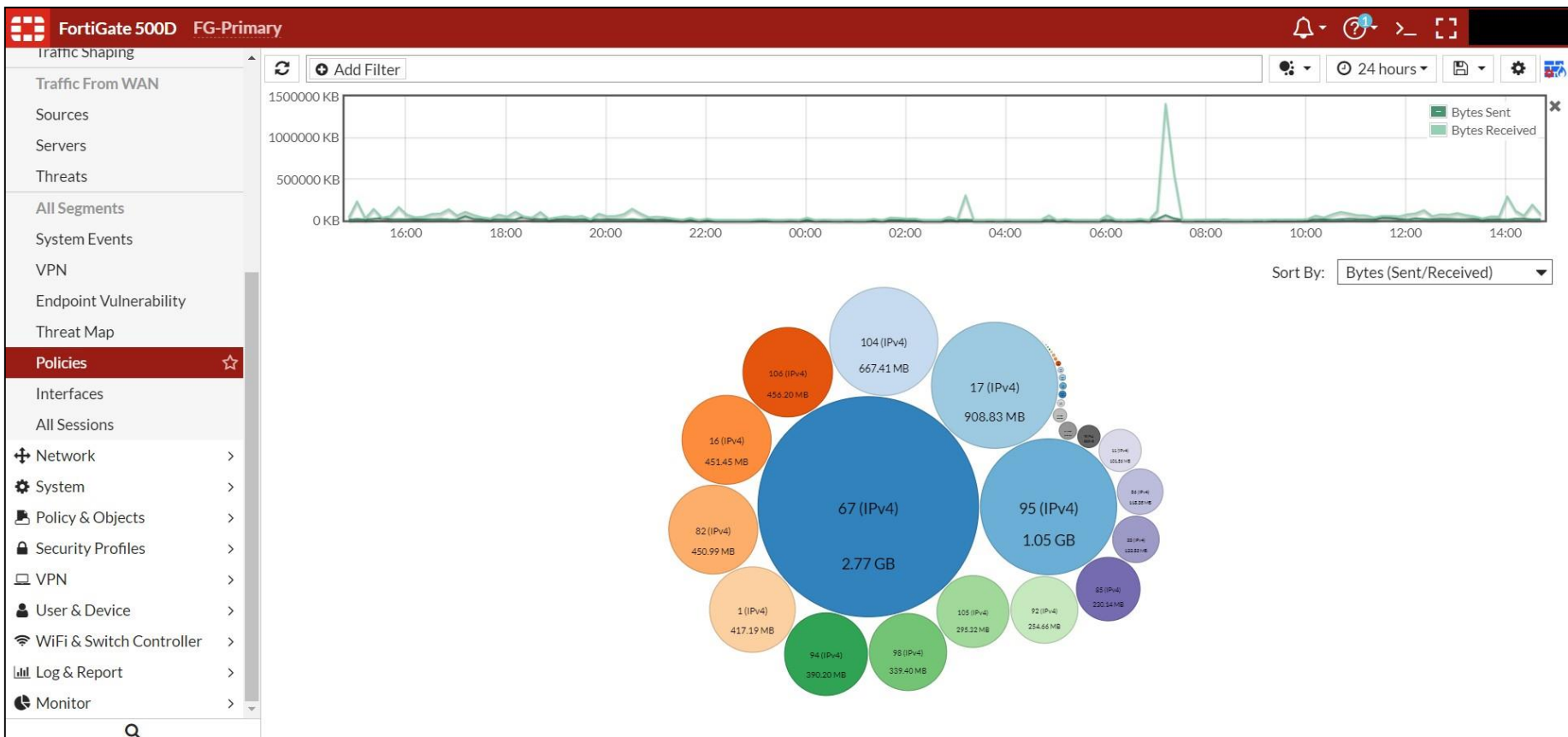
Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.



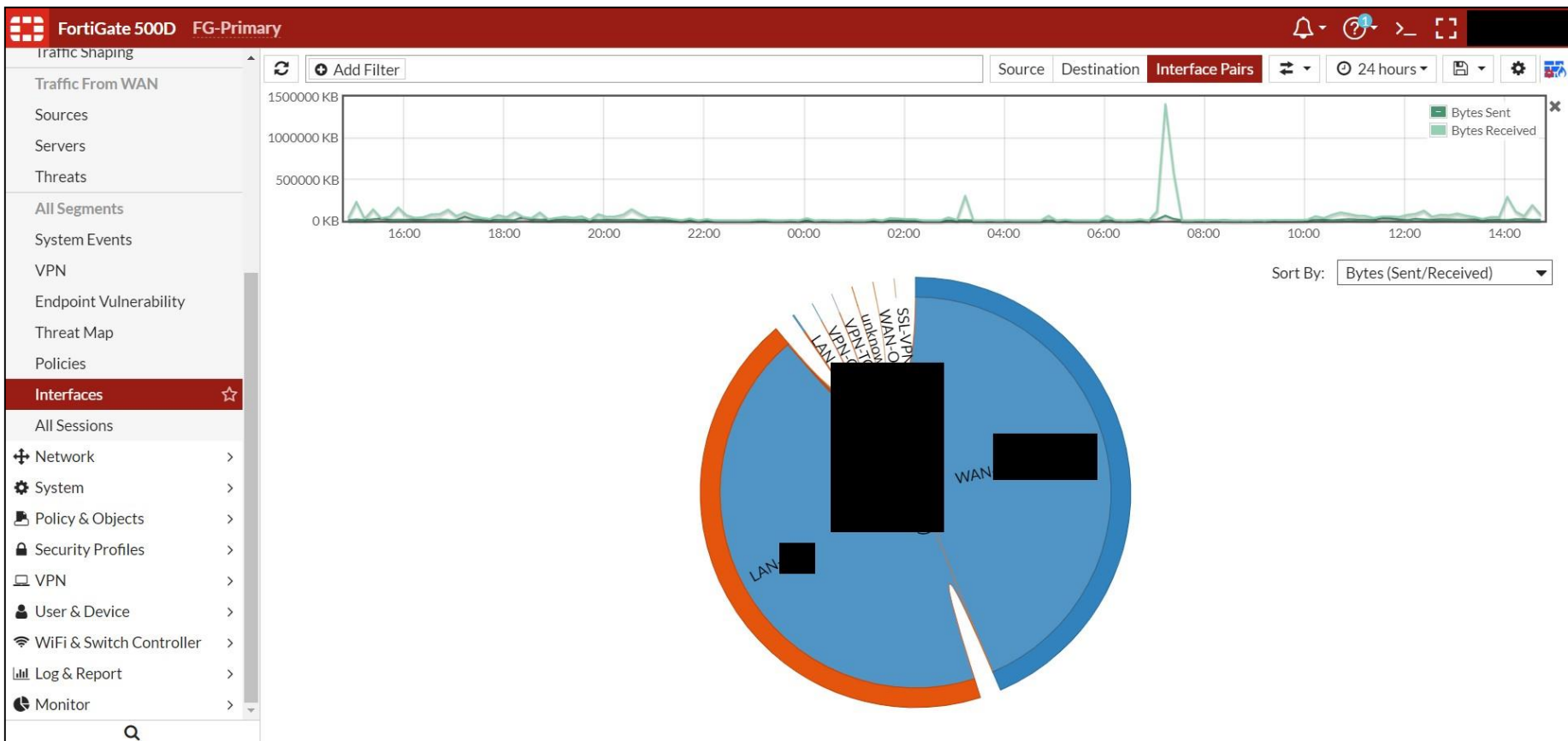
Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.



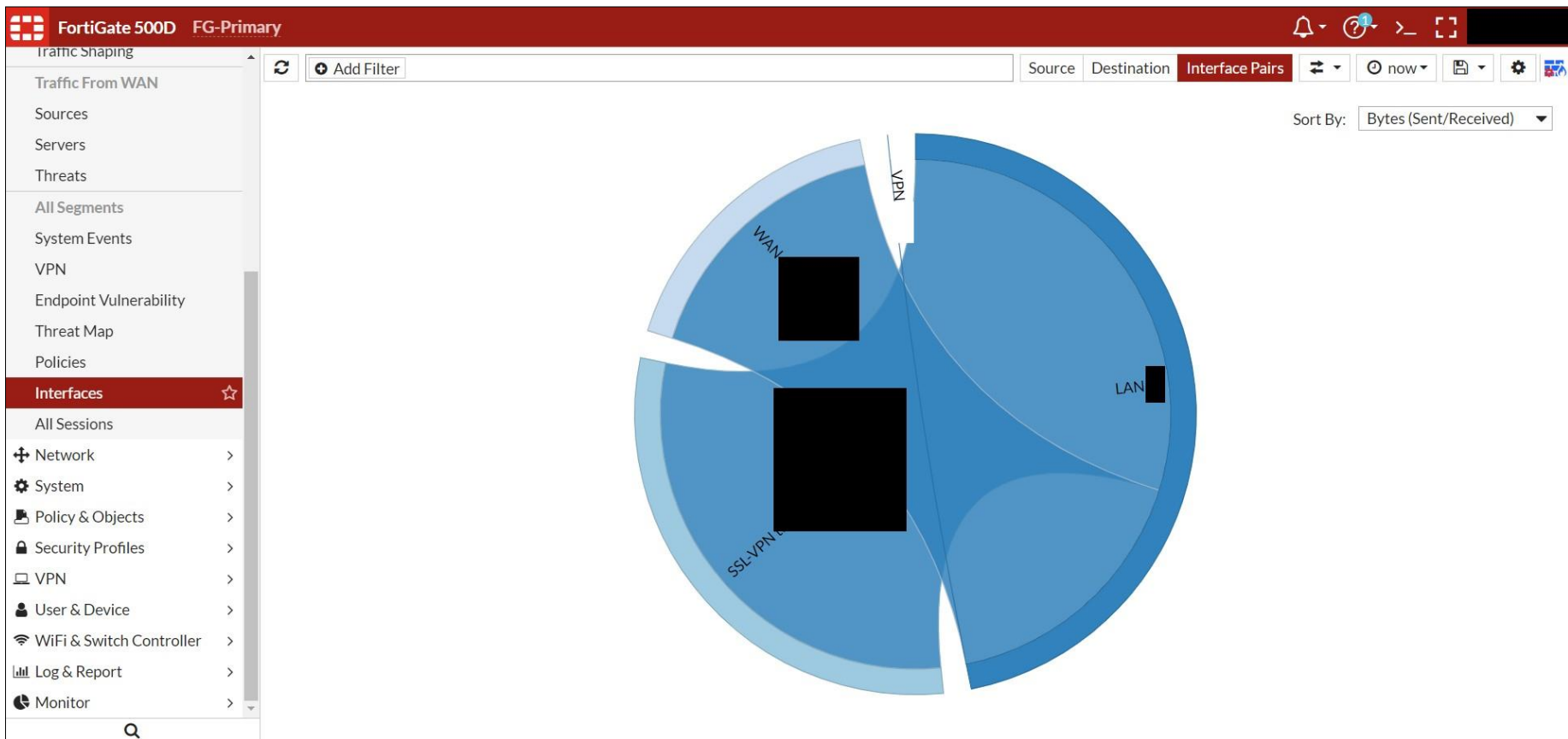
Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.



Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.



Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.



Por razones de estricta confidencialidad de la empresa solo mostraremos algunas interfaces que no impliquen riesgos en la seguridad, como es el caso de la presente imagen donde se ha ocultado algunos datos particulares del despliegue del UTM.

## ANEXO 11: ACTA DE IMPLEMENTACIÓN



### ACTA DE IMPLEMENTACIÓN


**“UNIFIED THREAT MANAGEMENT (UTM) PARA LA GESTIÓN DE LOS SERVICIOS DE SEGURIDAD BASADO EN COBIT 5 EN LA EMPRESA REM SYSTEMS S.A.C.”**

Mediante la presente acta de implementación se confirma y se respalda, que, en base de nuestros requerimientos y necesidades expuestas, se realizó la implementación del proyecto de seguridad informática que lleva como título: **“UNIFIED THREAT MANAGEMENT (UTM) PARA LA GESTIÓN DE LOS SERVICIOS DE SEGURIDAD BASADO EN COBIT 5 EN LA EMPRESA REM SYSTEMS S.A.C.”** realizado por el Sr. **LUIS ARNALDO GODOY FUENTES** con el fin de contribuir de manera óptima y eficiente.

Quedamos agradecidos por el apoyo y contribución de dicha implementación.

Lima, 10 de Marzo del 2021

Atentamente,

  
ADRIAN MARTIN ALCANTARA CORTEZ  
REM SYSTEMS S.A.C.  
GERENTE GENERAL  
Gerente General

Jr. Ernesto Mora 475 Piso 2, San Martín de Porres, Lima – Perú  
Teléfono: (511) 701 – 3625  
[www.remsystems.pe](http://www.remsystems.pe)



## ANEXO 12: INFORME DE IMPLEMENTACIÓN



### INFORME DE IMPLEMENTACIÓN

**“UNIFIED THREAT MANAGEMENT (UTM) PARA LA GESTIÓN DE LOS  
SERVICIOS DE SEGURIDAD BASADO EN COBIT 5 EN LA EMPRESA REM  
SYSTEMS S.A.C.”**

El que suscribe, en representación de la empresa REM SYSTEMS S.A.C. con  
RUC: 20601796881

CONSTA QUE:

La implementación del proyecto de seguridad informática que lleva como título:  
“UNIFIED THREAT MANAGEMENT (UTM) PARA LA GESTIÓN DE LOS  
SERVICIOS DE SEGURIDAD BASADO EN COBIT 5 EN LA EMPRESA REM  
SYSTEMS S.A.C.” realizado por el Sr. LUIS ARNALDO GODOY FUENTES, ha  
ayudado de manera significativa a que los niveles de ciberseguridad se  
optimicen.

La tecnología implementada tiene todos los servicios para brindar una defensa  
efectiva para garantizar la seguridad en todos los puntos de la red, las  
aplicaciones, el data center, el tráfico de internet y los puntos de acceso.

Lima, 18 de Marzo del 2021

Atentamente,

ADRIAN MARTIN ALCANTARA CORTEZ

GERENTE GENERAL  
REM SYSTEMS S.A.C.  
Adrian Alcantara Cortez  
Gerente General

Jr. Ernesto Mora 475 Piso 2, San Martin de Porres, Lima – Perú

Teléfono: (511) 701 – 3625

[www.remsystems.pe](http://www.remsystems.pe)



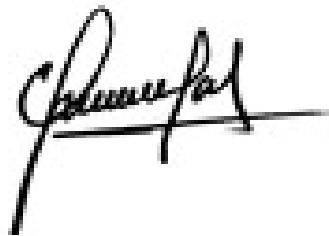
	<b>ACTA DE APROBACIÓN DE ORIGINALIDAD DE TESIS</b>	Código : <a href="#">F06-PP-PR-02.02</a>
		Versión
		: <span style="float: right;">09</span>
		Fecha
		: <span style="float: right;">27-09-2021</span>
Página	: <span style="float: right;">3 de 14</span>	

Yo, Mgtr. Ing. Robert Eduardo Ormeño Rojas docente de la Facultad de Ingeniería y Arquitectura y Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo – Lima Norte, revisor (a) de la tesis titulada:

“UNIFIED THREAT MANAGEMET (UTM) PARA LA GESTIÓN DE LOS SERVICIOS DE SEGURIDAD BASADO EN COBIT 5 EN LA EMPRESA REM SYSTEMS S.A.C.” de los (de la) estudiante: GODOY FUENTES, LUIS ARNALDO constato que la investigación tiene un índice de similitud de 30% verificable en el reporte de originalidad del programa Turnitin.

El/la suscrito (a) analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

Lima 27 de septiembre del 2021



.....  
Firma

Mgtr. Ing. Robert Eduardo Ormeño Rojas

DNI: 44439590

Elaboró	Dirección de Investigación	Revisó	<a href="#">Representante del SGC</a>	Aprobó	<a href="#">Vicerrectorado de Investigación</a>
---------	----------------------------	--------	---------------------------------------	--------	---