UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para seguridad de la información en Municipalidades

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
INGENIERO DE SISTEMAS

AUTORES:

Bermudo Flores, Esving (ORCID:0000-0001-7275-5021)

Gomez Poma, Carlos Enrique (ORCID:0000-0002-8183-5506)

ASESOR:

Mg. Saboya Rios, Nemias (ORCID:0000-0002-7166-2197)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA – PERÚ

2022

Dedicatoria

Está dedicado primeramente a nuestro señor Dios, por habernos dado, salud y bendiciones con nuestros hijos y hermanos por darnos las fuerzas por haber confiado en nosotros para seguir adelante.

Agradecimiento

A nuestras familias por haber depositado su confianza en nosotros para lograr este objetivo. A nuestros docentes que día a día con gran esfuerzo nos apoyó para lograr esta meta.

índice de contenidos

Índice de tablas

Índice de figuras

Resumen

La investigación tiene el objetivo de determinar la eficacia del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en municipalidades, con la finalidad de establecer controles para la seguridad de la información y generar confianza en la confidencialidad, integridad y disponibilidad de dicha información. El estudio se ejecutó en la municipalidad de Miraflores con la participación de 25 trabajadores del área de Tecnología de la Información para la encuesta de percepción del usuario en referente al marco de trabajo, y se hizo registro de fichaje en 21 días laborables de lunes a viernes en el pre test y post test para los 6 indicadores de la variable dependiente, Asimismo, el trabajo fue de tipo aplicativo con un diseño pre experimental, se utilizó dos tipos instrumentos de recolección de datos: el cuestionario de percepción y el fichaje. El cuestionario de percepción fue aplicado a 25 trabajadores del área Tecnología de la Información. Los fichajes se realizaron en 21 días laborables de lunes a viernes en el pre test y post test a todos los indicadores de la variable dependiente. Los hallazgos muestran que el porcentaje de intentos de usuarios no autorizados mejoró en un 80.72%, el porcentaje de amenazas detectadas mejoró en un 80.45%, el porcentaje de incidencias en acceso de aplicaciones disminuyó en un 1.75% en comparación al pre test, Además, el porcentaje de equipos de cómputo vulnerables disminuyó en un 85.26%, el porcentaje de disponibilidad de los sistemas mejoró en un 11.03%, y el porcentaje de incidencias en el data center disminuyó en un 24.99%. Por lo tanto, los resultados obtenidos comprobaron la eficacia del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de la información siendo un aporte fundamental para la mejora de los niveles de seguridad institucional en el área de Tecnología de la Información.

***Palabras claves**:* UTM, Seguridad de Información, Gestión de Riesgos.

Abstract

The research aims to determine the effectiveness of the framework based on unified threat management (UTM) for information security in municipalities, in order to establish controls for information security and generate trust in confidentiality, completeness and availability of such information. The study was carried out in the municipality of Miraflores with the participation of 25 workers from the Information Technology area for the user perception survey regarding the framework, and a registration record was made in 21 working days from Monday to Friday. in the pre-test and post-test for the 6 indicators of the dependent variable. Likewise, the work was of an application type with a pre-experimental design, two types of data collection instruments were used: the perception questionnaire and the signing. The perception questionnaire was applied to 25 workers in the Information Technology area. The signings were made in 21 working days from Monday to Friday in the pre-test and post-test to all the indicators of the dependent variable. The findings show that the percentage of unauthorized user attempts improved by 80.72%, the percentage of detected threats improved by 80.45%, the percentage of application access incidents decreased by 1.75% compared to the pretest, in addition, the percentage of vulnerable computer equipment decreased by 85.26%, the percentage of system availability improved by 11.03%, and the percentage of incidents in the data center decreased by 24.99%. Therefore, the results obtained confirmed the effectiveness of the framework based on unified threat management (UTM) for information security, being a fundamental contribution to the improvement of institutional security levels in the Information Technology area. Information.

Keywords: UTM, Information Security, Risk Management

I. INTRODUCCIÓN

A nivel mundial, con la aparición del coronavirus COVID-19, las Tecnologías de Información y Comunicación ha jugado un papel transcendental e imprescindible en el desarrollo de las actividades de manera remota, permitiendo la transferencia y reciprocidad de toda la información (Garcia, 2020, párr. 1). Todo ello, ha provocado una gran masificación e hiperconectividad que facilita las comunicaciones y desenvolvimiento de toda una sociedad (las comunicaciones, el transporte, dinamización de comercios, los servicios financieros, los servicios de emergencia, el comercio electrónico, entre otros); corriendo el riesgo de ataques cibernéticos si no se ha gestionado las medidas de seguridad de la información de manera efectiva (Leiva 2015, párr. 2).

Los ataques cibernéticos son uno de los delitos informáticos que ha crecido en los últimos tiempos. Según ICE (2022, párr. 2-4), en Latinoamérica en el 2021 aumentó en un 38% y en el 2021 con 1118 ataques, en tal sentido, los sectores más afectados fueron educación e investigación con 75%; los sectores gubernamentales, 47%, comunicaciones, 51%, proveedores de servicios gestionados y servicio de internet, 67% y salud, 71%. Por su parte, Andina (2022, párr. 3) indica que los países de Latinoamérica que han sido en gran medida víctimas de ataques cibernéticos se destaca Colombia (11.2 mil millones), Brasil (88.5 millones), México (156 mil millones) y Perú (11.5 mil millones).

El Perú, específicamente, es uno de los países afectado por los intentos de ataques cibernéticos, un estudio realizado por Fortinet 2022 señala que más 32 millones de intentos al día o 1.3 millones cada hora, en promedio; debido al incremento del trabajo y educación remota amenazando la ciberseguridad corporativa y personal respectivamente; en casos de distribución de virus malware y troyano inyectadas en aplicaciones de Microsoft Office (Andina, 2022, párr. 1).

En este orden de ideas, las municipalidades que conforman Perú se encuentran afectadas por los ataques cibernéticos, ya que se han encargado de debilitar las vulnerables tecnológicas de las instituciones con el fin de obtener información confidencial y de valor para actos ilícitos que sobrelleva graves riesgos y amenazas que consiguen perturbar a la Seguridad Nacional. En el contexto del problema, la

Municipalidad de Miraflores no cuenta con mecanismos y políticas de seguridad informáticas permanentes y efectivas para la custodia de la información, por lo que se encuentra vulnerable ante los ataques cibernéticos sensibles, debido que no cuenta con dispositivos de protección efectivos ante el crecimiento de las redes y la seguridad de la información.

En este sentido, las organizaciones necesitan una serie de normas y reglas, así como diversos controles que le brinde seguridad, garantizando que sus recursos tecnológicos sean utilizados de manera correcta, respondiendo a la confidencialidad de la información ~~a~~ de sus usuarios y proporcionando entornos seguros que brinden confianza adecuada para transmitir la información (Cabrera, Garcia y Salinas, 2019, p. 1).

En este contexto, la Municipalidad de Miraflores debe actuar estableciendo controles para la seguridad de la información y generar confianza de acceso, integridad y confidencialidad a través de un enfoque de seguridad integral que detecte las amenazas antes que ocurran. Además, se debe aplicar acciones que mitiguen a tiempo obteniendo el nivel de credibilidad institucional.

Para esta investigación se definió el siguiente problema general de la investigación: ¿En qué medida el marco de trabajo basado en la gestión unificada de amenazas (UTM) favorece la seguridad de información en la Municipalidad de Miraflores? Asimismo, se definieron los siguientes problemas específicos: 1) ¿En qué medida el marco de trabajo basado en la gestión unificada de amenazas (UTM) favorece la confidencialidad de la información en la Municipalidad de Miraflores?; 2) ¿En qué medida el marco de trabajo basado en la gestión unificada de amenazas (UTM) favorece la integridad de la información en la Municipalidad de Miraflores?; 3) ¿En qué medida el marco de trabajo basado en la gestión unificada de amenazas (UTM) favorece la disponibilidad de la información en la Municipalidad de Miraflores?.

Para esta investigación se definió el siguiente objetivo general de la investigación: Determinar la eficacia del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de la información en la Municipalidad de Miraflores. Asimismo, los siguientes objetivos específicos: 1) Determinar la eficacia del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la

confidencialidad de la información en la Municipalidad de Miraflores; Determinar la eficacia del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la integridad de la información en la Municipalidad de Miraflores; 3) Determinar la eficacia del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la disponibilidad de la información en la Municipalidad de Miraflores.

Como justificación metodológica se utilizó la norma de calidad ISO/IEC 27001 para la administración de la información que permita implementar un marco de trabajo basado en la gestión unificada de amenazas (UTM) que favorece la seguridad informática en la municipalidad, reduciendo los riesgos informáticos (Normas ISO, 2022, p. 1). Asimismo, para la justificación tecnológica se realizó la implantación en la Gerencia de Informática y Tecnología de la Información de la Municipalidad de Miraflores, un equipo de gestión unificada de amenazas, utilizando Sophos XGS3300 para la gestión de seguridad lógica y perimetral, se obtendrá un control de aplicaciones, prevención de intrusiones, antivirus, filtrado de URL, sandboxing e inspección SSL, de esa manera prescindir el traspaso de código malicioso, las tentativas de intrusión por medio de la red. Por otro lado, para la justificación práctica; con el uso tecnológico de la gestión unificada de amenazas se solventó en un buen porcentaje la problemática presentada con la seguridad informática, ya que se contará con control de aplicaciones, prevención de intrusiones, antivirus, filtrado de URL, sandboxing e inspección SSL. Aunado a esto, se tendrá un enlace a Internet, el cual permite publicar los servicios que presta la municipalidad a la ciudadanía; y también permite el acceso a Internet a los colaboradores de las diferentes áreas orgánicas de la Municipalidad. Y por último, la justificación social, se presentan los beneficiarios de implantar en la Gerencia de Informática y Tecnología de la Información de la Municipalidad de Miraflores, fueron todos los ciudadanos que integran la mencionada municipalidad, ya que toda la información será protegida ante los ataques cibernéticos y tendrá la seguridad que la información que se maneja no haya sido vulnerada ni utilizada para actos ilícitos.

Con respecto a las hipótesis, se definió como hipótesis general: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la seguridad

de información en la Municipalidad de Miraflores. Además, se definieron las siguientes hipótesis específicas: 1) El Marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la confidencialidad de la información en la Municipalidad de Miraflores; 2) El Marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la integridad de la información en la Municipalidad de Miraflores; 3) El Marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la disponibilidad de la información en la Municipalidad de Miraflores.

II. MARCO TEÓRICO

Para el desarrollo de este proyecto se examinaron investigaciones previas tanto a nivel nacional como internacional como base referencial de esta investigación.

Con respecto a los antecedentes internacionales, se cita a Calderón, Tovar y García (2019) (Calderon Diaz, Tovar Semenate y Garcia Cuellar, 2019), en un estudio de investigación utilizó la metodología de análisis de decisión multicriterio AHP sugerida por Thomas L. Saaty, donde se aplicó una encuesta, que evidencia la oportunidad del proyecto, Los resultados muestra que se obtuvo con la implementación del sistema de seguridad perimetral la red se encuentra segura, de esta manera, se puede monitorear y crear reportes de casos que se presenten, en cuanto a los acontecimientos que afecten la seguridad de la información de tal manera, que se pueda los respectivos bloqueos.

El aporte del estudio la investigación fue la seguridad de información y su aplicación en la implementación de un sistema de seguridad.

Por otro lado, Avendaño, Díaz y Tafur (2019) realizaron una investigación, cuya la metodología fue cualitativa basado en la observación de los comportamientos que tienen los usuarios al momento de manipular la red de cómputo, asimismo, el uso apropiado de los equipos informáticos y la manera como protegen su información. También, la verificación de las alternativas para proteger y realizar las respectivas medidas que disminuyan la pérdida de la información y las amenazas o vulnerabilidades en el sistema de información.

El aporte de conocimiento de la investigación fue la utilización del dispositivo de seguridad UTM que alberga diferentes servicios para la integridad de la red y la implantación de políticas de seguridad ineludibles la cualquiera para cualquier empresa.

En consecución, García (2021) realizó un estudio cuyo método fue histórico lógico, método descriptivo, método deductivo, método inductivo, método bibliográfico. En la conclusión, muestra que el análisis realizado dio como resultado la identificación de la vulnerabilidad que presenta la infraestructura y la definición de los requisitos para implementar el sistema mencionado utilizando cámaras de video vigilancia.

El aporte de conocimiento de la investigación fue la teoría seleccionada sobre sistemas de seguridad para hacer el estudio de factibilidad.

Además, Montecé, Arguello y Vargas (2017) diseñaron una investigación, donde los hallazgos muestran que el diseño de un control de seguridad de acceso para planteles de educación media presta un buen margen de confidencialidad y control de acceso; siendo estos aspectos significativos de la seguridad en la infraestructura tecnológica sujetas a las inquietudes de los usuarios.

El aporte de conocimiento de la investigación fue la teoría seleccionada sobre sistemas de seguridad en el aspecto o criterio de confidencialidad.

Otra contribución a esta tesis fue el de Chaverra (2021) aplicaron un método de investigación basado en la Norma ISO-27001, cuyas conclusiones fueron que todo centro educativo debe adquirir un esquema de resguardo de las bases de datos inequívoco y eficiente que impida que la información se maneje ilícitamente, garantizando así su seguridad académica.

El aporte de la investigación fue el método investigativo basado en la Norma ISO-27001, que pretende proporcionar la disponibilidad, acceso restringido e integridad de la información.

Y por último a nivel internacional, se puede mencionar a Villa (2019) que concluye en su investigación que el diseño ha permitido realizar una operación confidencial e inequívoca, aminorando los riesgos y optimizando la resiliencia ante otros acontecimientos de ciberseguridad sobre dichas PMU.

El aporte de la investigación fue el procedimiento de ratificación de requisitos para preservar la seguridad del sistema computacional.

En referencia a los antecedentes nacionales, Vázquez (2020) aplicó en su investigación una metodología basada en la ISO/IEC 27001:2013; norma de calidad estandarizada. En la conclusión muestra que el diseño permitió definir como se tratarán los riesgos informáticos alineados a los objetivos de la empresa.

El aporte a la investigación fue la determinación de los controles para la mejora de la seguridad de la información utilizando la norma de calidad ISO/IEC 27001:2013.

En este mismo sentido, Ruiz y Delgado (2018) realizaron un estudio donde con una metodología aplicativa porque aporta solución y la mejora de un problema, además de ser no experimental y descriptiva. Concluyeron que con la aplicabilidad del firewall pfSense (instalación y configuración) se obtuvo un significativo declive de las vulnerabilidades en la red.

El aporte de conocimiento de la investigación se basó respecto a la implementación de la seguridad de los servicios académicos.

Otro antecedente de relevación fue el de Alvarado y Sánchez (2020), en una investigación no experimental de tipo longitudinal. Los autores concluyeron que los controles de la seguridad implementados fueron la base primordial para establecer mejores de nivel seguridad en el proceso de desarrollo de sistemas y del producto. Se obtuvo inicialmente un resultado del 48.95%, ubicando al proceso en un nivel de seguridad Parcialmente Logrado. Luego, se implementó oportunidades de mejora y se obtuvo un 81.80%, con un incremento del 32.85% del nivel seguridad de la información alcanzando un cumplimiento en dichos controles.

El aporte de conocimiento de la investigación se basó en los controles aplicando la norma ISO/IEC 27002:2015.

También se tomó como referencia, Niño (2018), en su investigación se basó en un modelo PDCA y la metodología aplicada fue Magerit VS 3 para obtener un sistema de gestión de la información basados en el estándar NTP ISO/IEC 27001:2014, en la Dirección Ejecutiva de Difusión Estadística y de Producción Estadística. En la conclusión, muestra que con el estudio permitió conocer las amenazas que se producían en los activos de información en ODEI Lambayeque, al realizar un análisis de riesgos tipo cuantitativo que produjo un nivel de madurez con respecto a la seguridad de la información que se encontraba muy bajo.

El aporte a esta investigación se basó en la elaboración y aplicación de un trabajo para el análisis de riesgos que en el instituto ODEI Lambayeque para la observancia de la legislación y promover las buenas prácticas.

Así mismo, Jara (2018) realizó una investigación aplicando un diseño pre-experimental con corte longitudinal, además de un método hipotético deductivo y

un enfoque cuantitativo. La población fue registro de los activos y el instrumento utilizado son fichas de observación. Los resultados evidenciaron que hubo un adelanto al aplicar este sistema sobre el proceso de gestión del riesgo, demostrado a través del procedimiento estadístico de Wilcoxon.

El aporte de conocimiento de la investigación se basó en la metodología de investigación aplicada bajo un enfoque cuantitativo y diseño pre-experimental.

Y para concretar los antecedentes se menciona a Taboada (2021) arribó a la conclusión de su investigación que la evaluación del modelo fue ejecutada por profesionales expertos, con el fin de tantear la aplicabilidad en el sector de estudio, dando como resultado de su confiabilidad en un 72%, siendo válido para ayudar a optimizar los activos de información financiera de la institución por medio de la seguridad.

Para reforzar el aspecto teórico se tomará como contenido primordial la Gestión Unificada de Amenazas (UTM), que es un producto de seguridad de la información que proporciona muchas funciones de protección a un solo punto en la red ayudando a cumplir y contrarrestar fallos por inexperiencia en controles de seguridad, ataques informáticos, violación de políticas de acceso y una inadecuada administración de los sistemas de información (Flórez, Arboleda y Cadavid, 2018, p.38).

Los UTM poseen técnicas que compactan el hardware o de software los cuales incluye funcionalidades como Firewall, Filtrado de contenido en la red, Antivirus, Anti-Spyware y Anti-spam, además de prevención y detección de intrusiones. También, pueden ofrecen servicios de enrutamiento remoto, compatibilidad para redes privadas virtuales (Virtual Private Network - VPN,) y traducción de direcciones de red (Network Address Translation - NAT) (Kaspersky, 2021, párr. 1).

Las empresas que protegen su infraestructura informática pueden optar por adquirir los productos UTM que les permiten administrar en un solo equipo su seguridad de información con asistencia de TI. Por ello, tuvieron aceptación en el mercado, debido a su alcance en amenazas mixtas, que se basa en la combinación

de otros tipos de malware y ataques simultáneos a diferentes partes de la red) (Kaspersky, 2021, párr. 2).

Entre las ventajas del UTM podemos mencionar que se simplifica en un único dispositivo la arquitectura de red, funciones integradas de seguridad, reportes completos del estado de la red y menos controles de seguridad por parte del personal de Tecnologías de la Información. Pero además de ventajas tiene desventajas, ya que proporciona un único punto de defensa también instituye un único punto de falla. (Kaspersky, 2021, párr. 4). 1) Sophos Firewall, proporciona Protección y rendimiento potentes y los dispositivos de la serie XGS con procesadores de flujo Xstream dedicados procuran un acrecentamiento de velocidad de aplicaciones, inspección TLS de alto rendimiento y una poderosa defensa frente a amenazas. La arquitectura de Xstream de Sophos Firewall se diseñó para brindar unos niveles sorprendentes de claridad, resguardo y rendimiento, con el propósito de confrontar los problemas de ataques de las redes. 2) Aceleración de aplicaciones, Sophos Firewall eleva el tráfico de aplicaciones de SaaS, SD-WAN y en la nube como VoIP, vídeo, entre otros; por medio de sus adecuadas políticas, situándola en la ruta rápida FastPath a través del procesador de flujo Xstream, logrando dirigirse de forma profunda a la ruta rápida FastPath, sin escaneo de seguridad agregada para la búsqueda de amenazas. Todos esto con el fin de disminuir la latencia y perfecciona el rendimiento general. 3) SD-WAN, Sophos Firewall con SD-WAN de Xstream brinda una solución SD-WAN potente e integrada, con selección de enlaces y enrutamiento fundados en el rendimiento, transiciones de cero impactos entre enlaces en caso de interrupción, orquestación centralizada administrada en la nube y aceleración FastPath de Xstream del tráfico de túnel VPN, lo que la convierte en una de las mejores y más flexibles soluciones SD-WAN disponibles en un firewall hoy en día.

Además de ello, 4) Administrar fácilmente múltiples firewalls, Sophos Central facilita la configuración, inspección y gestión diaria de Sophos Firewall. Además, brinda alertas, administración de copias de resguardo, reajuste del firmware y el suministro de nuevos firewalls. Esto permite la administración de todos sus dispositivos desde una única consola, configurar cambios programar copia de seguridad y programar actualizaciones firmware. 5) Generación de informes de firewall en la nube, Sophos

Central es una eficaz herramienta para gestionar informes con visualización detallada de la red a lo largo del tiempo; cuenta con informes integrados y pueden hacerse personalizados. Esto permite un mejor análisis de la red para detectar comportamientos inciertos de los usuarios. 6) Protección contra la propagación lateral, Esta protección bloquea espontáneamente los sistemas comprometidos en cada punto de la red para detener al momento los ataques; haciendo que los endpoints correctos contrarresten los afectados, generando un aislamiento completo que impide amenazas por la red y el robo de datos.

En consecución, 7) ID de usuario sincronizado, excluye la falta de agentes de autenticación de clientes o servidores, con la comunicación entre el endpoints y el firewall ya que se integran y comparten información por medio de Security Heartbeat. 8) SD-WAN sincronizada; Enrutamiento de aplicaciones potente y de confianza, la SD-WAN sincronizada optimiza la selección de rutas WAN para las aplicaciones empresariales significativas optimizando la eficiencia de la red. 9) Protección potente, este diseño expone los riesgos clandestinos, bloquear amenazas y reconocer automáticamente los incidentes, ayudando a tener el control de la red. La protección next-gen como el Deep Learning y la prevención de intrusiones le admiten conservar su organización resguardada de ataques e infiltraciones, ya que con antelación da respuesta automática ante amenazas evitando las filtraciones y la propagación lateral. 10) Protección de redes, Prevención frente a intrusiones next-gen (IPS), VPN sin cliente: HTML5 Ì VPN SD-RED, Gestión de dispositivos SD-RED, Reconocimiento TLS 1.3 con excepciones predefinidas, Generación de informes detallados de redes y amenazas, Integración con los endpoints de Sophos para identificar e incomunicar amenazas (Seguridad Sincronizada con Security Heartbeat), examen minucioso de paquetes de transmisión (Motor DPI de Xstream), protección hacia amenazas avanzadas (ATP). 11) Protección web, exploración de aplicaciones por diferentes criterios (usuario, categoría, grupo, entre otros), observación TLS 1.3 con excepciones predestinadas, utiliza el Control de aplicaciones sincronizado para enrutar apps incógnitas (SD-WAN sincronizada), inspección detallada de paquetes de transmisión (Motor DPI de Xstream:), control web: por categoría, palabra clave, usuario, grupo, URL, entre otros. 12) Protección de día cero, se estudian los archivos desconocidos mediante IA, ML y espacios seguros, utiliza múltiples

modelos de Deep Learning, reproducción de informes de análisis de amenazas, fiscalización detallada de paquetes de transmisión, información y análisis basados en la nube.

Aunado a esto, se abarco la teoría de gestión de riesgos, que se basa en un conjunto de actividades regularizadas que tratan de administrar e inspeccionar los riesgos que se presentan en una organización(Alvan, Soler y Oñate, 2018, p. 240).

Otra definición de gestión de riesgos la proporciona (Martínez y Blanco, 2017, párr. 28), la define como un enfoque, un sistema, un proceso, una práctica, una nueva forma de gestión, que proporciona a la dirección información respecto a los riesgos que se expone la organización y posibilita las estrategias para asumirlo.

El proceso de gestión de riesgos presenta un proceso integral que integra contexto, apreciación del riesgo, comunicación y consulta, monitoreo y control y tratamiento de riesgos.

Figura 1. Etapas de la gestión de riesgo

Fuente: Albán, Soler y Oñate (2018).

Y otro aspecto importante, trata de la Seguridad de la información, que Según (Pruna y Yarad, 2020, párr. 4), se refiere a una sucesión de medidas y procedimientos que se deben aplicar para proteger la integridad, la confidencialidad y disponibilidad de la información utilizando de recursos técnicos y humanos; para así mantener en normal funcionamiento de los sistemas informáticos, tanto del hardware como de software

Por otro lado, Reyna y Olivera (2017, p. 34) exponen que son medidas de protección de la infraestructura tecnológica de la organización, que permiten generar estrategias de contraataque para mitigar los delitos a través de esta red que contrarreste las amenazas del acceso ilícito de la información, vulnerando su seguridad e integridad.

La seguridad de la información se orienta a garantizar que la información este a tiempo y que sea confiable e integra al hacer un buen uso de la misma (Peñuela, 2018, párr. 4); siendo estos los elementos o principios básicos que la concretan; asociados a un plan estratégico para mitigar los riesgos asociados a los proceso y utilización de recursos que lo soportan. Por ello, para cualquier organización la seguridad informática es imprescindible y debe contener todos los aspectos que

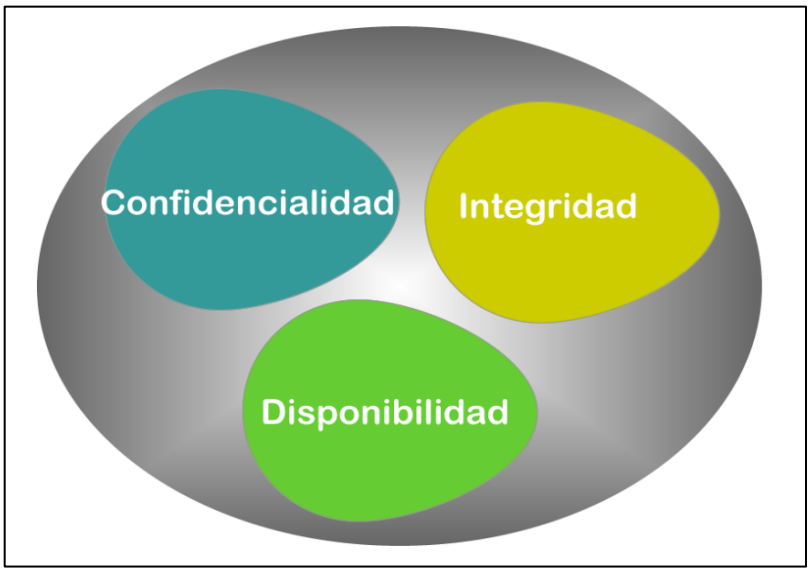
conforman la organización; siendo importante establecer las normas de revisiones periódicas, valoración de riesgos y controles para la protección de la información.

Existen normas ya prestablecidas y que permiten aplicar buenas prácticas de un estándar de seguridad de información, como la norma ISO/IEC 27001, que permite asegurar los activos de información tomando en cuenta las tres características fundamentales: confidencialidad, integridad y disponibilidad.

Dimensiones de la variable dependiente: seguridad de la información

La determinación de las dimensiones de la variable dependiente se centrará en los principios básicos de la norma ISO/IEC 27001 que ayuda a proteger la información de cualquier organización.

Figura 2. Características de Norma ISO/IEC 27001.



Fuente: Elaboración Propia (2022)

Como primera dimensión, se obtuvo la Confidencialidad, que según la norma ISO/IEC 27001, los sistemas deben tener la capacidad de resguardar los datos ante los usuarios no autorizados para el manejo de la información oportuno.

Esta dimensión tiene como Indicador # 1, el porcentaje de intentos de usuarios no autorizados; Rocha (2011) señalan que la confidencialidad, tiene como propósito advertir la utilización no autorizada de la información por personas sin permiso, es decir, que los datos de acceso deben ser conocidos por las personas responsable de la información. Por otro lado, Romero et al., (2018, p. 22), expresan que la

autenticación de usuarios, permite identificar qué quién accede a la información es la persona correcta.

$$\%IUNA = \frac{NINA}{NTI} * 100$$

Siendo, %IUNA = Porcentaje de intentos de usuarios no autorizados; NINA = Número de intentos no autorizados; NTI = Número totales de intentos

Otro indicador de esta dimensión es el Indicador # 2: porcentaje de amenazas detectadas, donde Romero et al., (2018, p. 22) indican que una vulnerabilidad es una falla que encuentra un atacante generando una inseguridad para la organización, convirtiéndose en una amenaza para los sistemas informáticos. Tales como Firewalls mal Configurados, Suplantación de contraseñas, Contraseñas débiles, Correos electrónicos infectados por virus, entre otros.

$$\%AD = \frac{NAD}{NTA} * 100$$

Dónde, %AD = Porcentaje de amenazas detectadas; NAD = Número de amenazas detectadas; NTA = Número totales de amenazas.

La segunda dimensión es la Integridad, según la norma ISO/IEC 27001, los sistemas de seguridad deben tener la capacidad preservar y conservar la fidelidad de la información y las técnicas de proceso que la manejan y transforman. Sus indicadores, son el Indicador # 3: porcentaje de incidencias en acceso de aplicaciones; Rocha (2011, p. 29), define que la integridad afirma que la información sea puntual, completa, sin variaciones o alteraciones en su contenido, por personas no autorizados.

$$\%IAA = \frac{NIAD}{NTAA} * 100$$

Siendo, % IAA = Porcentaje de incidencias de acceso aplicaciones, NIAD = Número de incidencias detectadas y NTAA = Número total de acceso aplicaciones.

Otro indicador que se definió fue el Indicador # 4: porcentaje de equipos de cómputos vulnerables, Romero et al., (2018, p. 26) señalan que para garantizar la integridad de la información se debe considerar el monitoreo del tráfico de red, la auditoria de los sistemas, la implementación de los sistemas de control de cambios y las copias de seguridad, que en caso de no lograr impedir que se maneje o pierda la información se pueda recobrar estado anterior.

$$\%ECV = \frac{NECV}{NTE} * 100$$

Dónde, % ECV = Porcentaje de equipos de cómputos vulnerables, NECV = Número de equipos de cómputos vulnerables y NTE = Número total de equipos.

Y la última dimensión de esta variable es la Disponibilidad, Según la norma ISO/IEC 27001, los sistemas de seguridad deben tener la capacidad de proveer el acceso y la consulta de la información cuando el solicitante autorizado lo requiera.

En este sentido, el indicador definido es el Indicador # 5: porcentaje de disponibilidad de los sistemas; Rocha, (2011, p. 29), indica que la disponibilidad afirma que los usuarios pueden tener acceso en el momento requerido y de manera fiable a sus recursos de información, admitiendo de esta manera la continuidad del negocio.

$$\%DS = (\frac{NSD}{NSR} * 100$$

Dónde, % DS = Porcentaje de disponibilidad de sistemas; NSD = Número de sistemas disponibles y NSR = Número de sistemas requeridos.

Además de3 este indicador, se precisó el Indicador # 6: porcentaje de incidencias en el data center. Romero et al.,(2018, p. 27) mencionan que la información y sistemas son seguros si solo acceden personas autorizadas y si puede detectar a

tiempo el acceso a personas ajenas, garantizando un nivel de servicio y acceso a la información aceptable según las necesidades.

$$\%IDC = \frac{NIDC}{NP} * 100$$

Siendo, $\%IDC$ = Porcentaje de incidencias en el data center, NIDC = Número fallas detectadas y NP = Número de peticiones.

A continuación, se presenta el enfoque conceptual:

Amenazas: son acontecimientos que ponen en peligro los procesos o recursos (Romero et al., 2018).

Ataques activos: son acciones inmediatas que buscan dañar la infraestructura al realizar sabotajes o robo de información permanente hasta conseguirlo (Curioso y Espinoza, 2017).

Control de riesgos: Se basa en aplicar estrategias efectivas para establecer estrategias que permitan ejecutar acciones, contingencias, correcciones para evitar contrarrestar los riesgos (Rio y Cárdenas, 2021).

Delito informático: son actividades delictivas sobre la infraestructura tecnológica de cualquier organización o ciberespacio, como desfalcos, estafas, alteraciones, deterioros, fraudes, entre otros (Borghello, 2018).

Estándares de tecnologías de información y de comunicación: Es la serie de políticas, reglas o instrucciones que se aplican sobre las tecnologías de información y de comunicación (Curioso y Espinoza, 2017).

ISO/IEC 27001: es una norma para la gerencia de la seguridad de la información en las organizaciones NormasISO (2022).

Infraestructura tecnológica: Son todos los dispositivos tecnológicos que cuenta una empresa para su funcionamiento, como red de comunicaciones, servidores, equipos de cómputo, impresoras, red de datos, sistemas operativos, lenguajes de programación, bases de datos, sistemas de aplicaciones, entre otros (Curioso y Espinoza, 2017).

Mejora continua: es una fase que se encargada de conservar el estado de la infraestructura a través de la valoración y progreso continuo de la calidad de los procesos aplicados (Krishnan & Ravindran, 2018 Citado en Sánchez Casanova, 2021).

Políticas de seguridad: son mecanismos de seguridad que deben definirse notoriamente y donde se especifican las actividades que se deben realizar para desempeñar dichas funciones (Saari, 2021).

Riesgo: es la probabilidad de que algo perjudicial ocurra trayendo como consecuencia daños a recursos tangibles o intangibles y que impiden el desenvolvimiento efectivo de cualquier actividad (Romero et al., 2018).

Vulnerabilidades: son los fallos de los sistemas de seguridad y que pueden genera un problema si no se acciona a tiempo (Romero et al., 2018).

III. METODOLOGIA

3.1. Tipo y diseño de investigación:

3.1.1 Tipo de investigación Cuantitativa

Esta investigación es de tipo cuantitativo, ya que permite estimar volumen de la información y ratificar la hipótesis Hernández y Mendoza,(2018, p. 6). Al respecto, Hernández, Fernández y Baptista, (2014, p. 4) exponen que esta perspectiva maneja la recaudación de datos para examinar hipótesis a través del cálculo numérico y análisis estadístico, para así obtener el comportamiento.

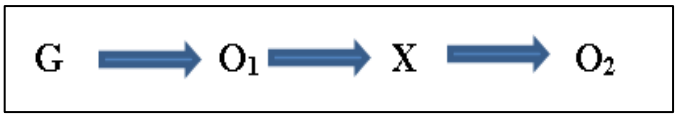
3.1.2 Tipo de investigación aplicada

La investigación aplicada trata de generar conocimientos para resolver un problema social o a nivel productivo. Lozada (2014, p. 35). Por lo tanto; se aplicará un marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

3.1.3 Diseño de investigación

- **Diseño experimental:**
  Hernández y Mendoza (2018, p. 153) lo definen como un modelo adaptable cuando se ejecuta la causa y el efecto; este estudio se procesa a través con la manipulación de la variable independiente causando el pretendido resultado.
- **Diseño pre-experimental:**
  Léon y Montero (2002, p. 229) indican que el análisis de los datos se ejecuta comparando datos directos derivados de un mismo sujeto en distintos tiempos de medición. En este proyecto de investigación se aplicará un pre Prueba y post Prueba, previa a la situación actual y luego de aplicar el marco de trabajo en la institución; con respecto tomando en cuenta la aplicabilidad de la variable dependiente (Ver figura 3).

Figura 3. Diseño de investigación pre experimental



Fuente: Elaboración propia

Dónde:

G = Grupo

O_1= Grupo experimental del pre test; contexto actual

X= Aplicación marco de trabajo

O_2=Post-test. Grupo experimental del post test; marco de trabajo implementado.

3.2. Variables y operacionalización:

3.2.1 Identificación de Variables

Variable independiente: Gestión de Riesgos

Definición conceptual: Martínez y Blanco (2017, párr. 28), la definen como un enfoque, un sistema, un proceso, una práctica, una nueva forma de gestión, que proporciona a la dirección información respecto a los riesgos que se expone la organización y posibilita las estrategias para asumirlo.

Definición operacional: Conjunto de procedimientos que debe establecerse para salvaguardar a la empresa sobre riesgo en la infraestructura tecnológica que puedan afectar su integridad y normal funcionamiento.

Variable dependiente: seguridad de información

Definición conceptual:

Es una cantidad de procedimientos coordinados y ajustados a las políticas de la empresa para proteger la integridad, la confidencialidad y disponibilidad de la información por medio de recursos técnicos y humanos; para así mantener en normal funcionamiento de los sistemas

informáticos, tanto del hardware como de software (Pruna y Yarad, 2020, párr. 6).

Definición operacional:

Son los mecanismos que deben tomar las organizaciones sobre su sistema tecnológico para defender y salvaguardar la data buscando conservar la confiabilidad, la disponibilidad y la rectitud de datos que conforman el activo organizacional.

Operacionalización de variables

Tabla 1. Operacionalización de la variable Seguridad de Información

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de Medición
Seguridad de Información	Es una cantidad de procedimientos coordinados y ajustados a las políticas de la empresa para proteger la integridad, la confidencialidad y disponibilidad de la información por medio de recursos técnicos y humanos; para así mantener en normal funcionamiento de los sistemas informáticos, tanto del hardware como de software (Pruna y Yarad, 2020, párr. 6).	Son los mecanismos que deben tomar las organizaciones sobre su sistema tecnológico para defender y salvaguardar la data buscando conservar la confiabilidad, la disponibilidad y la rectitud de datos que conforman el activo organizacional.	Confidencialidad	• % Intentos de usuarios no autorizados. • % amenazas detectadas.	Fichaje
			Integridad	• % de incidencias en acceso de aplicaciones • % de equipos de cómputos vulnerables	
			Disponibilidad	• % de disponibilidad de los sistemas • % de incidencias en el data center	

Fuente: Elaboración Propia (2022)

Tabla 2. Operacionalización de Gestión de Riesgo

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de Medición
Gestión de Riesgo	Ecured (2017), la define como un enfoque, un sistema, un proceso, una práctica, una nueva forma de gestión, que proporciona a la dirección información respecto a los riesgos que se expone la organización y posibilita las estrategias para asumirlo.	Es un conjunto de actividades que permiten la identificación, análisis, evaluación y tratamientos de los riesgos que pueden afectar la infraestructura tecnológica de una organización.	Identificación de Riesgos	• Identificación de Activos Críticos • Identificación Amenazas de Activos. • Detección de Vulnerabilidades de Activos.	Cuestionario de percepción
			Análisis de Riesgos	• Frecuencia de Ocurrencia del riesgo. • Detección de Riesgos a tiempo. • Tiempo Promedio de Resolver la ocurrencia del Riesgos.	
			Evaluación de Riesgos	• Tiempo Promedio de Resolver la ocurrencia del Riesgos.	
			Tratamiento de Riesgos	• Cumplimiento de Políticas de Seguridad. • Implementación de los procesos de auditoria**.**	

Fuente: Elaboración Propia (2022

3.3. Población, muestra y muestreo:

Población

Según Arias, Villasís y Miranda, (2016), la población de estudio es una cantidad de personas que tienen una serie de criterios definido, restringido y asequible del tema de estudio. Este estudio, se realizó en la Municipalidad de Miraflores, conformada por 25 trabajadores en el área Tecnología de Información. Para la encuesta de percepción del usuario y de tipo de muestreo aleatorio simple, para el fichaje se realizó en 21 días laborables de lunes a viernes para el estudio pretest y pos-test para cada uno de los indicadores de las dimensiones confidencialidad, integridad y disponibilidad.

- **Criterio de inclusión:** son los 25 trabajadores de área de tecnología de información que interactúan con el marco de trabajo basado en la gestión unificada de amenazas (UTM)
- **Criterio de exclusión:** Se excluyen a los gerentes, subgerentes y DBA ya que ellos tienen permiso de navegación.

Muestra:

Según Arias, Villasís y Miranda (2016), la muestra cumple con una sucesión de juicios establecidos que forma parte de la población de estudio. Pero se tomará como muestra el total de la población, tomando en cuenta lo que refieren Salazar y Castillo (2018) son una serie de elementos escogidos de la población, además de ello, se puede seleccionar a la población si es menor a 30 elementos. Para la muestra se realizó una encuesta de percepción que estuvo conformada por 25 trabajadores del área de Tecnología de Información y el fichaje para todos los indicadores fue de 21 días laborables de lunes a viernes en pretest y post-test que son, porcentaje de intentos de usuario no autorizados, porcentaje de amenazas detectadas correspondiente a la dimensión confidencialidad y para los indicadores de la dimensión integridad son porcentaje de incidencias en acceso de aplicaciones y porcentaje de equipos de cómputo vulnerable se hizo con la misma cantidad de trabajadores por último para la dimensión disponibilidad se consideró estos indicadores

porcentaje de disponibilidad de los sistemas y porcentaje de incidencias en el data center.

Muestreo

El muestreo probabilístico aleatorio simple permite definir la población y se elabora una lista de todos los involucrados, concretando el tamaño de la muestra y se toman al azar los elementos (Hernández, Fernández y Baptista, 2014, p. 179).

Utilizaremos un muestreo aleatorio simple ya que la población es finita cada uno de las personas que lo conforman tiene la misma posibilidad de ser elegida; por su carácter de aleatoriedad. El muestreo se realizó con 25 trabajadores del área de Tecnología de Información para la encuesta de percepción del usuario, y el fichaje se realizó en 21 días laborables de lunes a viernes en el pretest y post-test para todos los indicadores de la variable dependiente para el marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de la municipalidad de Miraflores.

3.4. **Técnicas e instrumentos de recolección de datos:**

Se aplicó la encuesta, que es una técnica que permite conseguir información de la muestra seleccionada con la aplicación del instrumento delineados de manera anticipada y determinada (Hernández, Fernández y Baptista, 2014, p. 218).Como instrumento de recolección de datos se aplicó dos técnicas que fueron, la encuesta de percepción del usuario la cual se realizó a 25 trabajadores del área de Tecnología de Información , también se realizó el fichaje en 21 días laborables de lunes a viernes del pre-test y post-test de las dimensiones confidencialidad con sus respectivos indicadores que son porcentaje de intentos de usuarios no autorizados y porcentaje de amenazas detectadas, seguidamente la dimensión integridad y sus indicadores porcentaje de incidencias en acceso de aplicaciones y porcentaje de equipos de cómputo vulnerables y por último la dimensión disponibilidad con sus indicadores que son porcentaje de disponibilidad de los sistemas y porcentaje de incidencias en el data center frente a las acciones del Marco de trabajo basado en la gestión

unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Para validar el instrumento se utilizó con la técnica juicio de expertos, tomando la experiencia en el tema de personal calificado (Lacave et al., 2015, p. 138). En este informe de investigación se estableció tres (3) expertos; uno el área metodológica, otro en el área de seguridad y otro un experto general en el tema.

3.5. **Procedimientos:**

El procedimiento para llevar a cabo este informe de investigación se realizó el siguiente procedimiento.

Se buscó información en los buscadores confiables y en las bases de datos de las diferentes universidades públicas y privadas respecto a nuestras variables independiente y dependiente, antecedentes internacionales y nacionales respectivos al tema de nuestra investigación, se presentó la carta de aceptación a la Municipalidad de Miraflores para la realización del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores. Además, se realizó los registros del Fichaje en 21 días laborables de lunes a viernes para el pre-test y post-test de los siguientes indicadores: porcentaje de intentos de los usuarios no autorizados y porcentaje de amenazas detectas referente a la dimensión confidencialidad enseguida los indicadores porcentaje de incidencias en acceso de aplicaciones y porcentaje de equipo de cómputo vulnerables de la dimensión integridad por último los indicadores porcentaje de disponibilidad de los sistemas y porcentaje de incidencias en el data center de la dimensión disponibilidad. También se realizó la encuesta de percepción a 25 trabajadores de la Municipalidad referente al marco de trabajo, luego de obtener los resultados de registro de fichaje, encuesta de percepción de usuario tanto en pretest y post-test se verifico los datos obtenidos para trabajar en el software estadístico SPSS 26 para realizar el análisis descriptivo e inferencial por último nos entregaron la carta de conformidad.

3.6. **Método de análisis de datos:**

En este informe de investigación realizaremos el método de análisis, estadística descriptiva y estadística inferencial.

La estadística descriptiva e inferencial implica resumir los datos conseguidos para describir la actuación de un conjunto de personas (Kazmier, 2015, párr. 12). en el presente informe de investigación se analizó la media, desviación estándar, mediana y valores mínimos y máximos de los indicadores. Se utilizó el grafico de líneas para los indicadores cuantitativos como: porcentaje de intentos de usuarios no autorizados, porcentaje de amenazas detectadas, porcentaje de incidencias en acceso de aplicaciones, porcentaje de equipo de cómputo vulnerables, porcentaje de disponibilidad de los sistemas, porcentaje de incidencias en el data center; Por otro lado se realizó gráfico de barras para visualizar los resultados de percepción de usuario en referente al marco de trabajo que fueron 25 trabajadores del área de Tecnología de Información.

En este estudio, prueba de normalidad que se utilizo fue Shapiro-Wilk debido a que la muestra de estudio fue menor a 30 y se identificó que todos los indicadores de la variable dependiente no cumplen con el supuesto de normalidad. Luego se utilizó la estadística no paramétrica y se aplicó la prueba de wilcoxon debido a los indicadores que no cumplen con el supuesto de normalidad y son muestras de grupos únicos y por último la campa de gauss, se tiene que observar e interpretar a que zona cayo el resultado si se rechaza la hipótesis nula y se acepta la hipótesis alterna este análisis de datos se realizó con el software estadístico SPSS 26.0

3.7. **Aspectos éticos:**

En esta investigación, la recopilación de información se realizó de las bases de datos de las universidades nacionales e internacionales, utilizando las plataformas de investigación en línea de Science Direct, Google académico, IEEE Explore, SCOPUS, EBSCOhost, libros y, repositorios de universidades públicas y privadas. Además, seguirán los reglamentos y lo que estipula la resolución de consejo universitario N° 0200-2018/UCV Pág. 2 y la resolución N° 011-2020-VI-UCV de la Universidad César Vallejo.

Adoptaremos una posición neutral y evitar contaminar los resultados con subjetividades; tomando en cuenta criterios de sensatez y nitidez, garantizando la privacidad de la opinión emitida por el personal que labora en la municipalidad de Miraflores. El estudio es de carácter de confidencialidad ya que los datos obtenidos de la municipalidad de Miraflores no se divulgarán, Además se validó la originalidad e integridad del estudio cumpliendo con el porcentaje de similitud obtenido con el software turnitin.

IV. RESULTADOS

4.1. Resultados descriptivos de la investigación

4.1.1. Resultados descriptivos de gestión de riesgo

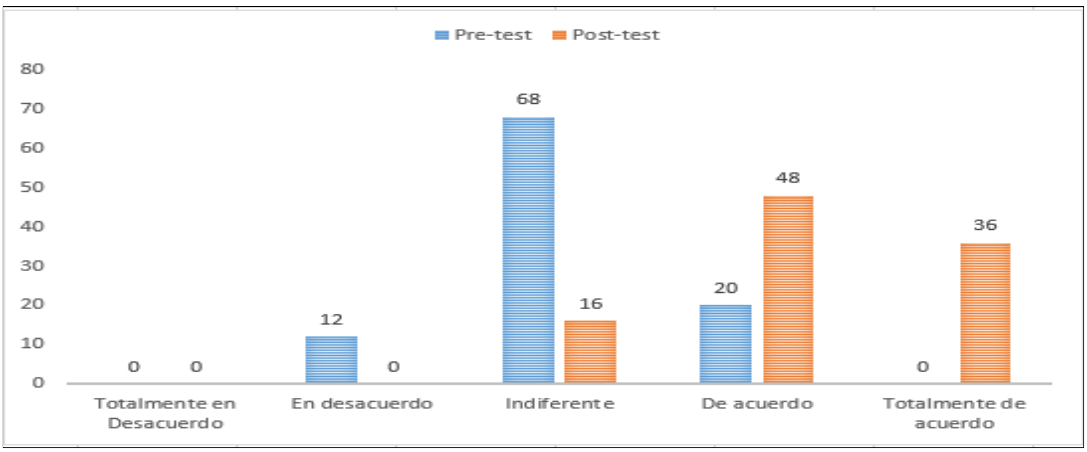
4.1.1.1. Resultados descriptivos de identificación de riesgo

En la tabla 3, se exponen los resultados del nivel de satisfacción de la Municipalidad de Miraflores, donde se presenta favorable del 28% (20% antes y 48% después) en el nivel *de acuerdo*, asimismo se visualiza una mejora significativa en el nivel *totalmente de acuerdo,* ya que antes de 0%, obtuvo un después de 36%. Estos resultados evidencian mejoras en la identificación de riesgos que presenta la aplicabilidad del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores (ver tabla 3).

Tabla 3. *Percepción del Usuario con respecto a la Identificación de* Riesgo

Niveles	Pre-test		Post-test	
	Frecuencia	Porcentaje	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0	0	0
En desacuerdo	3	12,0	0	0
Indiferente	17	68,0	4	16,0
De acuerdo	5	20,0	12	48,0
Totalmente de acuerdo	0	0	9	36,0
Total	25	100,0	25	100,0

Figura 4. percepción del usuario con respecto a la identificación de riesgo



Fuente: elFuente: elaboración propia

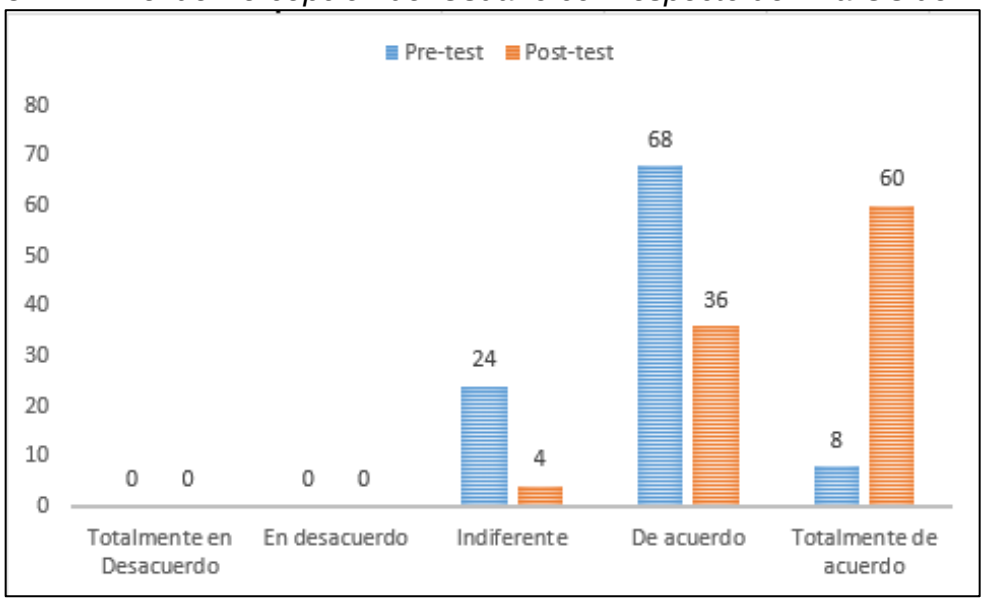
4.1.2 Resultados descriptivos de Análisis de riesgos

En la tabla 4, se muestra los resultados del nivel de satisfacción de los usuarios de la Municipalidad de Miraflores, donde se presenta favorable del 51% (8% antes y 60% después) en el nivel *de acuerdo*, aunque se evidencia un bajo porcentaje en el nivel *de acuerdo*, esto no afecta debido a que hay un mayor porcentaje en el nivel *totalmente de acuerdo* que sumado los dos niveles se da una diferencia de significación positiva de 20% (antes 76% después 96%). Estos resultados evidencian mejoras en el análisis de riesgos que presenta la aplicabilidad del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores (ver tabla 4).

Tabla 4. percepción del usuario con respecto de análisis de riesgo

Niveles	Pre-test		Post-test	
	Frecuencia	Porcentaje	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0	0	0
En desacuerdo	0	0	0	0
Indiferente	6	24,0	1	4,0
De acuerdo	17	68,0	9	36,0
Totalmente de acuerdo	2	8,0	15	60,0
Total	25	100,0	25	100,0

Figura 5. Nivel de Percepción del Usuario con respecto de Análisis de Riesgo



Fuente: elaboración propia

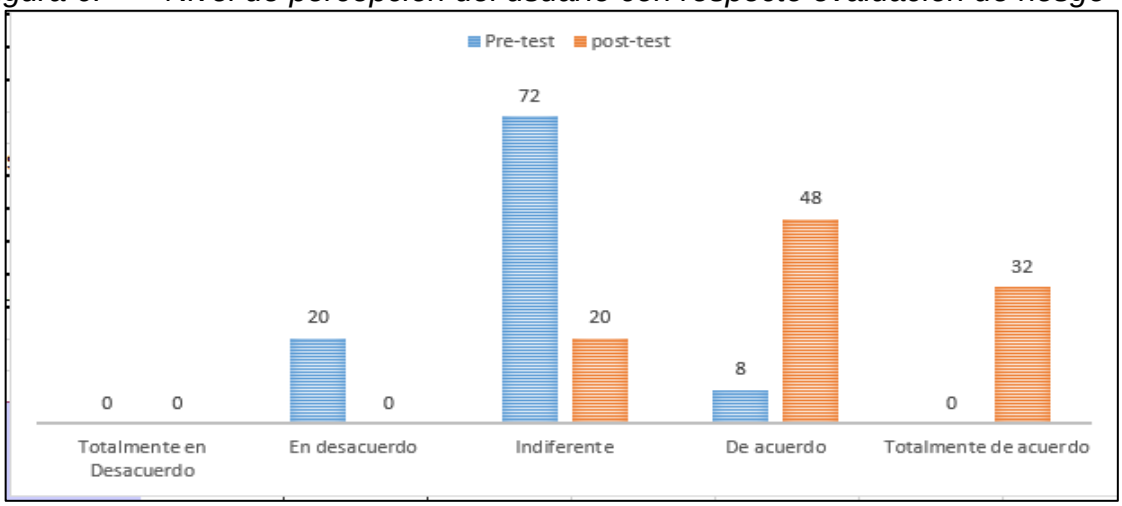
4.1.3 Resultados descriptivos de Evaluación de riesgos

En la tabla 5, los resultados de percepción de los usuarios de la Municipalidad de Miraflores, se presentan favorable del 40% (8% antes y 48% después) en el nivel *de acuerdo*, así mismo hubo una mejora significativa en el nivel *totalmente de acuerdo,* ya que antes de 0%, obtuvo un después de 32%. Estos resultados evidencian mejoras en la evaluación de riesgos que presenta la aplicabilidad del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores (ver tabla 5).

Tabla 5. percepción del usuario con respecto evaluación de riesgo

Niveles	Pre-test		Post-test	
	Frecuencia	Porcentaje	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0	0	0
En desacuerdo	5	20,0	0	0
Indiferente	18	72,0	5	20,0
De acuerdo	2	8,0	12	48,0
Totalmente de acuerdo	0	0	8	32,0
Total	25	100,0	25	100,0

Figura 6. Nivel de percepción del usuario con respecto evaluación de riesgo



Fuente: elaboración propia

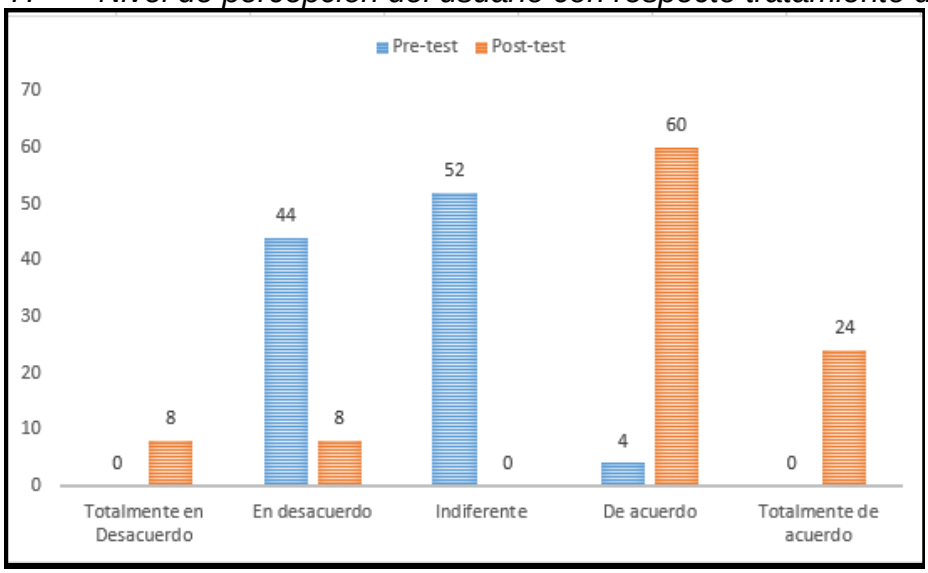
4.1.4 Resultados descriptivos de tratamiento de riesgos

En la tabla 6, se evidencia los resultados del nivel de satisfacción que tuvieron los usuarios de la Municipalidad de Miraflores encuestados, donde se presenta favorable del 36% (4% antes y 60% después) en el nivel *de acuerdo*, así mismo hubo una mejora significativa en el nivel *totalmente de acuerdo,* ya que antes de 6%, obtuvo un después de 24%. Estos resultados evidencian mejoras en la evaluación de riesgos que presenta la aplicabilidad del Marco de trabajo basado en la gestión unificada de amenazas (UTM) en la Municipalidad de Miraflores (ver tabla 6).

Tabla 6. percepción del usuario con respecto tratamiento de riesgo

Niveles	Pre-test		Post-test	
	Frecuencia	Porcentaje	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0	2	8,0
En desacuerdo	11	44,0	2	8,0
Indiferente	13	52,0	0	0
De acuerdo	1	4,0	15	60,0
Totalmente de acuerdo	0	0	6	24,0
Total	25	100	25	100,0

Figura 7. Nivel de percepción del usuario con respecto tratamiento de riesgo



Fuente: Elaboración propia

4.2 Resultados descriptivos de la investigación – seguridad de información

4.2.1 Resultados descriptivos – porcentaje de intentos de usuarios no autorizados

Con respecto al indicador porcentaje de intentos de usuarios no autorizados, se evidenció en la tabla 1, donde muestra que el promedio después de haber realizado el marco de trabajo (UTM) con respecto a la confidencialidad presento un óptimo rendimiento respecto al antes con valores de 15,95 y 96,67 respectivamente, por otro lado, la seguridad de los accesos a los usuarios no autorizados es mayor con 18,61, y los valores máximos y mínimos del después son superiores con valores 67,00 y 100,00, donde expresa que el Marco de trabajo basado en la gestión unificada de amenazas en municipalidades, ayudo a incrementar los bloqueos de navegación de usuarios no autorizados (ver tabla 7).

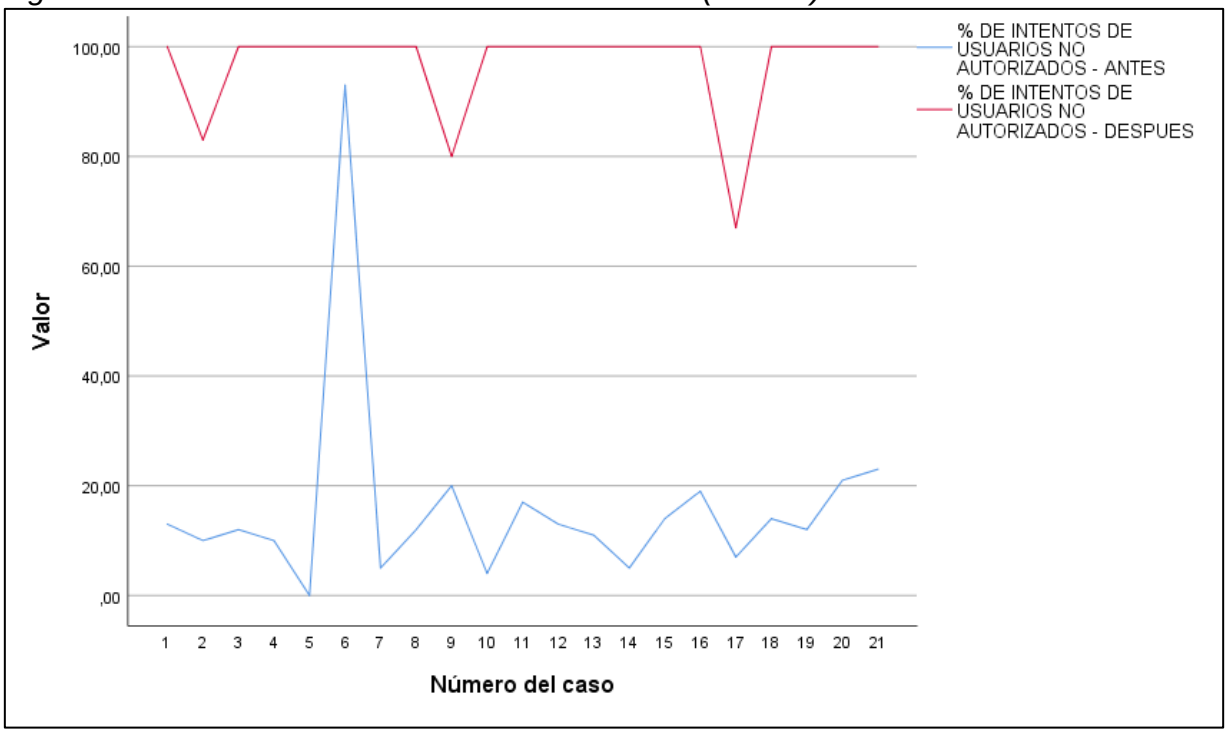
Tabla 7. Análisis descriptivos del Indicador (PIUNA)

Estadísticos	PIUNA_Antes	PIUNA_Después
N	21	21
Media	15,9524	96,6667
Mediana	12,0000	100,0000
Desv. Desviación	18,60504	8,78825
Mínimo	0,00	67,00
Máximo	93,00	100,00

Fuente: Elaboración propia

Los resultados reflejan que el equipo anterior UTM no estaba funcionando al 100% respecto a la dimensión confidencialidad el cual permitía navegar a paginas no autorizadas, figura 8, muestra los resultados antes y después de la implementación del marco de trabajo (línea azul) donde se observa la deficiencia del equipo anterior luego de la implementación la seguridad de bloqueo (línea roja), ha mejorado significativamente indicando que los usuarios no autorizados ya no pueden navegar libremente, esto mejoro de manera significativa(ver figura 8).

Figura 8. Estadísticos de líneas del Indicador (PIUNA)



Fuente: elaboración propia

4.2.2 Resultados descriptivos – porcentaje de amenazas detectadas

En este caso, porcentaje de amenazas detectadas, los resultados muestran (tabla 2) que el promedio después de haber realizado el marco de trabajo (UTM) con respecto a la confidencialidad presento un óptimo rendimiento respecto al antes con valores de 18,29 y 98,76 respectivamente, por otro lado, la seguridad a las amenazas detectadas es mayor que 7,07 con valores 93,00 (mínimos) y 100,00 (máximos), indicando que Marco de trabajo basado en la gestión unificada de amenazas en municipalidades, ayudo a controlar y detectar las amenazas(ver tabla 8).

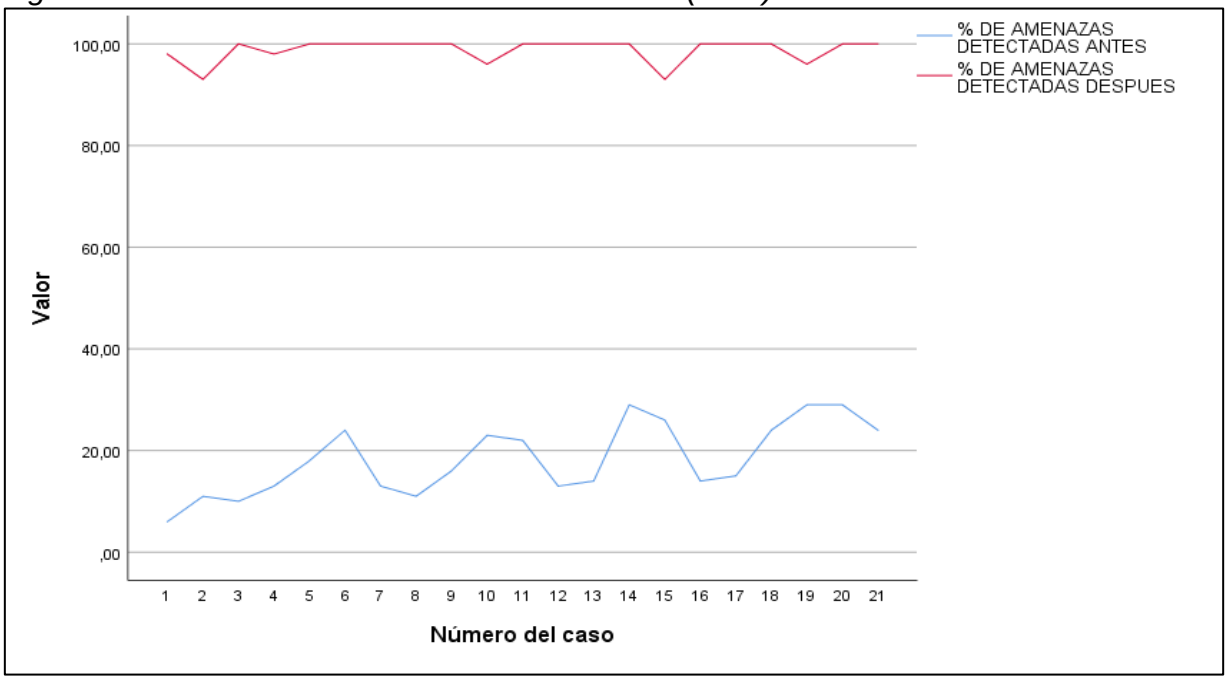
Tabla 8. Análisis descriptivos del Indicador (PAD)

Estadísticos	PAD_Antes	PAD_Después
N	21	21
Media	18,2857	98,7619
Mediana	16,0000	100,0000
Desv. Desviación	7,07208	2,30010
Mínimo	6,00	93,00
Máximo	29,00	100,00

Fuente: Elaboración propia

Los valores comparativos sobre indicador porcentaje de amenazas detectadas refleja que el equipo anterior UTM no estaba funcionando al 100%, respecto a la dimensión confidencialidad, el cual no permitía detectar las amenazas que afectan a la mayoría de equipos, la figura 9, nos muestra los resultados antes y después de la implementación del marco de trabajo (línea azul) donde se observa la deficiencia del equipo anterior, luego de la implementación, la seguridad ante amenazas incrementó favorablemente (línea roja)(ver figura 9).

Figura 9. Estadístico de líneas del Indicador (PAD)



Fuente: elaboración propia

4.2.3. Resultados descriptivos del porcentaje de incidencias en acceso de aplicaciones

Al referirnos al indicador porcentaje de incidencias en acceso de aplicaciones se evidencia en la tabla 10 que el promedio después de haber realizado el Marco de trabajo (UTM) con respecto a la integridad presento un óptimo rendimiento respecto al antes con valores de 2,14 y 0,19 respectivamente. Además, el porcentaje de incidencias en aplicaciones es 1,53 reflejando margen favorable, con valores 0,00 y 1,00 antes y después respectivamente, mostrando que marco de trabajo basado en la gestión unificada de amenazas en municipalidades, ayudó a disminuir significativamente las incidencias (ver tabla 9).

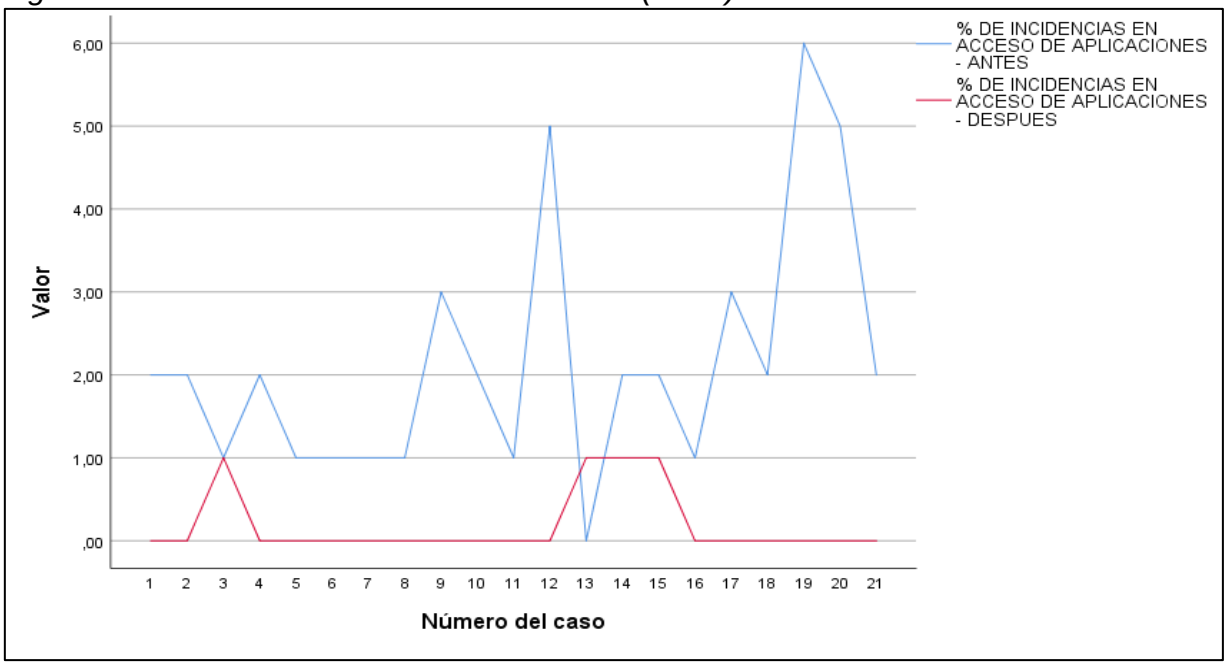
Tabla 9. Análisis descriptivos del Indicador (PIAA)

Estadísticos	PIAA_Antes	PIAA_Después
N	21	21
Media	2,1429	0,1905
Mediana	2,0000	0,0000
Desv. Desviación	1,52597	0,40237
Mínimo	0,00	0,00
Máximo	6,00	1,00

Fuente: Elaboración propia

Dichos resultados reflejan que el equipo UTM anterior no estaba funcionando al 100%, el cual, no permitía detectar las incidencias al acceso de aplicaciones, la figura 10, presenta que la información antes y después de la implementación del marco de trabajo (línea azul) se observa una deficiencia del equipo anterior, luego de la implementación la integridad mejoro significativamente (línea roja) (ver figura 10).

Figura 10. Estadístico líneas del Indicador (PIAA)



Fuente: elaboración propia

4.2.4 Resultados descriptivos – porcentaje de equipo de cómputo vulnerables

Con respecto a este indicador se presenta en la tabla 10, donde el promedio después de haber realizado el marco de trabajo (UTM) con respecto a la integridad presento un óptimo rendimiento de 4,19 y 1,0000 respectivamente. En referencia al porcentaje de equipos de cómputo vulnerables fue de 1,57 en ascenso al obtener y los valores superiores con valores 1,00 y 1,00 (máximos y mínimos), revelando que el UTM basado en la gestión unificada de amenazas en municipalidades, ayudo a reducir la vulnerabilidad de los equipos (ver tabla 10).

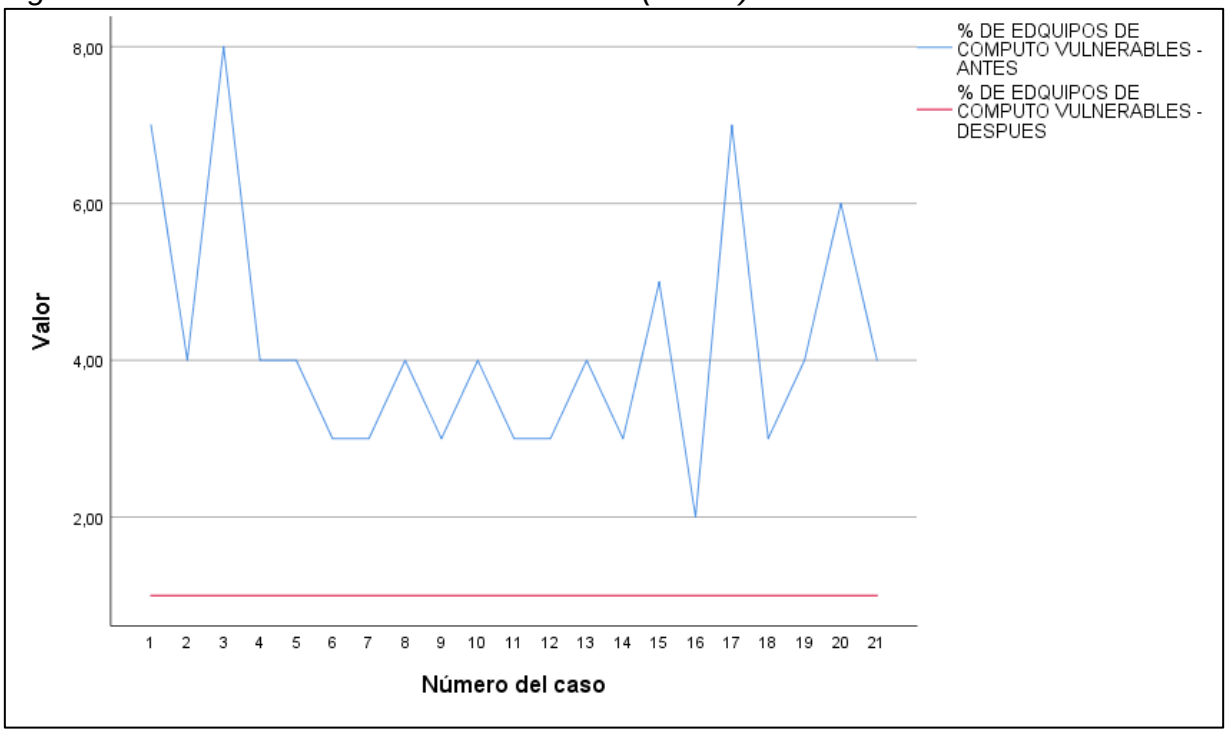
Tabla 10. Análisis descriptivos del Indicador (PECV)

Estadísticos	PECV_Antes	PECV_Después
N	21	21
Media	4,1905	1,0000
Mediana	4,0000	1,0000
Desv. Desviación	1,56905	0,00000
Mínimo	2,00	1,00
Máximo	8,00	1,00

Fuente: Elaboración propia

En figura 11, se muestra que el equipo UTM anterior no estaba funcionando al 100%, el cual no permitía detectar todas las vulnerabilidades de los equipos, la figura 8, exhibe que antes de la implementación del marco de trabajo (línea azul) se observa una deficiencia del equipo anterior, luego de la implementación de la dimensión integridad los equipos mejoro en la detección de vulnerabilidades favorablemente (línea roja) (ver figura 11).

Figura 11. Estadístico líneas del Indicador (PECV)



Fuente: elaboración propia

4.2.5 Resultados descriptivos – porcentaje de disponibilidad de los sistemas

Con respecto al indicador, se evidenció en la tabla 11, donde muestra que el promedio después de haber realizado el marco de trabajo (UTM) con respecto a la dimensión disponibilidad obtuvo valores de 88,62 y 99,67 respectivamente en el antes. En cambio, la disponibilidad de los sistemas es mayor con 29,59, y con valores 98,00 y 100,00 con respecto al después, indicando que ligeramente el UTM basado en la gestión unificada de amenazas en municipalidades, ayudó a incrementar la disponibilidad los sistemas (ver tabla 11).

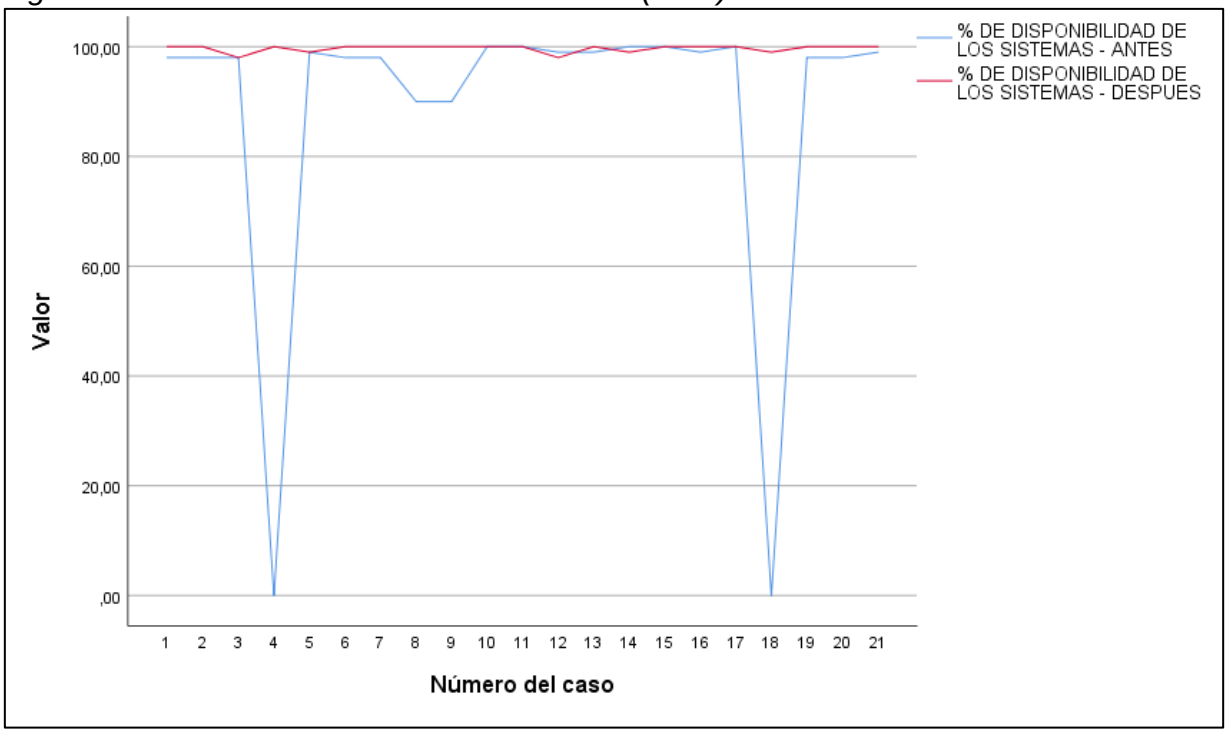
Tabla 11. Análisis descriptivos del Indicador (PDS)

Estadísticos	PDS_Antes	PDS_Después
N	21	21
Media	88,6190	99,6667
Mediana	98,0000	100,0000
Desv. Desviación	29,59134	0,65828
Mínimo	0,00	98,00
Máximo	100,00	100,00

Fuente: Elaboración propia

En la figura 12, se muestra que las políticas del equipo anterior UTM no estaba funcionando al 100 % respecto a la dimensión disponibilidad, el cual no permitía el ingreso a los sistemas publicados, la figura 12, se visualiza antes de la implementación del marco de trabajo (línea azul) tiene un ligero incremento del equipo anterior, luego de la implementación, la disponibilidad se incrementó ligeramente (línea roja) (ver figura 12).

Figura 12. Estadístico líneas del Indicador (PDS)



Fuente: elaboración propia

4.2.6 Resultados descriptivos – porcentaje de incidencias en el data center

Con respecto al indicador porcentaje de incidencias en el data center, en la tabla 12 muestra que el promedio después de haber realizado el marco de trabajo (UTM) con respecto a la dimensión disponibilidad presenta 28,19 y 3,05 respectivamente en el antes, con una disminución en las incidencias. Por otro lado, el porcentaje de incidencias en el data center es menor al antes con 18,63 con valores 0,00 (antes) y 33,00 (después), indicando que marco de trabajo basado en la gestión unificada de amenazas en municipalidades, ayudo a disminuir las incidencias en el data center (ver tabla 12).

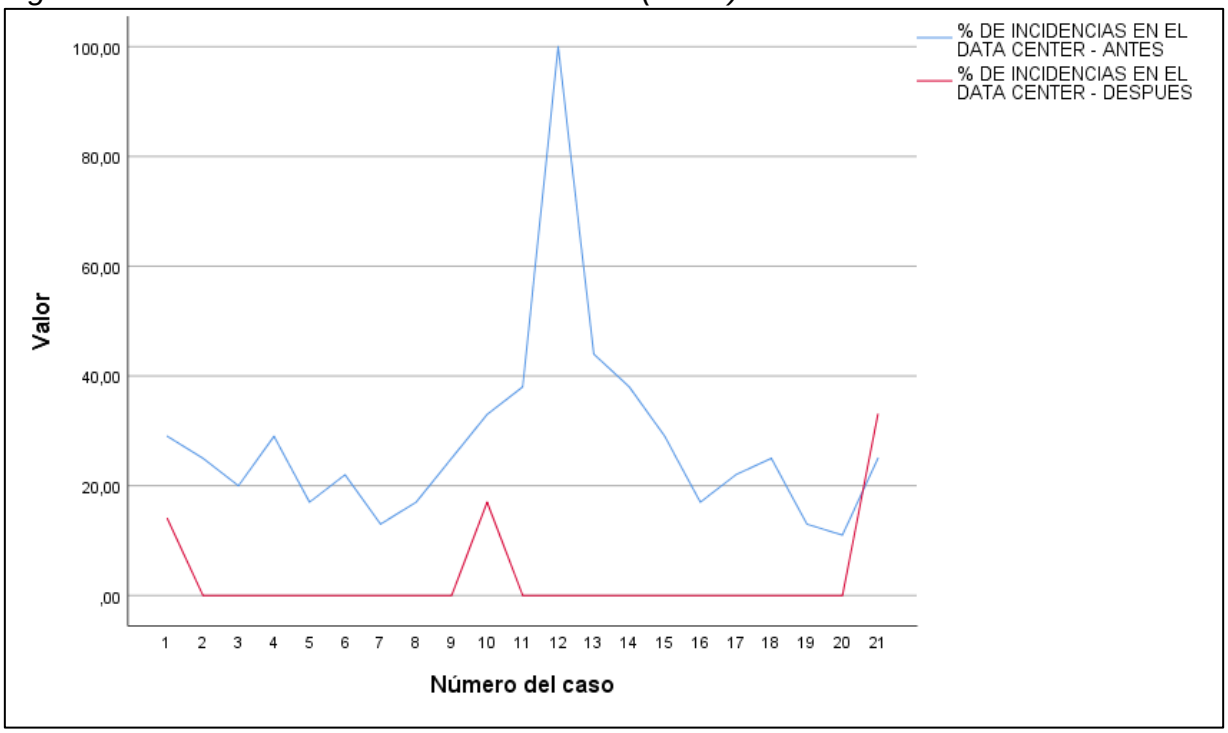
Tabla 12. Análisis descriptivos del Indicador (PIDC)

Estadísticos	PIDC_Antes	PIDC_Después
N	21	21
Media	28,1905	3,0476
Mediana	25,0000	0,0000
Desv. Desviación	18,62960	8,30347
Mínimo	11,00	0,00
Máximo	100,00	33,00

Fuente: Elaboración propia

En la figura 13, el porcentaje de incidencias en el data center reflejan que el equipo anterior UTM no detectaba las incidencias al 100%, respecto a la dimensión disponibilidad este disminuyo ligeramente con el antes, en la figura 1, se puede visualizar el antes de la implementación del marco de trabajo (línea azul) donde se observa la deficiencia del equipo anterior, luego de la implementación las incidencias en el data center (línea roja) disminuyo significativamente indicando que las incidencias bajaron (ver figura 13).

Figura 13. Estadístico líneas del Indicador (PIDC)



Fuente: elaboración propia

4.3 Resultados del contraste de hipótesis de la investigación

4.3.1 Análisis de normalidad de los datos – Shapiro-Wilk

Hipótesis de normalidad

Ho: Los datos analizados presentan una distribución normal

Ha: Los datos analizados no presentan una distribución normal

Análisis de normalidad Shapiro-Wilk

Se realizó la prueba de Shapiro-Wilk con muestra menor a 30 casos, donde se concluyó que la utilización de la estadística no paramétrica para todos. Adicionalmente se reconoció para todos los indicadores y las 3 dimensiones de la variable seguridad de información se ajustaban a poblaciones para muestras no paramétricas, por consiguiente, es necesario la aplicación de la prueba del Wilcoxon. Para el indicador porcentaje de intentos de usuarios no autorizados los resultados en sig = 0.000, fue menor que el valor del α = 0.05. Para el indicador porcentaje de amenazas detectadas del sig = 0.000, fue menor que el valor del α = 0.05. Y para el indicador porcentaje de incidencias de acceso aplicaciones de la dimensión integridad el valor del sig = 0,000, fue menor que el valor del α = 0.05. Para el siguiente indicador de la dimensión integridad, el porcentaje de equipos de cómputo vulnerables el valor del sig = 0.000, fue menor que el valor del α = 0.05. Para el siguiente indicador de la dimensión disponibilidad el porcentaje de disponibilidad de los sistemas el valor sig = 0.000, fue menor que el valor del α = 0.05. Por último, el indicador porcentaje de incidencias en el data center de la dimensión disponibilidad el valor del sig = 0.000, fue menor que el valor del α = 0.05. Dichos indicadores serán contrastados con 95% de confianza (ver tabla 13).

Tabla 13. Pruebas estadísticas de Shapiro Wilk

INDICADORES	Pre-test			Pos-test		
	Shapiro-Wilk			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Porcentaje de intentos de usuarios no autorizados	0.529	21	**0.000**	0.442	21	**0.000**
Porcentaje de amenazas detectadas	0.924	21	**0.103**	0.603	21	**0.000**
Porcentaje de incidencias de acceso aplicaciones	0.824	21	**0.002**	0.484	21	**0.000**
Porcentaje de equipos de cómputo vulnerables	0.909	21	**0.052**	0.761	21	**0.000**
Porcentaje de disponibilidad de los sistemas	0.403	21	**0.000**	0.564	21	**0.000**
Porcentaje de incidencias en el data center	0.873	21	**0.000**	0.432	21	**0.000**

4.4 Contraste de hipótesis - seguridad de información

4.4.1 Contraste de hipótesis – porcentaje de intentos de usuarios no autorizados

Formulación de hipótesis

Ho: $Me^1 = Me^2$: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) no es efectivo para la seguridad de información en la Municipalidad de Miraflores.

Ha: $Me^1 \neq Me^2$: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la seguridad de información en la Municipalidad de Miraflores.

Nivel de confianza

Nivel de confianza del 0.95 - Nivel de significancia del α=0.05

Regla de decisión

Rechazar la Ho si sig < α

Aceptar la Ho si sig > α

Estadística de prueba:

El estadístico utilizado es de la prueba de wilcoxon para muestras relacionadas (Sanchez, 2015, p. 18), porque las variables analizadas no cumplieron el supuesto de normalidad.

$$T = Min[T(+), T(-)]$$

Como T se ajusta a una distribución NORMAL se debe utilizar la fórmula:

$$Z = \frac{T - n(n+1)/4}{\sqrt{n(n+1)(2n+1)/24}}$$

Resultados del estadístico de prueba utilizando SPSS 26.0

Comparando los dos momentos de estudio de la variable porcentaje de intentos de usuarios no autorizados (pre-test y pos-test), el promedio del rango negativo ($\bar{x} = 11.00$) es mayor al positivo ($\bar{x} = 0.00$), esto implica que los resultados obtenidos del pos-test fueron superiores en 21 casos eficiencia, señalando que el marco de trabajo ayudó a incrementar la seguridad de información en la navegación de los usuarios, Asimismo, la suma de rango se inclina el resultado a favor del estudio (ver tabla 14).

Tabla 14. Estadístico wilcoxon del indicador (PIUNA)

Indicador		N	Rango promedio	Suma de rangos
Porcentaje de intentos de usuarios no autorizados Pre - Post	Rangos negativos	21[a]	11,00	231,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	21		

En la tabla 15, la prueba de wilcoxon, el sig = 0.000< α = 0.05, obteniendo que los porcentajes de usuarios no autorizados tienen diferencias favorables al estudio pre y post test.

Tabla 15. Prueba wilcoxon del indicador (PIUNA)

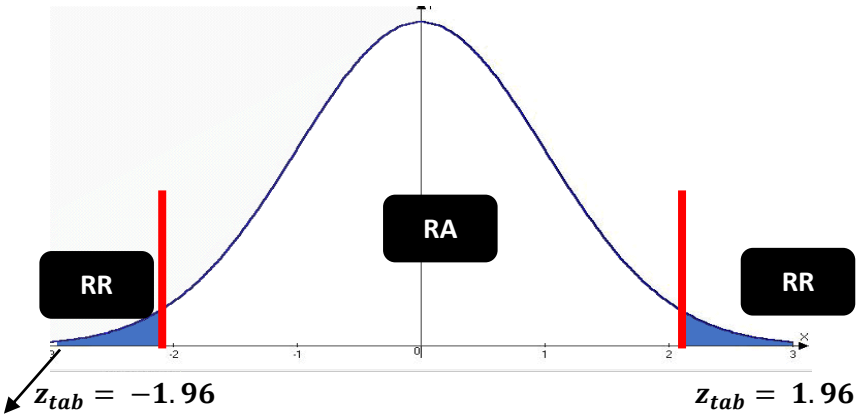
Prueba	porcentaje de intentos de usuarios no autorizados
Z	-4,017[b]
Sig. asintótica(bilateral)	**0,000**

Distribución de la estadística de prueba:

La prueba aproximada de normalidad distribuida como $Z_{tab}(1-\propto/2)$ se obtuvo como resultados $z_{tab}(0{,}95) = 1{,}96$. En la figura 14 se presenta la comparación

Zcal = -4,017(ver figura 14).

Figura 14. Campana de Gaus del Indicador (PIUNA)



Fuente: elaboración propia

En esta figura 14 el Zcal se posicionó en la región de rechazo, a favor de Ha. Esto indica que el marco de trabajo favoreció positivamente en el porcentaje de intentos de usuarios no autorizados con un 95% de confianza. Esto quiere decir que el intento de usuarios no autorizados bajo significativamente y se incrementó la seguridad de información en la municipalidad de Miraflores.

4.4.2 Contraste de hipótesis – porcentaje de amenazas detectadas

Formulación de hipótesis

Ho: $Me^1 = Me^2$: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) no es efectivo para la seguridad de información en la Municipalidad de Miraflores.

Ha: $Me^1 \neq Me^2$: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la seguridad de información en la Municipalidad de Miraflores.

Nivel de confianza

Nivel de confianza del 0.95 - Nivel de significancia del α=0.05

Regla de decisión

Rechazar la Ho si sig < α

Aceptar la Ho si sig > α

Estadística de prueba:

El estadístico utilizado es de la prueba de wilcoxon para muestras relacionadas (Sanchez, 2015, p. 18), porque las variables analizadas no cumplieron el supuesto de normalidad.

$$T = Min[T(+), T(-)]$$

Como T se ajusta a una distribución NORMAL se debe utilizar la fórmula:

$$Z = \frac{T - n(n+1)/4}{\sqrt{n(n+1)(2n+1)/24}}$$

Resultados del estadístico de prueba utilizando SPSS 26.0

Con respecto al porcentaje de amenazas detectadas (pre-test y pos-test), el resultado promedio el rango negativo ($\bar{x} = 11$) es superior al positivo ($\bar{x} = 0.0$). Esto implica que los resultados obtenidos en el pos-test fueron superiores en 21 casos, señalando que el marco de trabajo ayudó a detectar de forma eficiente las posibles amenazas (ver tabla 16).

Tabla 16. Estadístico wilcoxon del indicador (PAD)

Indicador		N	Rango promedio	Suma de rangos
% DE AMENAZAS DETECTADAS Pre - Post	Rangos negativos	21[a]	11,00	231,00
	Rangos positivos	0[b]	0,00	0,00
	Empates	0[c]		
	Total	21		

En la tabla 17, se presenta la prueba de wilcoxon, donde el sig = 0.000 < α = 0.05, y se evidencia que él porcentaje de amenazas detectadas respecto al antes y el después despliegan diferencia significativa donde se mejoró este criterio.

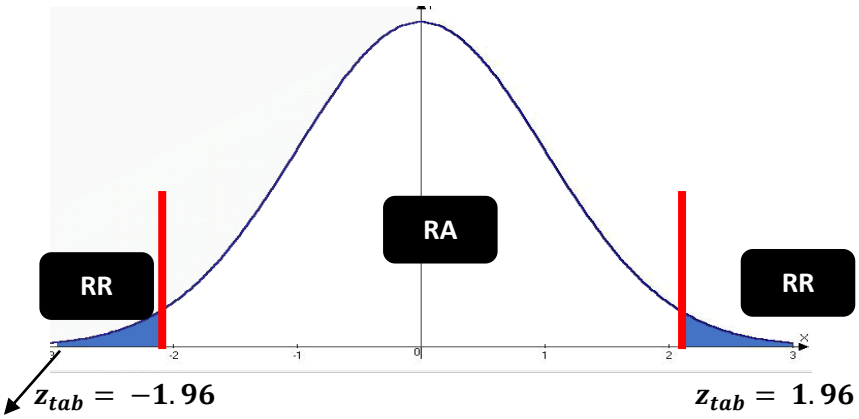
Tabla 17. Prueba de Wilcoxon del indicador (PAD)

Prueba	% DE AMENAZAS DETECTADAS
Z	-4,018[b]
Sig. asintótica(bilateral)	**0,000**

Distribución de la estadística de prueba:

La prueba aproximada de normalidad distribuida como $Z_{tab}(1-\propto/2)$, dando como valores $z_{tab}(0{,}95) = 1.96$. En este sentido, el resultado se comparó con el valor de Zcal = -4,018 y se representó en la campana de gaus (ver figura 15)

Figura 15. Campana de Gaus del Indicador (PAD)



Fuente: elaboración propia

En la figura 15, el resultado de Zcal está en región de rechazo, donde rechaza al Ho a favor de la Ha; por ello, se evidencia que el marco de trabajo favoreció en porcentaje de amenazas detectadas con un 95% de confianza. Esto quiere decir que el marco de trabajo detectará de forma eficiente las amenazas y mantendrá confidencialidad de la información en la municipalidad de Miraflores.

4.4.3 Contraste de hipótesis de % de incidencias en acceso de aplicaciones

Formulación de hipótesis

Ho: $Me^1 = Me^2$: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) no es efectivo para la seguridad de información en la Municipalidad de Miraflores.

Ha: $Me^1 \neq Me^2$: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la seguridad de información en la Municipalidad de Miraflores.

Nivel de confianza

Nivel de confianza del 0.95 - Nivel de significancia del α=0.05

Regla de decisión

Rechazar la Ho si sig < α

Aceptar la Ho si sig > α

Estadística de prueba:

El estadístico utilizado es de la prueba de wilcoxon para muestras relacionadas (Sanchez, 2015, p. 18), porque las variables analizadas no cumplieron el supuesto de normalidad.

$$T = Min[T(+), T(-)]$$

Como T se ajusta a una distribución NORMAL se debe utilizar la fórmula:

$$Z = \frac{T - n(n+1)/4}{\sqrt{n(n+1)(2n+1)/24}}$$

Resultados del estadístico de prueba utilizando SPSS 26.0

Los dos momentos de estudio del porcentaje de incidencias en accesos de aplicaciones, revela que el rango negativo ($\bar{x} = 10.79$) es superior al positivo ($\bar{x} = 5.00$); esto implica que los resultados del pretest fueron superiores en 19 casos y 1 caso no fue favorable, también hubo 1 empate, demostrando que el marco de trabajo ayudó a disminuir porcentaje de incidencias de acceso de aplicaciones. Así mismo la suma de rangos se inclina a favor del estudio (ver tabla 18).

Tabla 18. Estadístico wilcoxon del indicador (PIAA)

Indicador		N	Rango promedio	Suma de rangos
porcentaje de incidencias de acceso de aplicaciones Pre - Post	Rangos negativos	19[a]	10,79	205,00
	Rangos positivos	1[b]	5,00	5,00
	Empates	1[c]		
	Total	21		

En la tabla 19, la prueba de wilcoxon, el sig = 0.000< α = 0.05, se muestra que el porcentaje de incidencias en acceso de aplicaciones con el antes y el después presentan diferencia significativa y favorablemente al estudio.

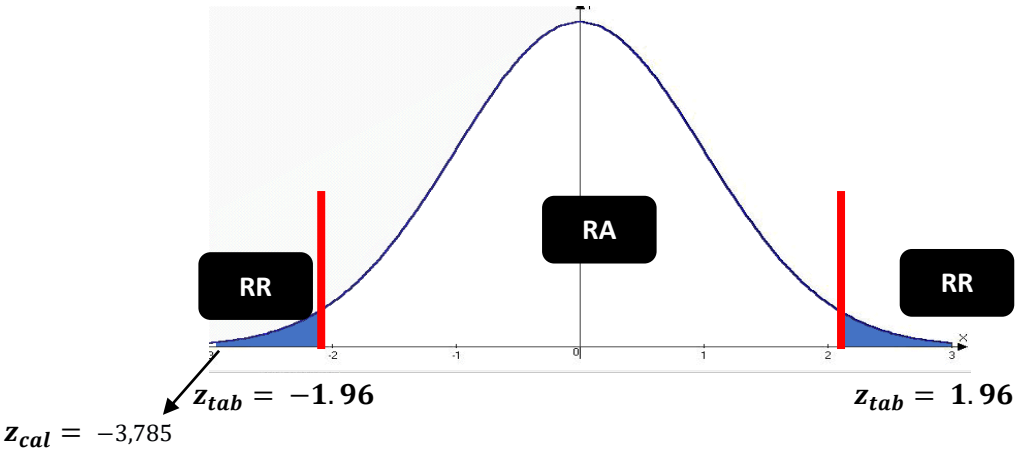
Tabla 19. Prueba Wilcoxon del indicador (PIAA)

Prueba	porcentaje de incidencias de acceso de aplicaciones
Z	-3,785[b]
Sig. asintótica(bilateral)	**0,000**

Distribución de la estadística de prueba:

Se manejó la prueba aproximada de normalidad distribuida como $Z_{tab}(1-\propto/2)$. Con resultado $z_{tab}(0{,}95) = 1.96$. Además, estos resultados de decisión se comparó con el valor de Zcal = -3,785 (ver figura 16).

Figura 16. Campana de Gaus del Indicador (PIAA)



Fuente: elaboración propia

En la figura 16, el resultado de Zcal se posiciona en la región de rechazo, en tal sentido, se rechaza el Ho y se aprueba la Ha, mostrando que existe suficiente evidencia estadística que el marco de trabajo contribuyó favorablemente en el porcentaje de incidencias en acceso de aplicaciones a con un 95% de confianza. Esto quiere decir que el marco de trabajo detectará de forma eficiente las incidencias en acceso de aplicaciones y mantendrá integridad de la información en la municipalidad de Miraflores.

4.4.4 Contraste de hipótesis de % de equipo de cómputo vulnerables

Formulación de hipótesis

Ho: $Me^1 = Me^2$: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) no es efectivo para la seguridad de información en la Municipalidad de Miraflores.

Ha: $Me^1 \neq Me^2$: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la seguridad de información en la Municipalidad de Miraflores.

Nivel de confianza

Nivel de confianza del 0.95 - Nivel de significancia del α=0.05

Regla de decisión

Rechazar la Ho si sig < α

Aceptar la Ho si sig > α

Estadística de prueba:

El estadístico utilizado es de la prueba de wilcoxon para muestras relacionadas (Sanchez, 2015, p. 18), porque las variables analizadas no cumplieron el supuesto de normalidad.

$$T = Min[T(+), T(-)]$$

Como T se ajusta a una distribución NORMAL se debe utilizar la fórmula:

$$Z = \frac{T - n(n+1)/4}{\sqrt{n(n+1)(2n+1)/24}}$$

Resultados del estadístico de prueba utilizando SPSS 26.0

El indicador porcentaje de equipos de cómputo vulnerables, indica el rango negativo ($\bar{x} = 11.00$) es superior al positivo ($\bar{x} = 0.0$), lo que implica que los resultados del pos-test fueron superiores en 21 casos, demostrando que el marco de trabajo contribuyó a disminuir el porcentaje de equipos de cómputo vulnerables, así mismo la suma de rangos se inclina a favor del estudio (ver tabla 20).

Tabla 20. Estadistico wilcoxon del indicador (PECV)

Indicador		N	Rango promedio	Suma de rangos
porcentaje de equipos de cómputo vulnerables Pre - Post	Rangos negativos	21[a]	11,00	231,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	21		

La tabla 21 evidencia el sig = 0.000< α = 0.05, con el porcentaje de equipos de cómputo vulnerables con diferencia significativa favorables al estudio.

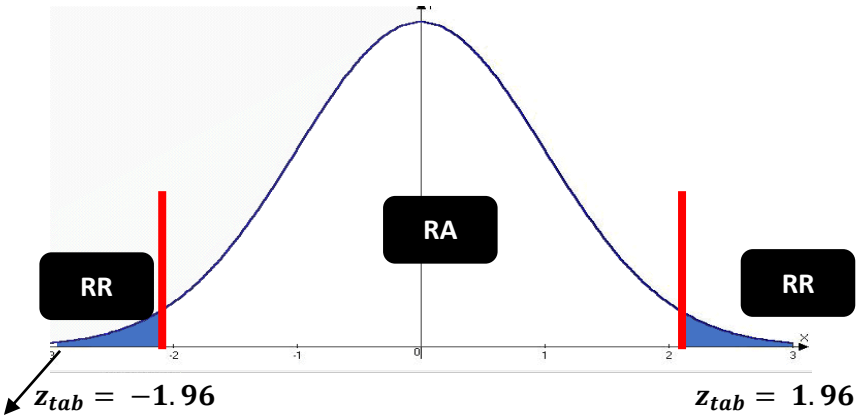
Tabla 21. prueba Wilcoxon del indicador (PECV)

Prueba	porcentaje de equipos de cómputo vulnerables
Z	-4,016[b]
Sig. asintótica(bilateral)	**0,000**

Distribución de la estadística de prueba:

Para la decisión del contraste de hipótesis se obtuvo $Z_{tab}(1-\propto/2)$ y para el reemplazo de valores $z_{tab}(0{,}95) = 1.96$. En este caso, el resultado se confrontó con Zcal = -4,016[b] obteniendo (ver la figura 17).

Figura 17. Campana de Gaus del indicador (PECV)



Fuente: elaboración propia

La figura 17, muestra que el resultado de Zcal está en la región de rechazo, rechazando al Ho y aprobando Ha; que se interpreta existencia suficiente de que el marco de trabajo favorece significativamente en el porcentaje de equipos de cómputo vulnerables (con 95% de confianza). esto quiere decir que los equipos de cómputo vulnerable se detectaran de forma eficiente y mantendrá integridad de la información en la municipalidad de Miraflores.

4.4.5 Contraste de hipótesis – porcentaje de disponibilidad de los sistemas

Formulación de hipótesis

Ho: $Me^1 = Me^2$: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) no es efectivo para la seguridad de información en la Municipalidad de Miraflores.

Ha: $Me^1 \neq Me^2$: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la seguridad de información en la Municipalidad de Miraflores.

Nivel de confianza

Nivel de confianza del 0.95 - Nivel de significancia del α=0.05

Regla de decisión

Rechazar la Ho si sig < α

Aceptar la Ho si sig > α

Estadística de prueba:

El estadístico utilizado es de la prueba de wilcoxon para muestras relacionadas (Sanchez, 2015, p. 18), porque las variables analizadas no cumplieron el supuesto de normalidad.

$$T = Min[T(+), T(-)]$$

Como T se ajusta a una distribución NORMAL se debe utilizar la fórmula:

$$Z = \frac{T - n(n+1)/4}{\sqrt{n(n+1)(2n+1)/24}}$$

Resultados del estadístico de prueba utilizando SPSS 26.0

El resultado indica que en promedio el rango negativo ($\bar{x} = 8.77$) es mayor al rango positivo ($\bar{x} = 3.00$), lo que implica que los resultados del pos-test fueron superiores en 13 casos demostrando que el marco de trabajo ayudó a incrementar el porcentaje de disponibilidad de los sistemas, y solo 2 casos no fueron favorables y 6 casos fueron empates, así mismo la suma de rangos el resultado inclina a favor del estudio (ver tabla 22).

Tabla 22. Estadístico de wilcoxon del indicador (PDS)

Indicador		N	Rango promedio	Suma de rangos
porcentaje de disponibilidad de los sistemas Pre - Post	Rangos negativos	13[a]	8,77	114,00
	Rangos positivos	2[b]	3,00	6,00
	Empates	6[c]		
	Total	21		

En la tabla 23. se presenta el sig = 0.000< α = 0.05, evidenciando que él porcentaje de disponibilidad de los sistemas presentan diferencia significativa favorables al estudio.

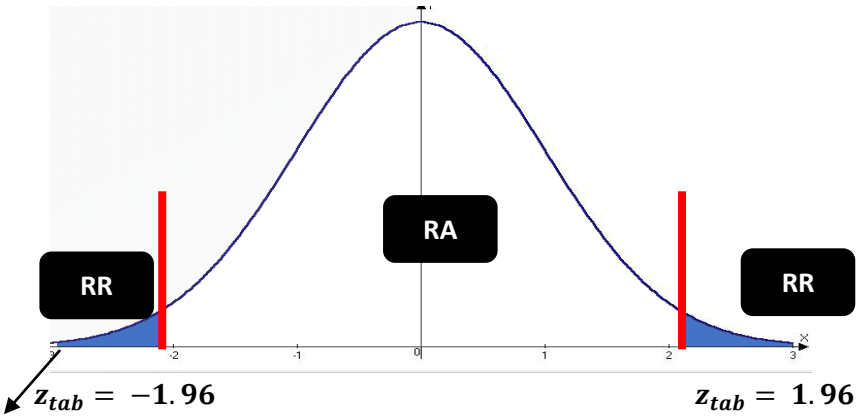
Tabla 23. prueba de Wilcoxon del indicador (PDS)

Prueba	porcentaje de disponibilidad de los sistemas
Z	-3,102[b]
Sig. asintótica(bilateral)	**0,000**

Distribución de la estadística de prueba:

La prueba aproximada de normalidad distribuida como $Z_{tab}(1-\propto/2)$. Al reemplazar los datos se obtuvo $z_{tab}(0{,}95) = 1.96$, donde se comparó con el valor de Zcal = -3,102[b] y se representó en la campana de gaus el cual se presenta a continuación (ver figura 18)

Figura 18. Campana de Gaus – del Indicador (PDS)



Fuente: elaboración propia

La figura 18, muestra que el resultado de Zcal está en la región de rechazo, rechazando Ho y aprobando Ha; en tal sentido, se concluye que existe suficiente evidencia que el marco de trabajo favoreció positivamente en el porcentaje de disponibilidad de los sistemas en la municipalidad de Miraflores.

4.4.6 Contraste de hipótesis – porcentaje de incidencias en el data center

Formulación de hipótesis

Ho: $Me^1 = Me^2$: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) no es efectivo para la seguridad de información en la Municipalidad de Miraflores.

Ha: $Me^1 \neq Me^2$: El Marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la seguridad de información en la Municipalidad de Miraflores.

Nivel de confianza

Nivel de confianza del 0.95 - Nivel de significancia del α=0.05

Regla de decisión

Rechazar la Ho si sig < α

Aceptar la Ho si sig > α

Estadística de prueba:

El estadístico utilizado es de la prueba de wilcoxon para muestras relacionadas (Sanchez, 2015, p. 18), porque las variables analizadas no cumplieron el supuesto de normalidad.

$$T = Min[T(+), T(-)]$$

Como T se ajusta a una distribución NORMAL se debe utilizar la fórmula:

$$Z = \frac{T - n(n+1)/4}{\sqrt{n(n+1)(2n+1)/24}}$$

Resultados del estadístico de prueba utilizando SPSS 26.0

El resultado indica que en promedio el rango negativo ($\bar{x} = 11.50$) es elevado con respecto al positivo ($\bar{x} = 1.00$), lo que implica que los resultados del pos-test fueron superiores en 20 casos, demostrando que el marco de trabajo permitió a disminuir las incidencias en el data center y solo 1 caso no fue favorable donde se concluye que la suma de rango inclina a favor del estudio (ver tabla 24).

Tabla 24. Estadístico wilcoxon del indicador (PIDC)

Indicador		N	Rango promedio	Suma de rangos
porcentaje de incidencias en el data center Pre - Post	Rangos negativos	20[a]	11,50	230,00
	Rangos positivos	1[b]	1,00	1,00
	Empates	0[c]		
	Total	21		

La tabla 25, el sig = 0.000< α = 0.05, demostrando de esta manera que el porcentaje de incidencias en el data center presentan discrepancia significativa de manera favorable al estudio (ver tabla 25).

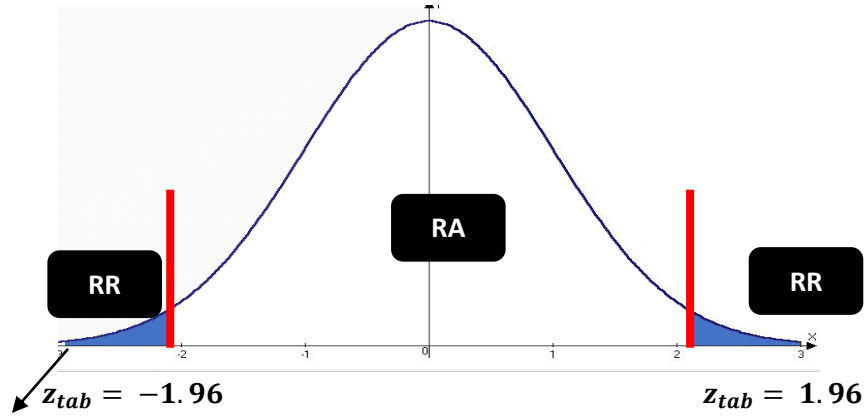
Tabla 25. prueba de Wilcoxon del indicador (PIDC)

Prueba	% DE INCIDENCIAS EN EL DATA CENTER
Z	-3,983[b]
Sig. asintótica(bilateral)	**0,000**

Distribución de la estadística de prueba:

La normalidad distribuida utilizada fue $Z_{tab}(1-\propto/2)$. Aplicado al estudio se tuvo como resultados $z_{tab}(0{,}95) = 1.96$. En este sentido, el resultado se comparó con el valor de Zcal = -3,983[b] y se representó gráficamente (ver figura 19)

Figura 19. Campana de Gaus – del Indicador (PIDC)



Fuente: elaboración propia

En la figura 19, el Zcal está ubicado en la región de rechazo, siendo Ho rechazado a favor de la Ha, donde se concluye, que existe suficiente evidencia estadística que el marco de trabajo contribuyó favorablemente en el porcentaje de incidencias en el data center al 95% margen de confianza. Permitiendo detectar las incidencias que puedan ocurrir en la disponibilidad de la municipalidad de Miraflores.

V. DISCUSIÓN

Los resultados del estudio fueron que existe una eficacia en la aplicabilidad del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de la información en la Municipalidad de Miraflores abarcando la confidencialidad, integridad y disponibilidad de información. En este sentido aplicar marcos de trabajo permite conocer el nivel de la seguridad de información de una institución; siendo esto avalado por el estudio realizado por Alvarado y Sánchez (2020) en su investigación concluyen que los controles de la seguridad implementados fueron la base primordial para establecer mejoras en el nivel seguridad en el proceso de desarrollo de sistemas y del producto. En cambio, en el estudio de Niño (2018) se aplicó la metodología MAGERIT, permitiéndonos conocer las amenazas a las cuales se hayan expuesto los activos de información en ODEI Lambayeque, obteniendo que el nivel de madurez en seguridad era muy bajo.

Los resultados obtenidos con respecto a la confidencialidad fueron que el valor de significancia es de 0,000 para porcentaje de Intentos de usuarios no autorizados y un 0,000 en porcentaje de amenazas detectadas; siendo menor al nivel de significación 0,05, proporcionando el marco de trabajo basado en la gestión unificada de amenazas (UTM) confidencialidad de la información en la Municipalidad de Miraflores. Esto también se refleja en los resultados del cuestionario aplicado al personal encuestado, al obtener un 72% sobre la consulta al marco de trabajo con respecto a la determinación de amenazas. Dichos resultados son avalados por los que expresa Montecé, Verdesoto y Vargas (2017) en su investigación, que expresa que toda institución debe diseñar controles de seguridad y prestar la correcta confidencialidad y control de acceso a los datos; siendo importante para la protección de la información.

Los resultados obtenidos con respecto a la integridad fueron que el valor de significancia es de 0,000 para porcentaje de incidencias en acceso de aplicaciones y un 0,000 en porcentaje de equipos de cómputos vulnerables; proporcionando el marco de trabajo basado en la gestión unificada de amenazas (UTM) en el aspecto de integridad de la información en la Municipalidad de Miraflores. Esto también se refleja en los resultados del cuestionario aplicado al personal encuestado, al obtener un 72% sobre la consulta al marco de trabajo con respecto a la

vulnerabilidad de cada equipo. Estos resultados fueron avalados por Chaverra, (2021) que indican es importante contar con un esquema fehaciente y eficaz que resguarde las bases de datos internas y evite que esta información se manipule indebidamente.

Los resultados obtenidos con respecto a la integridad fueron que el valor de significancia es de 0,000 para porcentaje de disponibilidad de los sistemas y un 0,000 en porcentaje de incidencias en el data center; proporcionando el marco de trabajo basado en la gestión unificada de amenazas (UTM) disponibilidad de la información en la Municipalidad de Miraflores. Esto también se refleja en los resultados del cuestionario aplicado al personal encuestado, al obtener un 84% sobre la consulta al marco de trabajo con respecto evaluación exhaustiva de los riesgos. Estos resultados están dentro del contexto que expresa Mendoza (2018 donde exponen que la implementación del Sistema de Gestión de Seguridad de la Información es significativa para mantener la información al alcance del personal autorizado proporcionando disponibilidad de información.

VI. CONCLUSIONES

Luego de realizar esta investigación y posteriormente haber obtenido los resultados del estudio, se llegó a las siguientes conclusiones respecto a los objetivos planteados:

- ✓ Se determinó la eficacia del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la confidencialidad de la información en la Municipalidad de Miraflores en los indicadores de estudio porcentaje de Intentos de usuarios no autorizados y porcentaje de amenazas detectadas; que definen la protección de la información sobre el acceso a la infraestructura tecnológica y por consiguiente a los datos institucionales.
- ✓ También, se detectó la eficacia del marco de trabajo basado en la gestión unificada de amenazas (UTM) para la integridad de la información en la Municipalidad de Miraflores en los indicadores de estudio sobre él porcentaje de incidencias en acceso de aplicaciones y el porcentaje de equipos de cómputos vulnerables; donde se puede preservar en un significativo porcentaje la minimización de los riesgos.
- ✓ Finalmente, se concluye que se determinó la eficacia del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la disponibilidad de la información en la Municipalidad de Miraflores en los indicadores de estudio porcentaje de disponibilidad de los sistemas y porcentaje de incidencias en el data center al proveer las alertas a los usuarios autorizados.
- ✓ Los resultados obtenidos a nivel general demuestran la eficacia del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de la información en la Municipalidad de Miraflores abarcando la confidencialidad, integridad y disponibilidad de información siendo un aporte fundamental para la mejora de los niveles de seguridad institucional en el área de Tecnología de la información.

VII. RECOMENDACIONES

Luego de obtener los resultados y de haberse cumplido los objetivos de la investigación, se realizó las siguientes recomendaciones:

- ✓ Realizar un monitoreo constante del acceso a los recursos de la infraestructura tecnológica a través del Marco de trabajo basado en la gestión unificada de amenazas (UTM).

- ✓ Planificar la aplicabilidad constante en el criterio de integridad sobre Marco de trabajo gestión unificada de amenazas (UTM) a fin de preservar y mantener el mejor funcionamiento de los procesos y la exactitud de la información.

- ✓ Garantizar continuamente el acceso de la información a través del uso del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la disponibilidad de la información en la Municipalidad de Miraflores.

- ✓ Realizar mejoras continuas al Marco de trabajo basado en la gestión unificada de amenazas (UTM) para ajustarlos a las necesidades actuales de la Municipalidad de Miraflores.

REFERENCIAS

ALBAN, Víctor ; SOLER, Rafael H. y ONATE, Alejandra. The Theory Of Networks And Risks Management. Scielo Revista Universidad y Sociedad [en linea]. Julio, 2018. vol.10 no.4. [Fecha de consulta: 01 de enero de 2022]. Disponible en: http://scielo.sld.cu/pdf/rus/v10n4/2218-3620-rus-10-04-239.pdf

ISSN 2218-3620

ALVARADO, Gaby y SÁNCHEZ, Miryam. Seguridad de la información en el proceso de desarrollo de sistemas y del producto mediante la implementación de controles de seguridad basado en la norma ISO 27002:2015 en la empresa BITNESS CORP S.A.C., 2020. ((Título profesional de: Ingeniero en Sistema).). Lima: Universidad Peruana Unión, 2020, 120 pp.

ANDINA. 2022. Perú sufrió más de 11.5 mil millones de intentos de ciberataques en 2021. Agencia Peruana de Noticias. [Fecha de consulta: 10 de enero de 2022]. Disponible en: https://andina.pe/agencia/noticia-peru-sufrio-mas-115-mil-millones-intentos-ciberataques-2021-881221.aspx.

ARIAS-GÓMEZ, Jesús; VILLASÍS-KEEVER, Miguel Ángel; MIRANDA NOVALES, María Guadalupe. El protocolo de investigación III: la población de estudio Revista Alergia México [en línea]. Junio, 2016, Vol. 63. [Fecha de consulta: 15 de enero de 2022]. Disponible en: https://www.redalyc.org/pdf/4867/486755023011.pdf

ISSN: 0002-5151

ARIAS, Jesús; VILLASÍS, Miguel; MIRANDA, María. El protocolo de investigación III: la población de estudio Revista Alergia México [en línea]. Junio, 2016, Vol. 63. Fecha de consulta: 15 de enero de 2022]. Disponible en: https://www.redalyc.org/pdf/4867/486755023011.pdf

ISSN: 0002-5151

AVENDAÑO, Alexander, DIAZ, David y TAFUR, Miguel. Análisis de Seguridad Perimetral en la Empresa Servitiendas de Colombia y Dsurtiend". (Título profesional de: Ingeniero en Sistema). Neiva: Universidad Cooperativa de Colombia. Neiva.2019, 45 pp.

BORGHELLO, Cristhian. Seguridad Informática - Implicancias E Implementación. Título profesional de: Ingeniero en Sistema). Universidad Politécnica de Valencia. 2019, 145 pp.

CALDERÓN, Daniel, TOVAR, Jhon Y GARCÍA, Leonardo (2019), titulado “Sistema de Seguridad Perimetral en la Empresa Jfc Eléctrica Engineering S.A.S”. (Título profesional de: Ingeniero en Sistema). Neiva: Universidad Cooperativa de Colombia. Neiva.2019, 98 pp.

CABRERA, Sandra, GARCIA, María y SALINAS, Juan. Modelo de Seguridad en Aplicaciones Web. (Título de Ingeniero en Informática). Mexico: Instituto Politecnico Nacional. 2019, 133 pp

CHAVERRA BARCO, Jilmar (2021), Implementación de sistema de gestión de la seguridad de la información para el aseguramiento del proceso de ingreso de notas en un portal web universitario. (Título de Ingeniero De Sistemas). Colombia: Universidad de San Buenaventura.

CURIOSO, Walter y ESPINOZA Elizabeth. Framework For The Strengthening Of Health Information Systems In Peru. Rev Peru Med Exp Salud Publica. [en línea]. 2015, Disponible en: http://www.scielo.org.pe/pdf/rins/v32n2/a19v32n2.pdf

FLÓREZ, Wilmar, ARBOLEDA, Carlos, CADAVID, John. Solución Integral de Seguridad para las Pymes mediante un UTM. USBMed, Vol. 3, No. 1, 2018. , pp. 35-42. Disponible en: https://revistas.usb.edu.co/index.php/IngUSBmed/article/view/262/176.

ISSN: 2027-5846.

GARCIA, Marcos (2021). Estudio de Factibilidad Para Implementación de Seguridad Perimetral Mediante Cámaras de Video Vigilancia en la Universidad Estatal del sur de Manabi (Título profesional de: Ingeniero en Sistema Computacionales). Jipijapa: Universidad Estatal del Sur de Manabí. 2021, 111pp.

GARCÍA, Juan. Las TIC en la pandemia Covid-19. Revista Nuevo Hospital. Vol. XVI (1 extra). [en línea]. 2020, Vol. XVI (1 extra). Fecha de consulta: 17 de enero de 2022]. Disponible en: https://www.saludcastillayleon.es/CAZamora/en/publicaciones/revista-nuevo-hospital-2020/nuevo-hospital-2020-junio-xvi-1-extraordinario-covid19/garcia-

vazquez-jc-las-tic-en-la-pandemia-covid-19-nuevo-hos.files/1638993-NUEVO%20HOSPITAL%202020%20Junio%3BXIV%20extraordinario%20COVID-13-14.pdf

ISSN:1578-7516

ICE Ciberataques en Latinoamérica aumentaron un 38% en 2021. [en línea]. Junio, 2022, [Fecha de consulta: 19 de enero de 2022]. Disponible en: https://ice.lat/blog/2022/01/20/ciberataques-en-latinoamerica-aumentaron-un-38-en-2021/.

HERNÁNDEZ, Roberto y MENDOZA, Christian. Metodología de la investigación: las rutas cuantitativas, cualitativas y mixta. 1ª ed. México: McGRAW-HILL interamericana editores. 2018. 753 pp.

ISBN: 9781456260965

HERNÁNDEZ, Roberto, FERNÁNDEZ, Carlos y BAPTISTA, María. Metodología de la investigación. 6ª ed. México: McGRAW-HILL interamericana editores. 2014. 634 pp.

ISBN: 9781456223960

KASPERSKY. ¿Qué es la gestión unificada de amenazas (UTM)?. 2021.. [Fecha de consulta: 21 de marzo de 2022]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/utm

KAZMIER, Leonardo. Estadística Aplicada a la Administración y la Economía. [en línea]. 2015. [Fecha de consulta: 21 de enero de 2022]. Disponible en: https://es.scribd.com/document/472912571/Estadistica-Aplicada-a-La-Administracion-y-La-Economia-Leonard-J-Kazmier-espanol-pdf

KRISHNAN, Grecia, & RAVINDRAN, Venicia. (2018). IT service management automation and its impact to IT industry. ICCIDS 2017 -International Conference on Computational Intelligence in Data Science, Proceedings–Janua, 5–8. https://doi.org/10.1109/ICCIDS.2017.8272633.

LACAVE, C.; MOLINA, A.; FERNÁNDEZ, M.; Redondo, M. Análisis de la confianza y validez de un cuestionario docente. En XXI Jornadas de la Enseñanza Universitaria de la Informática. Andorra La Vella. [en linea]. 2021. [Fecha de

consulta: 21 de enero de 2022]. Disponible en: https://upcommons.upc.edu/bitstream/handle/2117/76844/JENUI2015_146-153.pdf?sequence=1&isAllowed=y

ISBN: 978-99920-70-10-9

LEIVA, Eduardo. Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. Revista Latinoamericana de Ingeniería de Software. [en linea]. 2015, Vol. 3 [Fecha de consulta: 21 de enero de 2022]. Disponible en: http://revistas.unla.edu.ar/software/article/view/775

DOI: https://doi.org/10.18294/relais.2015.161-176

LEÓN, Orfelio. y MONTERO, Ignacio. Métodos de investigación en psicología y educación. 3ª ed. Madrid: McGraw-Hill/Interamericana de España, 2002. 394 pp.

ISSN: 1697-2600

LOZADA, J. Investigación Aplicada. CienciAmérica: Revista de divulgación científica de la Universidad Tecnológica Indoamérica. [en linea]. 2014, Vol. 3 [Fecha de consulta: 18 de enero de 2022]. Disponible en: http://cienciamerica.uti.edu.ec/openjournal/index.php/uti/article/view/30/23

ISSN-e 1390-9592

MARTÍNEZ, Rosalba; BLANCO, María. Risk management: from an emerging business management approach. Revista Venezolana de Gerencia. [en linea]. 2017, Vol. 22 [Fecha de consulta: 23 de enero de 2022]. Disponible en: https://www.redalyc.org/journal/290/29055967009/29055967009.pdf

ISSN: 1315-9984

MENDOZA, José, PÉREZ , Marcos y GRIMÁN, Jesús (2005). Prototype of Software Quality Systemic Model (SQSM). [en linea]. 2017, Vol. 8 [Fecha de consulta: 23 de enero de 2022]. Disponible en: https://www.redalyc.org/pdf/615/61580304.pdf

ISSN: . ISSN 1405-5546.

JARA - MENDOZA, Omar Yino (2018). Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018. (Título de Ingeniero De Sistemas) Perú: Universidad Cesar Vallejo.

MONTECÉ – MOSQUERA, Flranklin W.; VERDESOTO-ARGUELLO, Alexis E.; VARGAS-MARÍN, Hugo J. (2017). Software de seguridad que permita la confidencialidad de los datos del sistema de gestión y servicios académicos para planteles de educación media (SiViSA). Dom. Cien., ISSN: 2477-8818. Vol. 3(3). pp. 91-107.

NIÑO,Nilton Roger (2018). Modelo de un Sistema de Gestión de Seguridad de Información – Sgsi, para Fortalecer La Confidencialidad, Integridad, Disponibilidad Y Monitorear los activos de información para el Instituto Nacional de Estadística E Informática - Inei Filial Lambayeque. (Tesis de Postgrado). Perú: Universidad Nacional “Pedro Ruiz Gallo” Escuela De Postgrado. Lambayeque.

NormasISO. ISO 27001. Seguridad de la Información [en linea]. 2022, [Fecha de consulta: 23 de enero de 1996]. Disponible en: https://www.normas-iso.com/iso-27001/

PRUNA, Francisco y YARAD, Pamela y CARRION, Joe. Analysis Of The Characteristics Of The Microenterprise Sector In Latin America And Its Limitations In The Adoption Of Technologies For Information Security. Revista Científica ECOCIENCIA. [en linea]. 2020, Vol. 7 [Fecha de consulta: 23 de enero de 2022]. Disponible en: https://revistas.ecotec.edu.ec/index.php/ecociencia/article/view/303/233

ISSN: 1390-9320

PEÑUELA, Yini, (2018). Análisis e identificación del estado actual de la seguridad informática, dirigido a las organizaciones en Colombia, que brinde un diagnóstico general sobre la importancia y medidas necesarias para proteger el activo de la información (Monografía de investigación). Colombia: Universidad abierta y a distancia, Fusagasugá, 2018, 60 pp.

PMI (2017): A guide to the project management body of knowledge (Guía PMBoK), 6ª edición. Pensilvania, Project Management Institute.

REYNA, Daniel, y OLIVERA, Daniel. Las amenazas cibernéticas. México: Editorial Universidad de Xalapa. [en linea]. 2020, Vol. 7 [Fecha de consulta: 23 de enero de 2022]. Disponible en: https://ux.edu.mx/wp-content/uploads/11-LIBRO-CIBERSEGURIDAD-ilovepdf-compressed-1.pdf

RÍO Abel, y CARDENAS, Beitmantt. Systems dynamics, a way to optimize risk management. Revista EAN, Edición especial, Revista EAN. [en linea]. 2021, Edición especial [Fecha de consulta: 23 de enero de 2022]. Disponible en: https://journal.universidadean.edu.co/index.php/Revista/article/view/2021/1811ISSN: 1390-9320

DOI: https://doi.org/10.21158/01208160.n0.2018.2021

SAARI, Jorma. Políticas de Seguridad y Liderazgo. [en linea]. 2021, [Fecha de consulta: 13 de enero de 2022]. Disponible en: https://www.insst.es/documents/94886/162520/Cap%C3%ADtulo+59.+Pol%C3%ADtica+de+seguridad+y+liderazgo.

ROCHA, Cristhian. La Seguridad Informática. Revista Ciencia Unemi, vol. 4(5). [en linea]. 2011, Vol. 7 [Fecha de consulta: 23 de marzo de 2022]. Disponible : https://www.redalyc.org/pdf/5826/582663867004.pdf

ROMERO, Martha, FIGUEROA, Grace VERA, Denisse. Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. 3 Ciencias. Editorial Área de Innovación y Desarrollo, S.L. [en linea]. 2018, Vol. 10 [Fecha de consulta: 23 de enero de 2022]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

ISBN: 978-84-949306-1-4

ROMERO Martha, FIGUEROA, Grace, VERA, Denisse, ÁLAVA José, PARRALES Galo, ÁLAVA Christian, MURILLO, Ángel, CASTILLO, Miriam. Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. [en línea]. 2018. ISBN: 978-84-949306-1-4 DOI: http://dx.doi.org/10.17993/IngyTec.2018.46.

RUIZ, Kenny y DELGADO, Wilson. Implementación de una Solución de Seguridad Perimetral Open Source en la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo. Tesis (Título de Ingeniero De Sistemas). Chiclayo: Universidad De Lambayeque, 2018. 69 pp.

SANCHEZ, Reinaldo. Prueba de Wilcoxon-Mann-Whitney: mitos y realidades. Rev Mex Endocrinol Metab Nutr. 2015; V (2):18-21. Fecha de consulta: 17 de marzo de 2022]. Disponible en: https://biblat.unam.mx/hevila/Revistamexicanadeendocrinologiametabolismo&nutricion/2015/vol2/no1/3.pdf

SÁNCHEZ-CASANOVA, Fiorella. Implementación de ITIL versión 3 en las organizaciones: Razones del éxito y fracaso, 2021. Revista Científica De Sistemas E Informática, 1(2), 54-66. https://doi.org/10.51252/rcsi.v1i2.191

SALAZAR, Cecilia y DEL CASTILLO, Santiago. Fundamentos Básicos de Estadisticas. 2018. 1ª edición. [En línea]. Fecha de consulta: 17 de marzo de 2022]. Disponible en: http://www.dspace.uce.edu.ec/bitstream/25000/13720/3/Fundamentos%20B%C3%A1sicos%20de%20Estad%C3%ADstica-Libro.pdf

TABOADA CORNETERO, Luis Raúl (2021) Modelo de Seguridad de la Información para contribuir en la mejora de la Seguridad de los Activos de Información Financiera de las Unidades de Gestión Educativa Local de Lambayeque. Perú: Universidad Católica Santo Toribio De Mogrovejo.

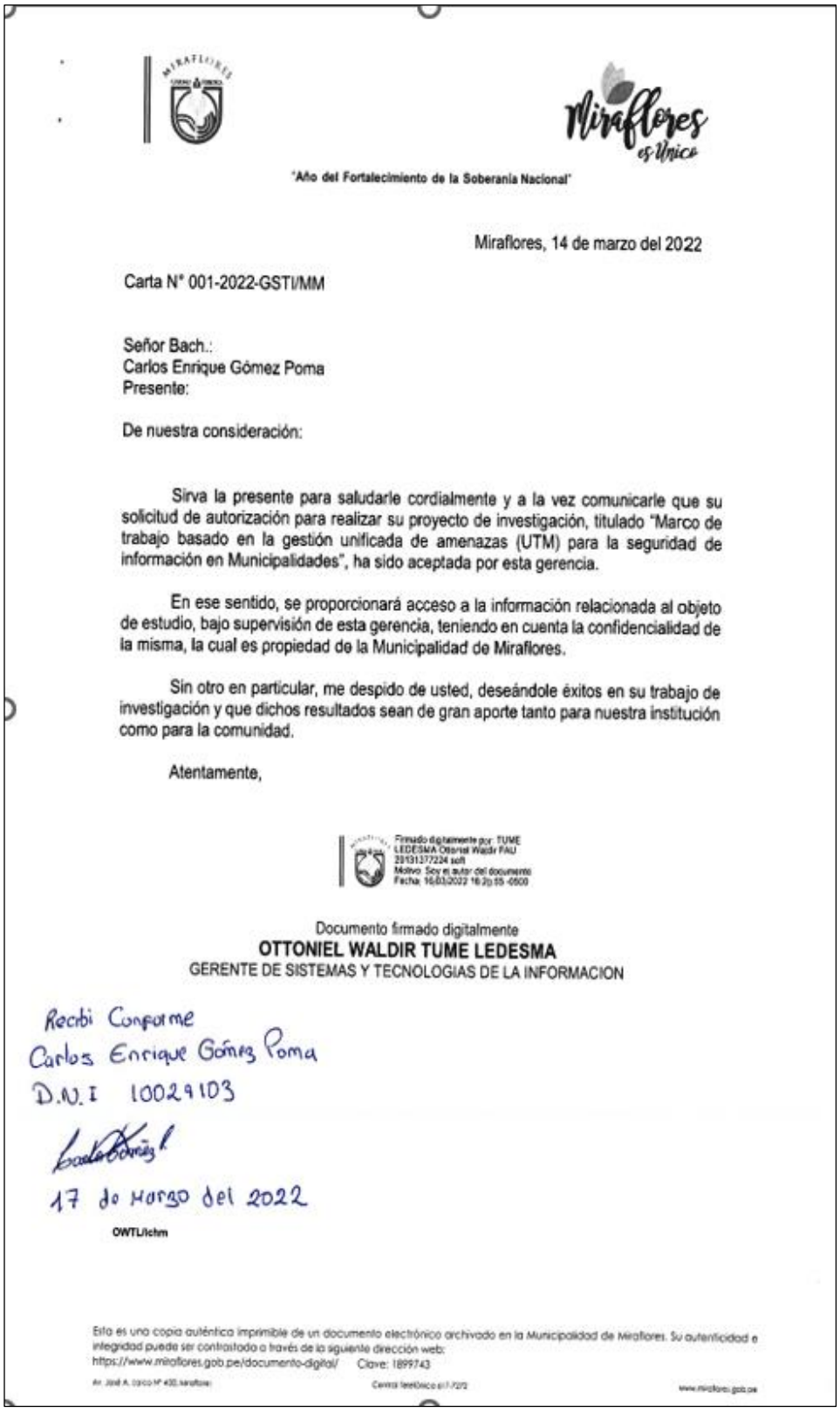
VÁSQUEZ, Agustín. Diseño de un Sistema de Gestión de Seguridad de Información para la empresa Neointel SAC basado en la norma ISO/IEC 27001:2013. (Título de Ingeniero De Sistemas). Lima: Universidad Peruana de Ciencias Aplicadas. 2020, 259 pp.

VILLA TRUJILLO, Rubén Darío (2019). Modelo de ciberseguridad en las Unidades de medición fasorial (PMU) del nuevo sistema inteligente de supervisión y control avanzado de tiempo real (ISAAC) del sistema eléctrico Nacional. (Tesis de Maestría) Colombia: Institución Universitaria.

WALTER Harold. CURIOSO, Alfonso, ESPINOZA, Elizabeth. Framework for the strengthening of Health Information Systems in Peru. Revista Peruana de Medicina Experimental y Salud Publica.[en línea]. 2015, Vol. 32. Fecha de consulta: 17 de enero de 2022]. Disponible en: http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1726-46342015000200019
ISSN 1726-4634

ANEXOS

Anexo 1: Carta de autorización para la realización y difusión de resultados.



"Año del Fortalecimiento de la Soberanía Nacional"

Miraflores, 14 de marzo del 2022

Carta N° 001-2022-GSTI/MM

Señor Bach.:
Carlos Enrique Gómez Poma
Presente:

De nuestra consideración:

Sirva la presente para saludarle cordialmente y a la vez comunicarle que su solicitud de autorización para realizar su proyecto de investigación, titulado "Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en Municipalidades", ha sido aceptada por esta gerencia.

En ese sentido, se proporcionará acceso a la información relacionada al objeto de estudio, bajo supervisión de esta gerencia, teniendo en cuenta la confidencialidad de la misma, la cual es propiedad de la Municipalidad de Miraflores.

Sin otro en particular, me despido de usted, deseándole éxitos en su trabajo de investigación y que dichos resultados sean de gran aporte tanto para nuestra institución como para la comunidad.

Atentamente,

Firmado digitalmente por: TUME LEDESMA Ottoniel Waldir FAU 20131377224 soft
Motivo: Soy el autor del documento
Fecha: 16/03/2022 16:20:55 -0500

Documento firmado digitalmente
OTTONIEL WALDIR TUME LEDESMA
GERENTE DE SISTEMAS Y TECNOLOGIAS DE LA INFORMACION

Recibi Conforme
Carlos Enrique Gómez Poma
D.N.I 10029103
17 de Marzo del 2022

OWTL/lchm

Esta es una copia auténtica imprimible de un documento electrónico archivado en la Municipalidad de Miraflores. Su autenticidad e integridad puede ser contrastado a través de la siguiente dirección web:
https://www.miraflores.gob.pe/documento-digital/ Clave: 1899743

Av. José A. Lores N° 430, Miraflores Central telefónica 617-7272 www.miraflores.gob.pe

"Año del Fortalecimiento de la Soberanía Nacional"

Miraflores, 14 de marzo del 2022

Carta N° 002-2022-GSTI/MM

Señor Bach.:
Esving Bermundo Flores
Presente:

De nuestra consideración:

Sirva la presente para saludarle cordialmente y a la vez comunicarle que su solicitud de autorización para realizar su proyecto de investigación, titulado "Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en Municipalidades", ha sido aceptada por esta gerencia.

En ese sentido, se proporcionará acceso a la información relacionada al objeto de estudio, bajo supervisión de esta gerencia, teniendo en cuenta la confidencialidad de la misma, la cual es propiedad de la Municipalidad de Miraflores.

Sin otro en particular, me despido de usted, deseándole éxitos en su trabajo de investigación y que dichos resultados sean de gran aporte tanto para nuestra institución como para la comunidad.

Atentamente,

Firmado digitalmente por: TUME LEDESMA Ottoniel Waldir FAU 20131377224 soft
Motivo: Soy el autor del documento
Fecha: 16/03/2022 16:21:45 -0500

Documento firmado digitalmente
OTTONIEL WALDIR TUME LEDESMA
GERENTE DE SISTEMAS Y TECNOLOGIAS DE LA INFORMACION

Recibí conforme
Esving Bermudo Flores
DNI: 48247132

OWTL/lchm

17/03/2022

Anexo 2: Carta de Conformidad de Proyecto

"Municipalidad de Miraflores"

"AÑO DEL FORTALECIMIENTO DE LA SOBERANIA NACIONAL"

Lima, 31 de mayo de 2022

Dirigido a:
Ing. M. Janina Cotrina Linares
Coordinadora Nacional del Taller de Titulación de Ingeniería de Sistemas
Universidad César Vallejo – Tarapoto
Presente. –

ASUNTO: CONFORMIDAD DEL PROYECTO

Es grato dirigirme a usted para saludarle cordialmente en nombre de la Gerencia de Sistemas y Tecnologías de la Información de la Municipalidad Distrital de Miraflores; hago de su conocimiento que el señor **Carlos Enrique Gómez Poma** con DNI **N°10029103, y Esving Bermudo Flores** con DNI **N° 48247132**, estudiantes de la experiencia curricular de Desarrollo del Proyecto de Investigación, de la carrera de **INGENIERIA DE SISTEMAS**, desarrollaron el proyecto **"Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en municipalidades"** el cual fue implementado para las pruebas respectivas de su funcionamiento.

En tal sentido, hago de su conocimiento que el Señor **Carlos Enrique Gómez Poma y Esving Bermudo Flores,** han realizado la entrega del proyecto. Por lo que se brinda la **CONFORMIDAD Y ACEPTACIÓN DEL PROYECTO** desarrollado de acuerdo al compromiso definido.

Atentamente

Firmado digitalmente por:
TUME LEDESMA Ottoniel
Waldir FAU 20131377224 soft
Motivo: Soy el autor del documento
Fecha: 31/05/2022 17:50:09-0500

Av. Larco 400 – Lima

Teléfono: 617-7272 Anx: 7550

Anexo 4: Operacionalización de variables

Operacionalización de variables

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de Medición
Dependiente: Seguridad de Información	La seguridad de la información se refiere al conjunto de medidas y procedimientos que se deben aplicar para proteger la integridad, la confidencialidad y disponibilidad de la información a través de recursos técnicos y humanos; para así mantener en normal funcionamiento de los sistemas informáticos, tanto del hardware como de software (Pruna y Yarad, 2020).	Es el conjunto de medidas o políticas que deben tomar las organizaciones sobre su sistema tecnológico para defender y salvaguardar la información buscando mantener la confidencialidad, integridad y la disponibilidad de datos que conforman el activo organizacional	Confidencialidad	• % Intentos de usuarios no autorizados. • % amenazas detectadas.	Escala de razón
			Integridad	• % de incidencias en acceso de aplicaciones • % de equipos de cómputos vulnerables	
			Disponibilidad	• % de disponibilidad de los sistemas • % de incidencias en el data center	

Fuente: Elaboración Propia (2022)

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de Medición
Gestión de Riesgo	Ecured (2017), la define como un enfoque, un sistema, un proceso, una práctica, una nueva forma de gestión, que proporciona a la dirección información respecto a los riesgos que se expone la organización y posibilita las estrategias para asumirlo.	Es un conjunto de actividades que permiten la identificación, análisis, evaluación y tratamientos de los riesgos que pueden afectar la infraestructura tecnológica de una organización.	Identificación de Riesgos	• Identificación de Activos Críticos • Identificación Amenazas de Activos. • Detección de Vulnerabilidades de Activos.	Encuesta de percepción
			Análisis de Riesgos	• Frecuencia de Ocurrencia del riesgo. • Detección de Riesgos a tiempo. • Tiempo Promedio de Resolver la ocurrencia del Riesgos.	
			Evaluación de Riesgos	• Tiempo Promedio de Resolver la ocurrencia del Riesgos.	
			Tratamiento de Riesgos	• Cumplimiento de Políticas de Seguridad. • Implementación de los procesos de auditoría.	

Fuente: Elaboración Propia (2022)

Anexo 5. Matriz de Consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES	MÉTODOS Y TÉCNICAS DE INVESTIGACIÓN
PROBLEMA GENERAL **PG:** ¿En qué medida el Marco de trabajo basado en la gestión unificada de amenazas (UTM) favorece para la seguridad de información en la Municipalidad de Miraflores? **PROBLEMAS ESPECIFICOS** **PE1:** ¿En qué medida el marco de trabajo basado en la gestión unificada de amenazas (UTM) favorece para la confidencialidad de la información en la Municipalidad de Miraflores? **PE2:** ¿En qué medida el marco de trabajo basado en la gestión unificada de amenazas (UTM) favorece para la integridad de la información en la Municipalidad de Miraflores? **PE3**: ¿En qué medida el marco de trabajo basado en la gestión unificada de amenazas (UTM) favorece para la disponibilidad de la información en la Municipalidad de Miraflores?	**OBJETIVO GENERAL** **OG**: Determinar la eficacia del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de la información en la Municipalidad de Miraflores. **OBJETIVOS ESPECIFICOS** **OE1:** Determinar la eficacia del marco de trabajo basado en la gestión unificada de amenazas (UTM) para la confidencialidad de la información en la Municipalidad de Miraflores. **OE2:** Determinar la eficacia del marco de trabajo basado en la gestión unificada de amenazas (UTM) para la integridad de la información en la Municipalidad de Miraflores. **OE3**: Determinar la eficacia del marco de trabajo basado en la gestión unificada de amenazas (UTM) para la disponibilidad de la información en la Municipalidad de Miraflores.	**HIPOTESIS GENERAL** **HG:** El Marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la seguridad de información en la Municipalidad de Miraflores. **HIPOTESIS ESPECIFICAS** **HE1:** El marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la confidencialidad de la información en la Municipalidad de Miraflores. **HE2:** El marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la integridad de la información en la Municipalidad de Miraflores. **HE3**: El marco de trabajo basado en la gestión unificada de amenazas (UTM) es efectivo para la disponibilidad de la información en la Municipalidad de Miraflores.	**VARIABLE INDEPENDIENTE:** **Gestión Unificada de Amenazas (UTM)** (Gestión de Riesgos) D1: **Identificación de Riesgos** Identificación de Activos Críticos Identificación Amenazas de Activos. Detección de Vulnerabilidades de Activos. D2: **Análisis de Riesgos** Frecuencia de Ocurrencia del riesgo. Detección de Riesgos a tiempo. Tiempo Promedio de Resolver la ocurrencia del Riesgos. D3: **Evaluación de Riesgos** Tiempo Promedio de Resolver la ocurrencia del Riesgos. D4: **Tratamiento de Riesgos** Cumplimiento de Políticas de Seguridad. Implementación de los procesos de auditoría**.** **VARIABLE DEPENDIENTE:** Seguridad De Información **D1: Confidencialidad** % Intentos de usuarios no autorizados. % amenazas detectadas. D2: **Integridad** % de incidencias en acceso de aplicaciones % de equipos de cómputos vulnerables D3: **Disponibilidad** % de disponibilidad de los sistemas % de fallas respecto a hardware del data center	**Tipo:** Cuantitativo - Aplicado **Diseño:** experimental de tipo pre-experimental  Donde: G = Grupo O_1= Grupo experimental del pre test, contexto actual X= Aplicación Marco de Trabajo O_2=post-test. Es una prueba a ser aplicada con el mismo grupo, pero con el marco de trabajo implementado. Muestreo Técnicas e Instrumento: Encuesta y Cuestionario

Anexo 6: instrumento de validación

UNIVERSIDAD CÉSAR VALLEJO

CARTA DE PRESENTACIÓN

Mgtr. Daniel Sanchez Jaramillo

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante de la Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo, en la sede Lima Norte, requiero su pronta ayuda para validar los instrumentos con los cuales recojo la información necesaria para poder desarrollar mi investigación.

El título de mi proyecto de investigación es: **Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en Municipalidades** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

Información general	Instrumento de uso del validador	Instrumentos a validar
- Carta de presentación. - Matriz de Operacionalización de las variables. - Matriz de consistencia. - Instrumentos a validar (6 fichas).	- Tabla de validación (1 por cada indicador) - Certificado de validez de contenido de los instrumentos.	Ficha de: 1 % de intentos de usuarios no autorizados 2 % amenazas detectadas 3 % de incidencias en acceso de aplicaciones 4 % de equipos de cómputo vulnerables 5 % de disponibilidad de los sistemas 6 % de incidencias en el data center

Expresándole nuestros sentimientos de respeto y consideración nos despedimos de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

Carlos Enrique Gómez Poma

Esving Bermudo Flores

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	INDICADOR: PORCENTAJE DE INTENTOS DE USUARIOS NO AUTORIZADOS. $\%IUNA = \frac{NINA}{NTI} x\ 100$	x		x		x		
	INDICADOR: PORCENTAJE AMENAZAS DETECTADAS.	Si	No	Si	No	Si	No	
2	$\%AD = \frac{NAD}{NTA} x\ 100$	x		x		x		
3	INDICADOR: PORCENTAJE DE INCIDENCIAS EN ACCESO DE APLICACIONES. $\%IAA = \frac{NIAD}{NTAA} x100$	x		x		x		
4	INDICADOR: PORCENTAJE DE EQUIPOS DE CÓMPUTO VULNERABLES. $\%ECV = \frac{NECV}{NTE} X100$	Si / x	No	Si / x	No	Si / x	No	
5	INDICADOR: PORCENTAJE DE DISPONIBILIDAD DE LOS SISTEMAS. $\%DS = \frac{NSD}{NSR} x100$	Si / x	No	Si / x	No	Si / x	No	
	INDICADOR: PORCENTAJE DE INCIDENCIAS EN EL DATA CENTER							
6	$\%FH = \frac{NFHD}{NP} x100$	x		x		x		

UNIVERSIDAD CÉSAR VALLEJO

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. DANIEL SANCHEZ JARAMILLO **DNI:** 16740150

Especialidad del validador:

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

29 de abril del 2022

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

FIRMA DIGITAL

Firmado digitalmente por: SANCHEZ JARAMILLO Daniel Ricardo FAU 20131377224 soft
Motivo: Doy V° B°
Fecha: 30/04/2022 03:45:55-0500

Mgtr. Daniel Sanchez Jaramillo

UNIVERSIDAD CÉSAR VALLEJO

CARTA DE PRESENTACIÓN

Mgtr. Jose Bustamante Romero

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante de la Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo, en la sede Lima Norte, requiero su pronta ayuda para validar los instrumentos con los cuales recojo la información necesaria para poder desarrollar mi investigación.

El título de mi proyecto de investigación es: **Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en Municipalidades** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

Información general	Instrumento de uso del validador	Instrumentos a validar
- Carta de presentación. - Matriz de Operacionalización de las variables. - Matriz de consistencia. - Instrumentos a validar (6 fichas).	- Tabla de validación (1 por cada indicador) - Certificado de validez de contenido de los instrumentos.	Ficha de: 1 % de intentos de usuarios no autorizados 2 % amenazas detectadas 3 % de incidencias en acceso de aplicaciones 4 % de equipos de cómputo vulnerables 5 % de disponibilidad de los sistemas 6 % de incidencias en el data center

Expresándole nuestros sentimientos de respeto y consideración nos despedimos de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

Carlos Enrique Gómez Poma

D.N.I.: 10029103

Esving Bermudo Flores

D.N.I.: 48247132

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	INDICADOR: PORCENTAJE DE INTENTOS DE USUARIOS NO AUTORIZADOS.	Si	No	Si	No	Si	No	
1	$\%IUNA = \frac{NINA}{NTI} x\ 100$	x		x		x		-
	INDICADOR: PORCENTAJE AMENAZAS DETECTADAS.	Si	No	Si	No	Si	No	
2	$\%AD = \frac{NAD}{NTA} x\ 100$	x		x		x		-
	INDICADOR: PORCENTAJE DE INCIDENCIAS EN ACCESO DE APLICACIONES.	Si	No	Si	No	Si	No	
3	$\%IAA = \frac{NIAD}{NTAA} x100$	x		x		x		-
	INDICADOR: PORCENTAJE DE EQUIPOS DE COMPUTO VULNERABLES.	Si	No	Si	No	Si	No	
4	$\%ECV = \frac{NECV}{NTE} X100$	x		x		x		-
	INDICADOR: PORCENTAJE DE DISPONIBILIDAD DE LOS SISTEMAS.	Si	No	Si	No	Si	No	
5	$\%DS = \frac{NSD}{NSR} x100$	x		x		x		-
	INDICADOR: PORCENTAJE DE INCIDENCIAS EN EL DATA CENTER	Si	No	Si	No	Si	No	
6	$\%FH = \frac{NFHD}{NP} x100$	x		x		x		-

UNIVERSIDAD CÉSAR VALLEJO

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

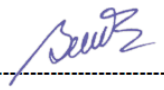
Apellidos y nombres del juez validador. Jose Bustamante Romero **DNI:** 40597166

Especialidad del validador:

Pertinencia: El ítem corresponde al concepto teórico formulado.
Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

29 de abril del 2022



Mgtr. Jose Bustamante Romero

UNIVERSIDAD CÉSAR VALLEJO

CARTA DE PRESENTACIÓN

Mgtr. Nemias Saboya Rios

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante de la Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo, en la sede Lima Norte, requiero su pronta ayuda para validar los instrumentos con los cuales recojo la información necesaria para poder desarrollar mi investigación.

El título de mi proyecto de investigación es: **Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en Municipalidades** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

Información general	Instrumento de uso del validador	Instrumentos a validar
- Carta de presentación. - Matriz de Operacionalización de las variables. - Matriz de consistencia. - Instrumentos a validar (6 fichas).	- Tabla de validación (1 por cada indicador) - Certificado de validez de contenido de los instrumentos.	Ficha de: 1 % de intentos de usuarios no autorizados 2 % amenazas detectadas 3 % de incidencias en acceso de aplicaciones 4 % de equipos de cómputo vulnerables 5 % de disponibilidad de los sistemas 6 % de incidencias en el data center

Expresándole nuestros sentimientos de respeto y consideración nos despedimos de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

Carlos Enrique Gómez Poma
D.N.I.: 10029103

Esving Bermudo Flores
D.N.I.: 48247132

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	INDICADOR: PORCENTAJE DE INTENTOS DE USUARIOS NO AUTORIZADOS.	Si	No	Si	No	Si	No	
1	$\%IUNA = \frac{NINA}{NTI} x\ 100$	x		x		x		
	INDICADOR: PORCENTAJE AMENAZAS DETECTADAS.	Si	No	Si	No	Si	No	
2	$\%AD = \frac{NAD}{NTA} x\ 100$	x		x		x		
	INDICADOR: PORCENTAJE DE INCIDENCIAS EN ACCESO DE APLICACIONES.							
3	$\%IAA = \frac{NIAD}{NTAA} x100$	x		x		x		
	INDICADOR: PORCENTAJE DE EQUIPOS DE COMPUTO VULNERABLES.	Si	No	Si	No	Si	No	
4	$\%ECV = \frac{NECV}{NTE} X100$	x		x		x		
5	INDICADOR: PORCENTAJE DE DISPONIBILIDAD DE LOS SISTEMAS.	Si	No	Si	No	Si	No	
	$\%DS = \frac{NSD}{NSR} x100$	x		x		x		
6	INDICADOR: PORCENTAJE DE INCIDENCIAS EN EL DATA CENTER							
	$\%FH = \frac{NFHD}{NP} x100$	x		x		x		

UNIVERSIDAD CÉSAR VALLEJO

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. SABOYA RIOS NEMIAS **DNI:** 42001721

Especialidad del validador:

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

24 de junio del 2021

Mgtr. Nemias Saboya Rios

Anexo 7. Ficha de registro del indicador: porcentaje Intentos de usuarios no autorizados - pre-test

FACULTAD DE INGENIERIA Y ARQUITECTURA

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Fichaje para el procesamiento de datos

FICHA DE REGISTRO DEL INDICADOR: porcentaje Intentos de usuarios no autorizados

IDENTIFICADOR	ISI01		
DEFINICIÓN			
Definición: porcentaje de acceso del personal no autorizados			
DIMENSIÓN			
Confidencialidad			
Técnica	Fichaje	Unidad de medida	Porcentaje
DESCRIPCION DE VARIABLES	FORMULAS		FUENTES DE INFORMACIÓN
%IUNA = Porcentaje de intentos de usuarios no autorizados NINA = Número de intentos no autorizados NTI = Número totales de intentos	%IUNA= ((NINA) / NTI)*100		Actividades diarias

Medición

N°	Fecha	Número de intentos no autorizados	Número totales de intentos	Observación	porcentaje de intentos de usuarios no autorizados
1	1/03/2022	15	2	13	0.13
2	2/03/2022	20	2	18	0.10
3	3/03/2022	17	2	15	0.12
4	4/03/2022	10	1	9	0.10
5	7/03/2022	8	0	8	0.00
6	8/03/2022	14	13	1	0.93
7	9/03/2022	21	1	20	0.05
8	10/03/2022	17	2	15	0.12
9	11/03/2022	25	5	20	0.20
10	14/03/2022	23	1	22	0.04
11	15/03/2022	12	2	10	0.17
12	16/03/2022	15	2	13	0.13
13	17/03/2022	18	2	16	0.11
14	18/03/2022	19	1	18	0.05
15	21/03/2022	29	4	25	0.14
16	22/03/2022	16	3	13	0.19
17	23/03/2022	27	2	25	0.07
18	24/03/2022	22	3	19	0.14
19	25/03/2022	25	3	22	0.12

20	28/03/2022	19	4	15	0.21
21	29/03/2022	26	20	0	0.23
Promedio					15.95%

Anexo 8. Ficha de registro del indicador: porcentaje Intentos de usuarios no autorizados - post-test

UCV UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERIA Y ARQUITECTURA

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Fichaje para el procesamiento de datos

FICHA DE REGISTRO DEL INDICADOR: porcentaje Intentos de usuarios no autorizados

IDENTIFICADOR	ISI01		
DEFINICIÓN			
Definición: porcentaje de acceso del personal no autorizados			
DIMENSIÓN			
Confidencialidad			
Técnica	Fichaje	Unidad de medida	Porcentaje
DESCRIPCION DE VARIABLES	FORMULAS		FUENTES DE INFORMACIÓN
%IUNA = Porcentaje de intentos de usuarios no autorizados NINA = Número de intentos no autorizados NTI = Número totales de intentos	%IUNA= ((NINA) / NTI)*100		Actividades diarias

Medición					
N°	Fecha	Número de intentos no autorizados	Número totales de intentos	Observación	porcentaje de intentos de usuarios no autorizados
1	1/04/2022	7	7	0	1.00
2	4/04/2022	6	5	1	0.83
3	5/04/2022	2	2	0	1.00
4	6/04/2022	2	2	0	1.00
5	7/04/2022	1	1	0	1.00
6	8/04/2022	1	1	0	1.00
7	11/04/2022	1	1	0	1.00
8	12/04/2022	6	6	0	1.00
9	13/04/2022	5	4	1	0.80
10	14/04/2022	2	2	0	1.00
11	15/04/2022	3	3	0	1.00
12	18/04/2022	3	3	0	1.00
13	19/04/2022	3	3	0	1.00

14	20/04/2022	1	1	0	1.00
15	21/04/2022	1	1	0	1.00
16	22/04/2022	1	1	0	1.00
17	25/04/2022	3	2	1	0.67
18	26/04/2022	2	2	0	1.00
19	27/04/2022	1	1	0	1.00
20	28/04/2022	2	2	0	1.00
21	29/04/2022	2	2	0	1.00
Promedio					96.67%

Anexo 9. Ficha de registro del indicador: porcentaje amenazas detectadas -pre-test

UCV
UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERIA Y ARQUITECTURA

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Fichaje para el procesamiento de datos

FICHA DE REGISTRO DEL INDICADOR: porcentaje de amenazas detectadas

IDENTIFICADOR	ISI02		
DEFINICIÓN			
Definición: porcentaje de amenazas detectadas			
DIMENSIÓN			
Confidencialidad			
Técnica	Fichaje	Unidad de medida	Porcentaje
DESCRIPCION DE VARIABLES	FORMULAS		FUENTES DE INFORMACIÓN
%AD = Porcentaje de Amenazas Detectadas NAD = Número de amenazas detectadas NTA = Número totales de amenazas	%AD= ((NAD) / NTA)*100		Actividades diarias

Medición					
N°	1/03/2022	Número de amenazas detectadas	Número totales de amenazas	Observación	Porcentaje de amenazas detectadas
1	1/03/2022	3	50	47	0.06
2	2/03/2022	5	45	40	0.11
3	3/03/2022	3	30	27	0.10
4	4/03/2022	6	47	41	0.13
5	7/03/2022	7	38	31	0.18
6	8/03/2022	9	37	28	0.24

7	9/03/2022	2	15	13	0.13
8	10/03/2022	5	47	42	0.11
9	11/03/2022	6	37	31	0.16
10	14/03/2022	11	47	36	0.23
11	15/03/2022	5	23	18	0.22
12	16/03/2022	4	30	26	0.13
13	17/03/2022	3	21	18	0.14
14	18/03/2022	8	28	20	0.29
15	21/03/2022	7	27	20	0.26
16	22/03/2022	5	35	30	0.14
17	23/03/2022	7	47	40	0.15
18	24/03/2022	9	37	28	0.24
19	25/03/2022	8	28	20	0.29
20	28/03/2022	4	14	10	0.29
21	29/03/2022	5	21	16	0.24
Promedio					18.31%

Anexo 10. Ficha de registro del indicador: porcentaje amenazas detectadas post-test

UCV UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERIA Y ARQUITECTURA

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Fichaje para el procesamiento de datos

FICHA DE REGISTRO DEL INDICADOR: porcentaje amenazas detectadas

IDENTIFICADOR	ISI02		
DEFINICIÓN			
Definición: porcentaje de amenazas detectadas			
DIMENSIÓN			
Confidencialidad			
Técnica	Fichaje	Unidad de medida	Porcentaje
DESCRIPCION DE VARIABLES	FORMULAS		FUENTES DE INFORMACIÓN
%AD = Porcentaje de Amenazas Detectadas NAD = Número de amenazas detectadas NTA = Número totales de amenazas	%AD= ((NAD) / NTA)*100		Actividades diarias
Medición			

N°	1/03/2022	Número de amenazas detectadas	Número totales de amenazas	Observación	% de amenazas detectadas
1	1/04/2022	49	50	1	0.98
2	4/04/2022	42	45	3	0.93
3	5/04/2022	30	30	0	1.00
4	6/04/2022	46	47	1	0.98
5	7/04/2022	38	38	0	1.00
6	8/04/2022	37	37	0	1.00
7	11/04/2022	15	15	0	1.00
8	12/04/2022	47	47	0	1.00
9	13/04/2022	37	37	0	1.00
10	14/04/2022	45	47	2	0.96
11	15/04/2022	23	23	0	1.00
12	18/04/2022	30	30	0	1.00
13	19/04/2022	21	21	0	1.00
14	20/04/2022	28	28	1	1.00
15	21/04/2022	25	27	0	0.93
16	22/04/2022	35	35	0	1.00
17	25/04/2022	47	47		1.00
18	26/04/2022	37	37		1.00
19	27/04/2022	27	28		0.96
20	28/04/2022	14	14		1.00
21	29/04/2022	21	21		1.00
Promedio					98.76%

Anexo 11. Ficha de registro del indicador: porcentaje de incidencias en acceso aplicaciones - pre-test

FACULTAD DE INGENIERIA Y ARQUITECTURA

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Fichaje para el procesamiento de datos

FICHA DE REGISTRO DEL INDICADOR: porcentaje de incidencias en acceso de aplicaciones

IDENTIFICADOR	ISI03		
DEFINICIÓN			
Definición: porcentaje de incidencias en acceso de aplicaciones			
DIMENSIÓN			
Integridad			
Técnica	Fichaje	Unidad de medida	Porcentaje
DESCRIPCION DE VARIABLES	FORMULAS		FUENTES DE INFORMACIÓN
% IAA = Porcentaje de incidencias de acceso aplicaciones NIAD = Número de incidencias detectadas NTAA = Número total de acceso aplicaciones	%IAA= ((NIAD) / NTAA)*100 Donde		Actividades diarias

Medición

N°	Fecha	Número de incidencias detectadas	Número total de acceso aplicaciones	Porcentaje de incidencias en acceso aplicaciones
1	1/03/2022	400	8	0.02
2	2/03/2022	400	7	0.02
3	3/03/2022	400	4	0.01
4	4/03/2022	400	6	0.02
5	7/03/2022	400	2	0.01
6	8/03/2022	400	4	0.01
7	9/03/2022	400	4	0.01
8	10/03/2022	400	3	0.01
9	11/03/2022	400	10	0.03
10	14/03/2022	400	8	0.02
11	15/03/2022	400	4	0.01
12	16/03/2022	400	20	0.05
13	17/03/2022	400	1	0.00
14	18/03/2022	400	8	0.02

15	21/03/2022	400	9	0.02
16	22/03/2022	400	2	0.01
17	23/03/2022	400	10	0.03
18	24/03/2022	400	6	0.02
19	25/03/2022	400	25	0.06
20	28/03/2022	400	20	0.05
21	29/03/2022	400	7	0.02
Promedio				2.00%

Anexo 12. Ficha de registro del indicador: porcentaje de incidencias en acceso de aplicaciones – post-test

UCV
UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Fichaje para el procesamiento de datos

FICHA DE REGISTRO DEL INDICADOR: porcentaje de incidencias en acceso de aplicaciones

IDENTIFICADOR	ISI03		
DEFINICIÓN			
Definición: porcentaje de incidencias en acceso aplicaciones			
DIMENSIÓN			
Integridad			
Técnica	Fichaje	Unidad de medida	Porcentaje
DESCRIPCION DE VARIABLES	FORMULAS		FUENTES DE INFORMACIÓN
% IAA = Porcentaje de incidencias de acceso aplicaciones NIAD = Número de incidencias detectadas NTAA = Número total de acceso aplicaciones	%IAA= ((NIAD) / NTAA)*100 Donde		Actividades diarias

Medición

N°	Fecha	Número de incidencias detectadas	Número total de acceso aplicaciones	Porcentaje de incidencias en acceso aplicaciones
1	1/04/2022	400	1	0.00
2	4/04/2022	400	0	0.00
3	5/04/2022	400	2	0.01
4	6/04/2022	400	1	0.00
5	7/04/2022	400	1	0.00

6	8/04/2022	400	0	0.00
7	11/04/2022	400	1	0.00
8	12/04/2022	400	1	0.00
9	13/04/2022	400	0	0.00
10	14/04/2022	400	0	0.00
11	15/04/2022	400	1	0.00
12	18/04/2022	400	1	0.00
13	19/04/2022	400	2	0.01
14	20/04/2022	400	2	0.01
15	21/04/2022	400	2	0.01
16	22/04/2022	400	1	0.00
17	25/04/2022	400	1	0.00
18	26/04/2022	400	1	0.00
19	27/04/2022	400	1	0.00
20	28/04/2022	400	1	0.00
21	29/04/2022	400	1	0.00
Promedio				0.25%

Anexo 13. Ficha de registro del indicador: porcentaje de equipos de cómputos vulnerables – pre-test

UCV
UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERIA Y ARQUITECTURA

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Fichaje para el procesamiento de datos

FICHA DE REGISTRO DEL INDICADOR: porcentaje de equipos de cómputos vulnerables

IDENTIFICADOR	ISI04		
DEFINICIÓN			
Definición: porcentaje de equipos de cómputos vulnerables			
DIMENSIÓN			
Integridad			
Técnica	Fichaje	Unidad de medida	Porcentaje
DESCRIPCION DE VARIABLES	FORMULAS		FUENTES DE INFORMACIÓN
% ECV = Porcentaje de equipos de cómputos vulnerables NECV = Número de equipos de cómputos vulnerables NTE = Número total de equipos	%ECV= ((NECV) / NTE)*100		Actividades diarias

Medición				
N°	Fecha	Número de equipos de cómputos vulnerables	Número total de equipos	Porcentaje de equipos de cómputo vulnerables
1	1/03/2022	50	758	0,066
2	2/03/2022	30	758	0,040
3	3/03/2022	60	758	0,079
4	4/03/2022	30	758	0,040
5	7/03/2022	27	758	0,036
6	8/03/2022	25	758	0,033
7	9/03/2022	20	758	0,026
8	10/03/2022	30	758	0,040
9	11/03/2022	20	758	0,026
10	14/03/2022	30	758	0,040
11	15/03/2022	20	758	0,026
12	16/03/2022	25	758	0,033
13	17/03/2022	33	758	0,044
14	18/03/2022	25	758	0,033
15	21/03/2022	35	758	0,046

16	22/03/2022	15	758	0,020
17	23/03/2022	50	758	0,066
18	24/03/2022	19	758	0,025
19	25/03/2022	33	758	0,044
20	28/03/2022	44	758	0,058
21	29/03/2022	33	758	0,044
Promedio				86.28%

Anexo 14. Ficha de registro del indicador: porcentaje de equipos de cómputos vulnerables – post-test

UCV
UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERIA Y ARQUITECTURA

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Fichaje para el procesamiento de datos

FICHA DE REGISTRO DEL INDICADOR: porcentaje de equipos de cómputos vulnerables

IDENTIFICADOR	ISI04		
DEFINICIÓN			
Definición: porcentaje de equipos de cómputos vulnerables			
DIMENSIÓN			
Integridad			
Técnica	Fichaje	Unidad de medida	Porcentaje
DESCRIPCION DE VARIABLES	FORMULAS		FUENTES DE INFORMACIÓN
% ECV = Porcentaje de equipos de cómputos vulnerables NECV = Número de equipos de cómputos vulnerables NTE = Número total de equipos	%ECV= ((NECV) / NTE)*100		Actividades diarias

Medición				
N°	Fecha	Número de equipos de cómputos vulnerables	Número total de equipos	Porcentaje de equipos de cómputo vulnerables
1	01/04/2022	7	758	0,009
2	04/04/2022	9	758	0,012
3	05/04/2022	7	758	0,009
4	06/04/2022	9	758	0,012
5	07/04/2022	8	758	0,011

6	08/04/2022	5	758	0,007
7	11/04/2022	9	758	0,012
8	12/04/2022	9	758	0,012
9	13/04/2022	8	758	0,011
10	14/04/2022	8	758	0,011
11	15/04/2022	5	758	0,007
12	18/04/2022	9	758	0,012
13	19/04/2022	9	758	0,012
14	20/04/2022	9	758	0,012
15	21/04/2022	5	758	0,007
16	22/04/2022	8	758	0,011
17	25/04/2022	8	758	0,011
18	26/04/2022	9	758	0,012
19	27/04/2022	5	758	0,007
20	28/04/2022	9	758	0,012
21	29/04/2022	7	758	0,009
Promedio				1.02%

Anexo 15. Ficha de registro del indicador: porcentaje de disponibilidad de los sistemas pre-test

UCV
UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERIA Y ARQUITECTURA

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Fichaje para el procesamiento de datos

FICHA DE REGISTRO DEL INDICADOR: porcentaje de disponibilidad de los sistemas

IDENTIFICADOR	ISI02		
DEFINICIÓN			
Definición: porcentaje de disponibilidad de los sistemas que se requieren			
DIMENSIÓN			
Disponibilidad			
Técnica	Fichaje	Unidad de medida	Porcentaje
DESCRIPCION DE VARIABLES	FORMULAS		FUENTES DE INFORMACIÓN
% DS = Porcentaje de disponibilidad de sistemas NSD = Número de sistemas disponibles	%DS= ((NSD) / NSR)*100		Actividades diarias

NSR = Número de sistemas requeridos		

Medición				
N°	Fecha	Número de sistemas disponibles	Número de sistemas requeridos	Porcentaje de disponibilidad de los sistemas
1	01/03/2020	130	133	0,98
2	02/03/2020	131	133	0,98
3	03/03/2020	130	133	0,98
4	04/03/2020	0	133	0,00
5	07/03/2022	132	133	0,99
6	08/03/2022	131	133	0,98
7	09/03/2022	131	133	0,98
8	10/03/2022	120	133	0,90
9	11/03/2022	120	133	0,90
10	14/03/2022	133	133	1,00
11	15/03/2022	133	133	1,00
12	16/03/2022	132	133	0,99
13	17/03/2022	132	133	0,99
14	18/03/2022	133	133	1,00
15	21/03/2022	133	133	1,00
16	22/03/2022	132	133	0,99
17	23/03/2022	133	133	1,00
18	24/03/2022	0	133	0,00
19	25/03/2022	130	133	0,98
20	28/03/2022	130	133	0,98
21	29/03/2022	132	133	0,99
Promedio				88.72%

Anexo 16. Ficha de registro del indicador: porcentaje de disponibilidad de los sistemas post-test

FACULTAD DE INGENIERIA Y ARQUITECTURA

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Fichaje para el procesamiento de datos

FICHA DE REGISTRO DEL INDICADOR: porcentaje de disponibilidad de los sistemas

IDENTIFICADOR	ISI02		
DEFINICIÓN			
Definición: porcentaje de disponibilidad de los sistemas que se requieren			
DIMENSIÓN			
Disponibilidad			
Técnica	Fichaje	Unidad de medida	Porcentaje
DESCRIPCION DE VARIABLES	FORMULAS		FUENTES DE INFORMACIÓN
% DS = Porcentaje de disponibilidad de sistemas NSD = Número de sistemas disponibles NSR = Número de sistemas requeridos	%DS= ((NSD) / NSR)*100		Actividades diarias

Medición				
N°	Fecha	Número de sistemas disponibles	Número de sistemas requeridos	Porcentaje de disponibilidad de los sistemas
1	01/04/2022	133	133	1,00
2	04/04/2022	133	133	1,00
3	05/04/2022	131	133	0,98
4	06/04/2022	133	133	1,00
5	07/04/2022	132	133	0,99
6	08/04/2022	133	133	1,00
7	11/04/2022	133	133	1,00
8	12/04/2022	133	133	1,00
9	13/04/2022	133	133	1,00
10	14/04/2022	133	133	1,00
11	15/04/2022	133	133	1,00
12	18/04/2022	131	133	0,98
13	19/04/2022	133	133	1,00

14	20/04/2022	132	133	0,99
15	21/04/2022	133	133	1,00
16	22/04/2022	133	133	1,00
17	25/04/2022	133	133	1,00
18	26/04/2022	132	133	0,99
19	27/04/2022	133	133	1,00
20	28/04/2022	133	133	1,00
21	29/04/2022	133	133	1,00
Promedio				99.75%

Anexo 17. Ficha de registro del indicador: porcentaje de incidencias en el data center pre-test

UCV UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERIA Y ARQUITECTURA

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Fichaje para el procesamiento de datos

FICHA DE REGISTRO DEL INDICADOR: porcentaje de incidencias en el data center

IDENTIFICADOR	ISI06			
DEFINICIÓN				
Definición: porcentaje de incidencias en el data center				
DIMENSIÓN				
Disponibilidad				
Técnica	Fichaje		Unidad de medida	Porcentaje
DESCRIPCION DE VARIABLES		FORMULAS		FUENTES DE INFORMACIÓN
% IDC = Porcentaje de incidencias en el data center NFD = Número fallas detectadas NP = Número de peticiones		%IDC= ((NFD) / NP)*100		Actividades diarias

Medición				
N°	Fecha	Número fallas detectadas	Número de peticiones	Porcentaje de incidencias En el data center
1	01/03/2022	2	7	0,29
2	02/03/2022	1	4	0,25
3	03/03/2022	1	5	0,20
4	04/03/2022	2	7	0,29

5	07/03/2022	1	6	0,17
6	08/03/2022	2	9	0,22
7	09/03/2022	1	8	0,13
8	10/03/2022	1	6	0,17
9	11/03/2022	2	8	0,25
10	14/03/2022	2	6	0,33
11	15/03/2022	3	8	0,38
12	16/03/2022	4	4	1,00
13	17/03/2022	4	9	0,44
14	18/03/2022	3	8	0,38
15	21/03/2022	2	7	0,29
16	22/03/2022	1	6	0,17
17	23/03/2022	2	9	0,22
18	24/03/2022	2	8	0,25
19	25/03/2022	1	8	0,13
20	28/03/2022	1	9	0,11
21	29/03/2022	2	8	0,25
Promedio				28.05%

Anexo 18. Ficha de registro del indicador: porcentaje de incidencias en el data center post-test

UCV
UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERIA Y ARQUITECTURA

Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en la Municipalidad de Miraflores.

Fichaje para el procesamiento de datos

FICHA DE REGISTRO DEL INDICADOR: porcentaje de incidencias en el data center

IDENTIFICADOR	ISI06		
DEFINICIÓN			
Definición: porcentaje de incidencias en el data center			
DIMENSIÓN			
Disponibilidad			
Técnica	Fichaje	Unidad de medida	Porcentaje
DESCRIPCION DE VARIABLES	FORMULAS		FUENTES DE INFORMACIÓN
% IDC = Porcentaje de incidencias en el data center	%IDC= ((NFD) / NP)*100		Actividades diarias

NFD = Número fallas detectadas NP = Número de peticiones		

Medición				
N°	Fecha	Número fallas detectadas	Número de peticiones	Porcentaje de incidencias En el data center
1	01/04/2022	1	7	0,14
2	04/04/2022	0	4	0,00
3	05/04/2022	0	5	0,00
4	06/04/2022	0	7	0,00
5	07/04/2022	0	2	0,00
6	08/04/2022	0	9	0,00
7	11/04/2022	0	8	0,00
8	12/04/2022	0	6	0,00
9	13/04/2022	0	8	0,00
10	14/04/2022	1	6	0,17
11	15/04/2022	0	8	0,00
12	18/04/2022	0	4	0,00
13	19/04/2022	0	3	0,00
14	20/04/2022	0	8	0,00
15	21/04/2022	0	7	0,00
16	22/04/2022	0	6	0,00
17	25/04/2022	0	9	0,00
18	26/04/2022	0	8	0,00
19	27/04/2022	0	8	0,00
20	28/04/2022	0	9	0,00
21	29/04/2022	1	3	0,33
Promedio				3.06%

Anexo 19. Cuestionario de percepción del usuario - UTM

Universidad César Vallejo

Encuesta de percepción sobre el "Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de información en municipalidades"

INVESTIGADORES: **Carlos Enrique Gómez Poma / Esving Bermudo Flores**

Nombre del entrevistado: **Javier Leónidas Vilchez López**

Fecha: 31/05/2022

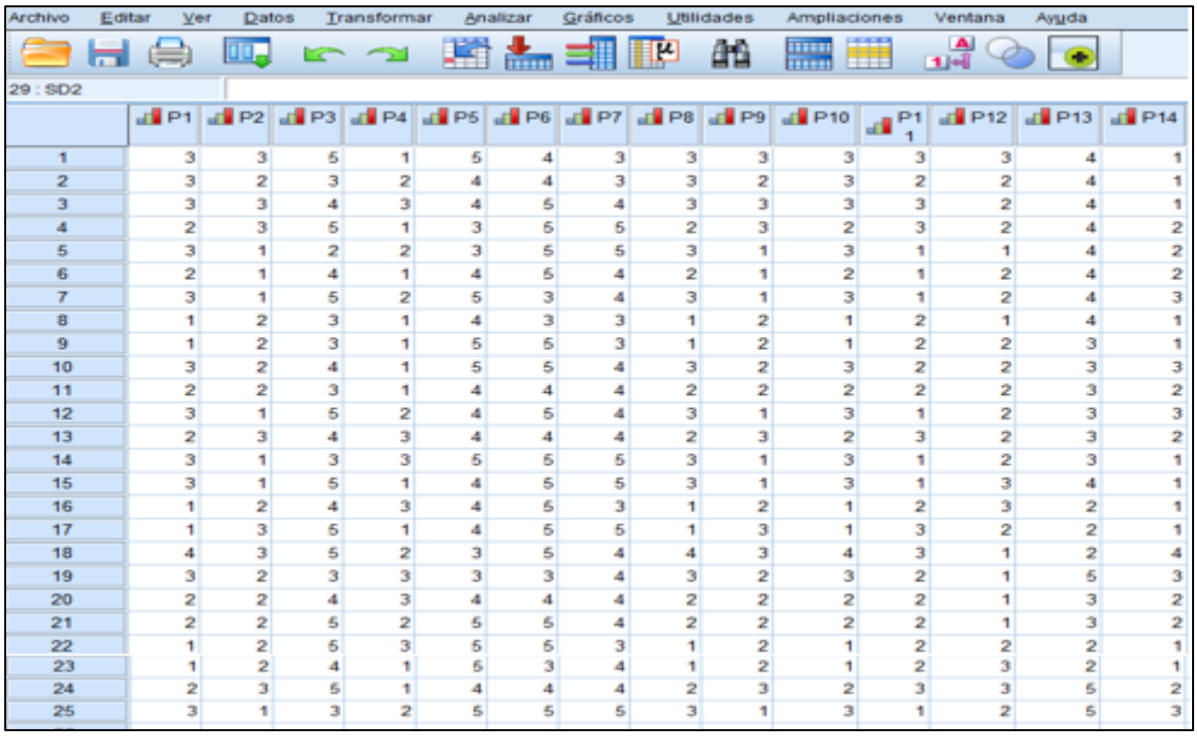
Instrucciones: Estimado usuario es importante conocer su opinión, marque con un aspa la respuesta según su criterio teniendo en cuenta los puntajes correspondientes de acuerdo al siguiente ejemplo

Totalmente en desacuerdo (1), En desacuerdo (2), Indiferente (3), De acuerdo (4), Totalmente de acuerdo (5)

N°	Items	Totalmente en desacuerdo	En desacuerdo	Indiferente	De acuerdo	Totalmente de acuerdo
		1	2	3	4	5
	IDENTIFICACIÓN DE RIESGOS					
1	¿El marco de trabajo maneja la identificación de todos los activos con que cuenta la organización?				X	
2	¿En el marco de trabajo se determina las amenazas a que se expone cada uno de los activos?				X	
3	¿El marco de trabajo detecta las vulnerabilidades de cada equipo?				X	
	ANÁLISIS DE RIESGOS					
4	¿El marco de trabajo contempla mejora continua sobre la Frecuencia de Ocurrencia del riesgo?					X
5	¿El marco de trabajo contempla una manual de tratamiento de los riesgos que pueden afectar la infraestructura tecnológica de la organización?					X
6	¿El marco de trabajo permite una evaluación exhaustiva de los riesgos a fin de que puedan ser mitigados a tiempo tomando en cuenta los factores que pueden generarlo?					X
	EVALUACIÓN DE RIESGOS					
7	¿El marco de trabajo contempla el tiempo promedio que cada riesgo debe ser mitigado?				X	
8	¿El marco de trabajo permite la revisión y evaluación periódica de los riesgos?			X		
9	¿El marco de trabajo permite la mitigación de riesgos temprana?				X	
10	¿El marco de trabajo permite la mitigación de riesgos antes de que ocurra?			X		
	TRATAMIENTOS DE RIESGOS					
11	¿El marco de trabajo permite el monitoreo de las acciones planificadas?				X	
12	¿El marco de trabajo permite llevar un control de los incidentes detectados y hacer mejoras continuas?				X	
13	¿Se cumplen las políticas de seguridad que se definen en el marco de trabajo?			X		
14	¿El marco de trabajo permite aplicar auditoria periódicas de los procesos?			X		

Firmado digitalmente por:
VILCHEZ LOPEZ Javier
Leonidas FAU 20131377224 soft
Motivo: Doy fe
Fecha: 01/06/2022 17:04:04-0500

Anexo 20. Procesamiento de datos Pre-test

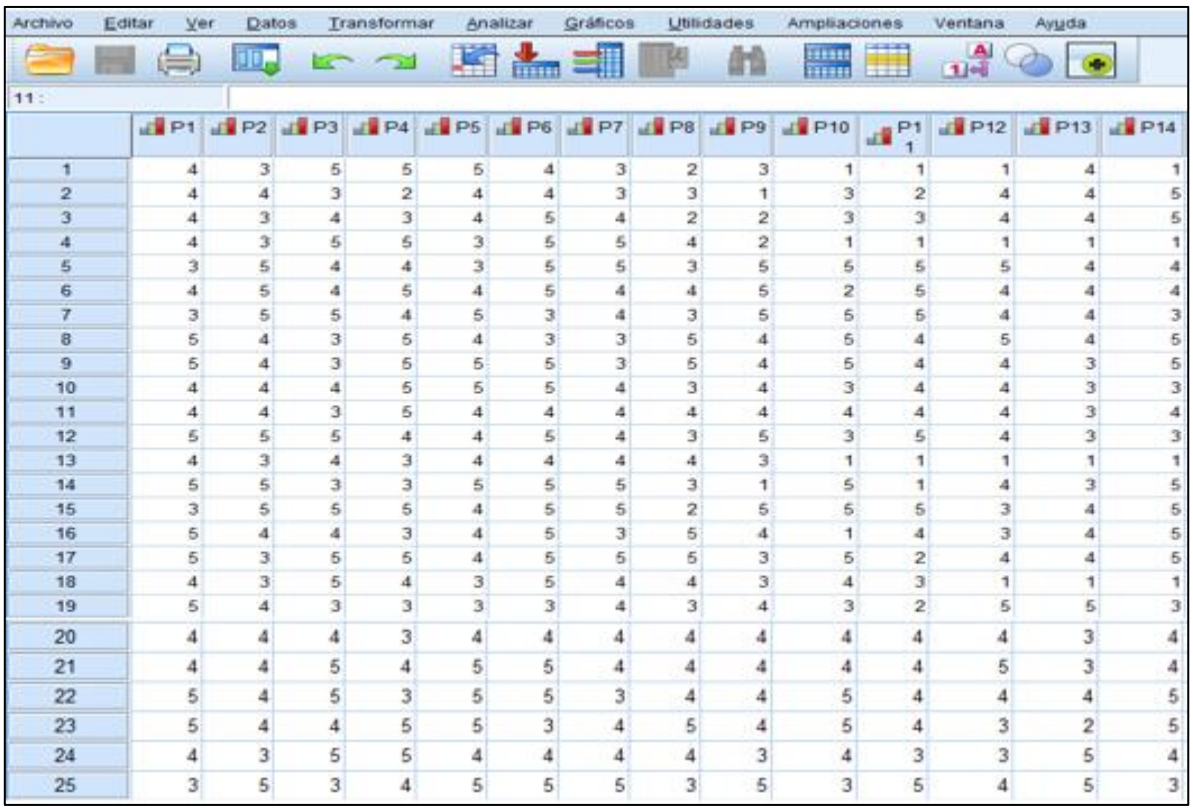


Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

29 : SD2

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
1	3	3	5	1	5	4	3	3	3	3	3	3	4	1
2	3	2	3	2	4	4	3	3	2	3	2	2	4	1
3	3	3	4	3	4	5	4	3	3	3	3	2	4	1
4	2	3	5	1	3	5	5	2	3	2	3	2	4	2
5	3	1	2	2	3	5	5	3	1	3	1	1	4	2
6	2	1	4	1	4	5	4	2	1	2	1	2	4	2
7	3	1	5	2	5	3	4	3	1	3	1	2	4	3
8	1	2	3	1	4	3	3	1	2	1	2	1	4	1
9	1	2	3	1	5	5	3	1	2	1	2	2	3	1
10	3	2	4	1	5	5	4	3	2	3	2	2	3	3
11	2	2	3	1	4	4	4	2	2	2	2	2	3	2
12	3	1	5	2	4	5	4	3	1	3	1	2	3	3
13	2	3	4	3	4	4	4	2	3	2	3	2	3	2
14	3	1	3	3	5	5	5	3	1	3	1	2	3	1
15	3	1	5	1	4	5	5	3	1	3	1	3	4	1
16	1	2	4	3	4	5	3	1	2	1	2	3	2	1
17	1	3	5	1	4	5	5	1	3	1	3	2	2	1
18	4	3	5	2	3	5	4	4	3	4	3	1	2	4
19	3	2	3	3	3	3	4	3	2	3	2	1	5	3
20	2	2	4	3	4	4	4	2	2	2	2	1	3	2
21	2	2	5	2	5	5	4	2	2	2	2	1	3	2
22	1	2	5	3	5	5	3	1	2	1	2	2	2	1
23	1	2	4	1	5	3	4	1	2	1	2	3	2	1
24	2	3	5	1	4	4	4	2	3	2	3	3	5	2
25	3	1	3	2	5	5	5	3	1	3	1	2	5	3

Anexo 21. Procesamiento de datos Post-test



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
1	4	3	5	5	5	4	3	2	3	1	1	1	4	1
2	4	4	3	2	4	4	3	3	1	3	2	4	4	5
3	4	3	4	3	4	5	4	2	2	3	3	4	4	5
4	4	3	5	5	3	5	5	4	2	1	1	1	1	1
5	3	5	4	4	3	5	5	3	5	5	5	5	4	4
6	4	5	4	5	4	5	4	4	5	2	5	4	4	4
7	3	5	5	4	5	3	4	3	5	5	5	4	4	3
8	5	4	3	5	4	3	3	5	4	5	4	5	4	5
9	5	4	3	5	5	5	3	5	4	5	4	4	3	5
10	4	4	4	5	5	5	4	3	4	3	4	4	3	3
11	4	4	3	5	4	4	4	4	4	4	4	4	3	4
12	5	5	5	4	4	5	4	3	5	3	5	4	3	3
13	4	3	4	3	4	4	4	4	3	1	1	1	1	1
14	5	5	3	3	5	5	5	3	1	5	1	4	3	5
15	3	5	5	5	4	5	5	2	5	5	5	3	4	5
16	5	4	4	3	4	5	3	5	4	1	4	3	4	5
17	5	3	5	5	4	5	5	5	3	5	2	4	4	5
18	4	3	5	4	3	5	4	4	3	4	3	1	1	1
19	5	4	3	3	3	3	4	3	4	3	2	5	5	3
20	4	4	4	3	4	4	4	4	4	4	4	4	3	4
21	4	4	5	4	5	5	4	4	4	4	4	5	3	4
22	5	4	5	3	5	5	3	4	4	5	4	4	4	5
23	5	4	4	5	5	3	4	5	4	5	4	3	2	5
24	4	3	5	5	4	4	4	4	3	4	3	3	5	4
25	3	5	3	4	5	5	5	3	5	3	5	4	5	3

Anexo 22. Marco de trabajo basado en la gestión unificada de amenazas (UTM) para seguridad de la información en Municipalidades

Objetivo:

Determinar la eficacia del Marco de trabajo basado en la gestión unificada de amenazas (UTM) para la seguridad de la información en la Municipalidad de Miraflores. Adquiriendo una solución de seguridad perimetral proactiva, integral y flexible mediante la tecnología de gestión de amenazas (Next Generation Firewall) para la Municipalidad de Miraflores.

Justificación:

La Gerencia de Sistemas y Tecnologías de la Información conto con un equipo de propósito específico Firewall Fortigate 800C, para el control de acceso y protección de la información, el cual para su adecuado funcionamiento necesitaba licenciarse para su uso, la que permitiría la protección frente a páginas web maliciosas, aplicaciones orientadas al robo de información, etc., además brindo conexión remota segura para los colaboradores que vienen laborando en la modalidad "remoto" y actualizaciones que permiten minimizar los riesgos de detener los servicios informáticos que brinda la entidad. Estos equipos se encontraban instalados en alta disponibilidad en el centro de datos del Palacio Municipal y actualmente su licencia caduca el 31 de diciembre del 2021, y no cuentan con soporte técnico vigente y su vigencia tecnológica según el fabricante ha concluido.
Por lo expuesto se requiere adquirir una solución de seguridad perimetral proactiva, integral y flexible mediante tecnología de gestión de amenazas que cuente con funciones de firewall, sistema de prevención de intrusos (IPS), VPN, control de aplicaciones, filtrado de contenido web, supervisión de clientes, Priorización de tráfico (QoS), gestión del ancho de banda, etc. El objetivo general es garantizar la seguridad de la información y la continuidad y el correcto funcionamiento de las redes y comunicaciones, así como blindar a la entidad de ataques externos que vengan de personas o grupos locales e internacionales (Hackers, activistas, crackers, programadores, colaboradores internos y/o externos, y otras amenazas).

Finalidad:

Identificar, analizar, evaluar y dar tratamiento a los riesgos de seguridad de la información según el alcance del SGSI, en cumplimiento con la normativa vigente para garantizar razonablemente el logro de los objetivos estratégicos y operativos de la organización.

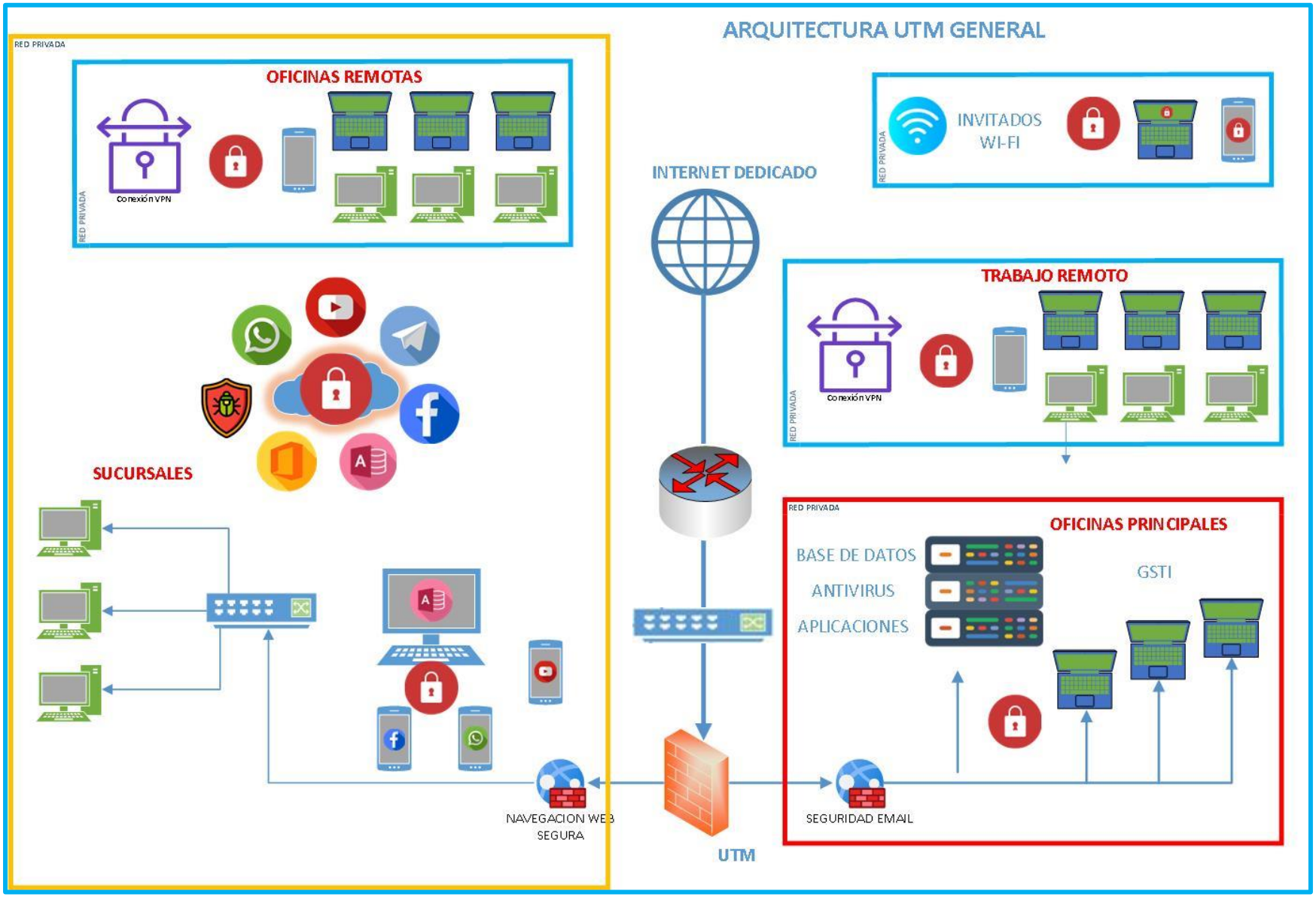
Alcance

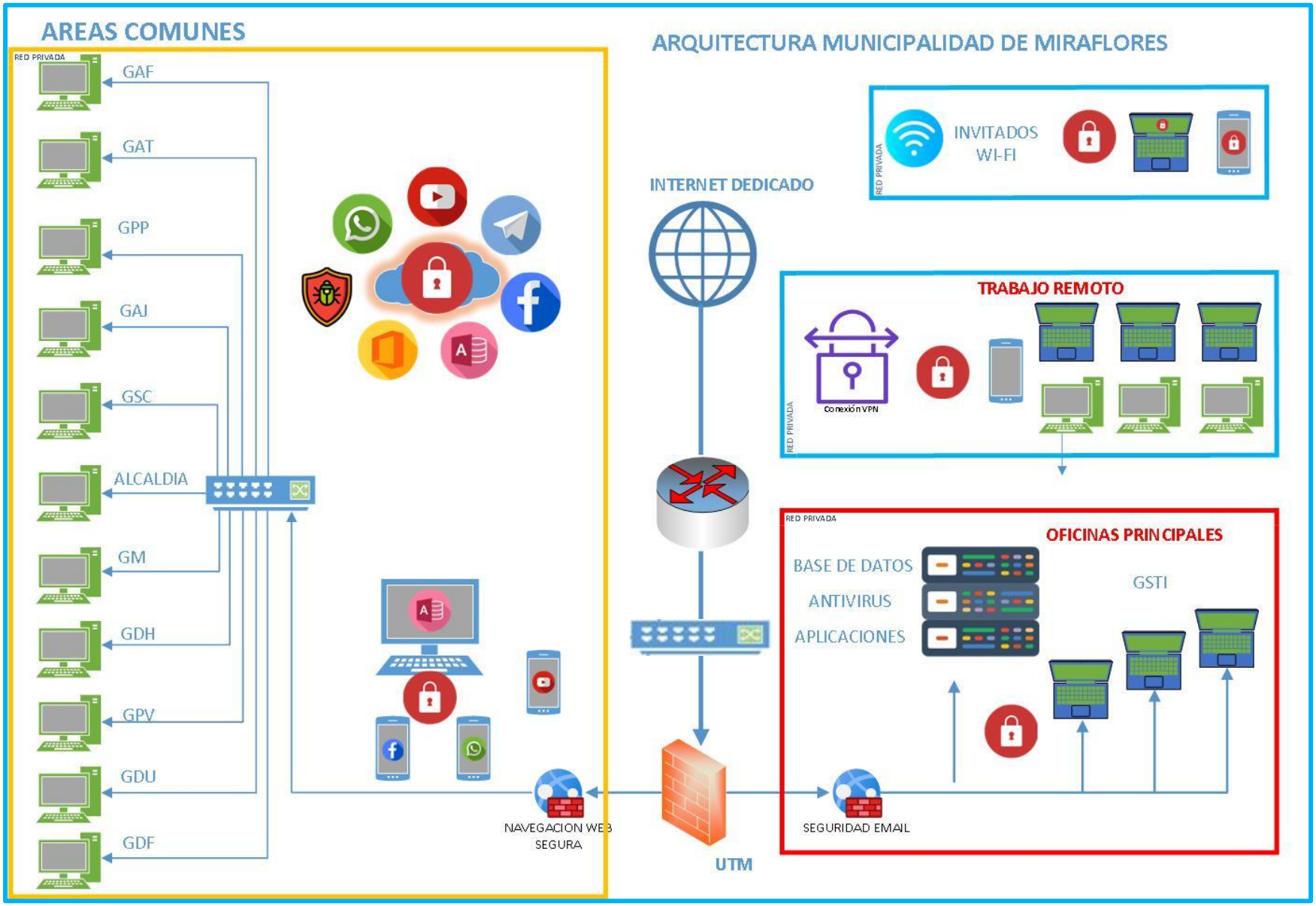
La municipalidad de Miraflores requiere una solución de Seguridad Gestionada Física a través de Firewalls Sophos XGS 3300 en Alta disponibilidad para la seguridad perimetral Las disposiciones contenidas en el presente documento se aplicarán en las actividades de gestión y tratamiento de los riesgos de seguridad de la información de la organización en el marco de los procesos contenidos dentro del Alcance.

RESPONSABLES

Propietarios de los Activos de la Información

- Municipalidad de Miraflores
- Gerencia de Sistemas Y tecnologías de la Información
- Gerente General
- Coordinador de redes y comunicaciones


ARQUITECTURA UTM GENERAL
RED PRIVADA
OFICINAS REMOTAS
Conexión VPN
RED PRIVADA
INVITADOS
WI-FI
RED PRIVADA
INTERNET DEDICADO
TRABAJO REMOTO
Conexión VPN
RED PRIVADA
SUCURSALES
RED PRIVADA
OFICINAS PRINCIPALES
BASE DE DATOS
ANTIVIRUS
APLICACIONES
GSTI
NAVEGACION WEB
SEGURA
SEGURIDAD EMAIL
UTM


AREAS COMUNES
ARQUITECTURA MUNICIPALIDAD DE MIRAFLORES
RED PRIVADA
GAF
GAT
GPP
GAJ
GSC
ALCALDIA
GM
GDH
GPV
GDU
GDF
INTERNET DEDICADO
INVITADOS
WI-FI
RED PRIVADA
TRABAJO REMOTO
Conexión VPN
RED PRIVADA
RED PRIVADA
OFICINAS PRINCIPALES
BASE DE DATOS
ANTIVIRUS
APLICACIONES
GSTI
NAVEGACION WEB
SEGURA
SEGURIDAD EMAIL
UTM

MARCO DE TRABAJO BASADO EN LA GESTIÓN UNIFICADA DE AMENZAS (UTM) PARA SEGURIDAD DE LA INFORMACIÓN EN MUNICIPALIDADES - MIRAFLORES

ENTRADA

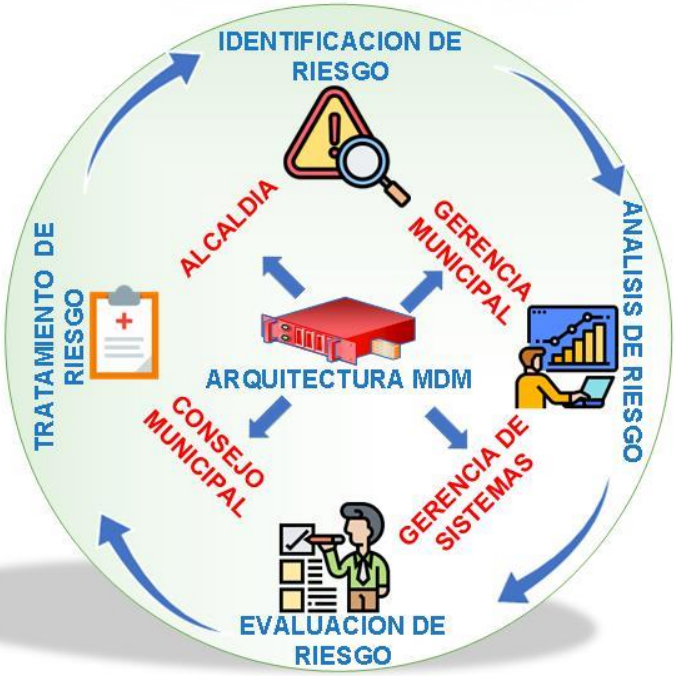
ETAPA 1

DIAGNOSTICO DE SEGURIDAD DE LA INFORMACION

COMPROMISO DE LA GERENCIA

VERIFICACIÓN DE REQUERIMIENTOS

- COMPROMISO
- REQUERIMIENTOS
- COSTOS
- POLITICAS
- MEJORAS



ETAPA 2

DESARROLLO Y EEJCUCION DEL MARCO DE TRABAJO

- CREAR ROLES
- CREAR POLITICAS
- REALIZAR PRUEBAS

Proceso

ETAPA 3

EVALUACION DE LA SEGURIDAD DE LA INFORMACION

CONFIDENCIALIDAD

% DE INTENTOS DE USAURIOS NO AUTORIZADOS

% DE AMENAZAS DETECTADAS

INTEGRIDAD

% DE INCIDENCIAS EN ACCESO APLICACIONES

% DE EQUIPOS DE COMPUTOS VULNERABLES

DISPONIBILIDAD

%DE DISPONIBILIDAD DE LOS SISTEMAS

% DE INCIDENCIAS EN EL DATA CENTER

SALIDA

ETAPA 1: DIAGNÓSTICO DE LA SEGURIDAD DE LA INFORMACIÓN:

Compromiso de la gerencia

- Implementación de Hardware en el centro de datos de la Gerencia de sistemas y tecnologías de la información.
- El contratista deberá realizar la implementación y migración de las reglas de seguridad y puesta en marcha.
- La generación e implementación de reglas deberá constar de: Firewall, IPS, VPN, Filtrado Web y de aplicaciones, antivirus, anti-spam

Deberá incluir capacitación para la administración del software.

Verificación de requerimiento

para este caso implemento un equipo UTM Sophos XGS 3300, El término **firewall UTM** o simplemente UTM (Unified Threat management/Gestión Unificada de Amenazas) es la nomenclatura dada a un dispositivo de hardware o software capaz de reunir diversas funciones de seguridad, como filtro de paquetes, proxy, sistemas de detección y prevención de intrusos , protección contra malware, control de aplicación, entre otros. De manera simplificada, el principal papel de un firewall en una red corporativa es regular el tráfico entre dos o más redes (internet y red interna, o redes internas, Internet y DMZ, entre otras), defendiendo los intereses y/o necesidades de control de las empresas.

Costos y beneficios

Detalle de la propuesta media Commerce Perú S.A.C.

Item	Descripción	Cant	Precio Total
1	XGS 3300 HW Appliance with 8 GE + 2 SFP + 2 SFP+ ports, 1 expansion bay for optional Flexi Port module, SSD + Base License (incl. FW, VPN & Wireless) for unlimited users + power cable	2	PEN 35,100.00
2	Licenciamiento Xstream Protection 12 - MOS	1	
3	Licenciamiento Email Protection 12 – MOS	1	
4	Servicio de configuración y puesta en marcha Soporte Técnico 24x7x365	1	PEN 0.00
		Total (PEN)	**PEN 35,100.00**

Detalle de la propuesta Darsystem E.I.R.L.

Cant.	DESCRIPCION	PRECIO UNITARIO US$	PRECIO TOTAL US$
2 UNID	FORTIGATE-600E HARDWARE PLUS 24X7 FORTICARE AND FORTIGUARD UNIFIED THREAT PROTECTION (UTP) - IMPORTARLO. Incluye las LICENCIAS por 1 año. (Soporte directo de la marca por 1 año.) con Ticket de atención.	12,685.00	25,370.00
2 UNID.	INSTALACION Y CONFIGURACION - Puesta en marcha e implementación. - Instalación de equipos de forma presencial - Configuración de licencias vía remoto - Migración de equipos y configuración presencial.	1,500.00	3,000.00
1 Uni.	SOPORTE STANDARD ANUAL - Local - Modalidad 8x5 - Soporte vía mesa de ayuda y correo - Soporte telefónico - Soporte Remoto (incluye: gestión, configuración)	1,800.00	1,500.00
5 Uni.	SOPORTE 24x7 - Local (Opcional) - Modalidad 24x7 (SLA 4 horas máximo) - Soporte vía mesa de ayuda y correo - Soporte telefónico - Soporte Remoto (incluye: gestión, configuración)	4,000.00	4,000.00
		SUB TOTAL US$	33,870.00
		IGV US$	6,096.60
		TOTAL US$	39,966.60

PRODUCTO	COSTO (Incluido IGV)	BENEFICIO
Firewall Fortigate 600E • Soporte estándar Anual 8x5 • Implementación • Capacitación • Licencia por 1 año	S/. 129,127.40	94
Firewall Sophos XGS 3300 • Licenciamiento 1 año • Configuración y puesta en marcha • Soporte técnico 24x7	S/. 35,100.00	95
Fuente: cotizaciones		

Toma de decisión

Propuesta de la empresa de MEDIA COMMERCE PERU S.A.C. por un precio de 39,966.60 nuevos soles

Políticas

La **política** del cortafuegos establece la configuración del cortafuegos en las estaciones de la red. Sólo las aplicaciones especificadas, o clases de aplicaciones, pueden acceder a la red empresarial o Internet.

Mejoras

La adquisición de la solución firewall permitirá a la Municipalidad distrital de Miraflores fortalecer y asegurar la seguridad perimetral de la Red local contra ataques externos e internos.

ETAPA 2: EJECUCION Y DESARROLLO DEL MARCO DE TRABAJO

Procedimientos

Las labores técnicas a realizar se llevarán a cabo en coordinación con la Gerencia de sistemas y tecnologías de la información.

Crear roles de navegación

Gerentes: acceso libre acceso

Sub Gerentes: acceso Limitado

Asistentes: acceso limitado

Colaboradores: solo a paginas gubernamentales

- Incluye la capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación.
- Posee integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.
- Identifica la IP y el usuario de Dominio en base a Event Viewer y WMI.
- Monitorear eventos de login y logout del Active Directory utilizando el

protocolo WinRM.

- Soporta la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios.
- Permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
- Permitir la definición de grupos dinámicos de usuarios.

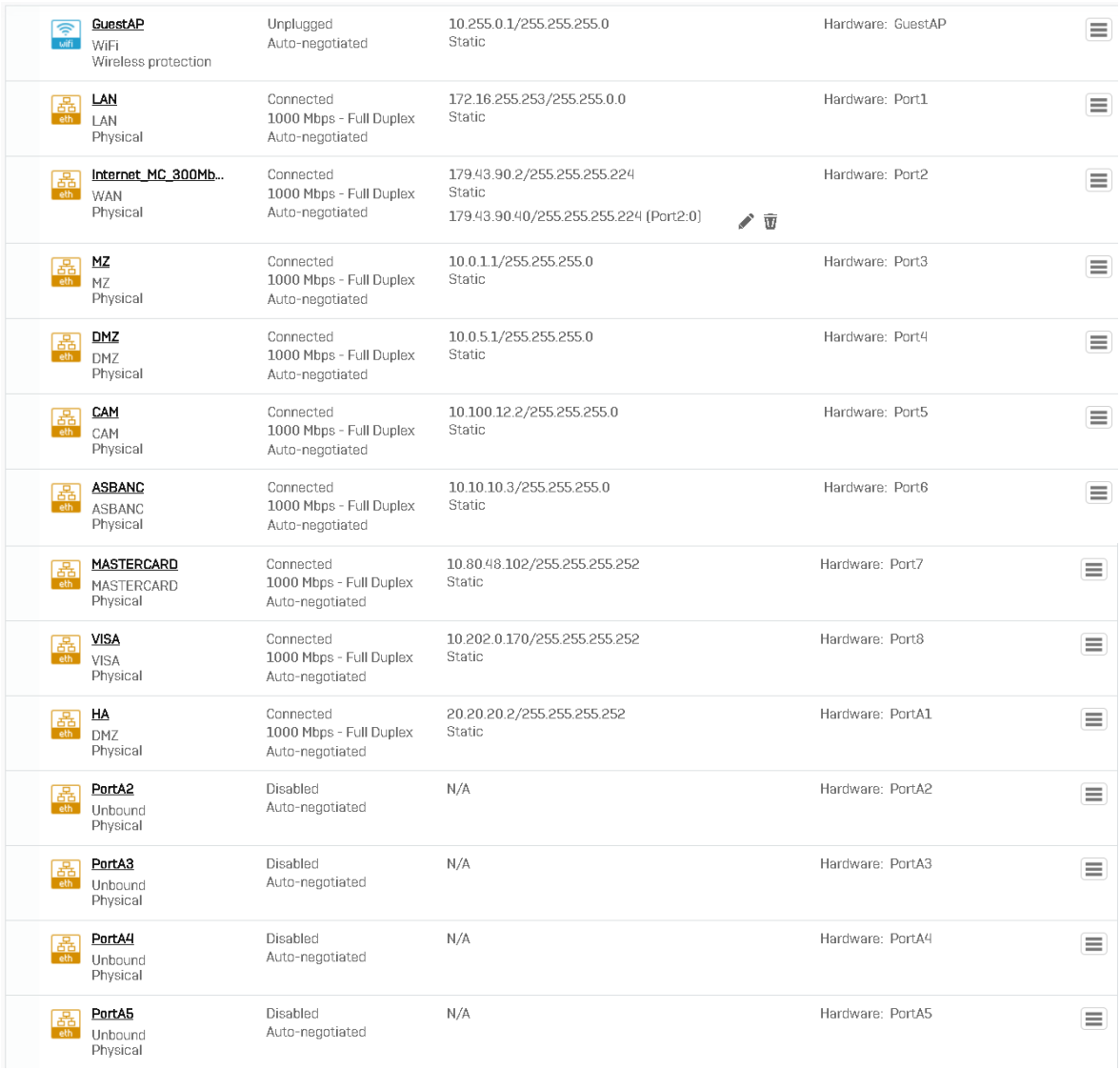
Crear políticas

- Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos) y categorías de aplicaciones.
- Deberá ser posible la identificación de la aplicación y la inspección de malware, spyware y exploits dentro del tráfico cifrado por los protocolos en mención.
- Permitir configurar, habilitar y programar políticas de seguridad por horario, teniendo la capacidad de habilitarse y deshabilitarse de manera automática sin requerir manipulación alguna por parte del analista de red.
- Las políticas de seguridad deben mostrar el tráfico consumido desde su creación.

Realizar pruebas

Paso 1- Configuración: Direccionamiento de IP

A continuación, se puede observar todo el direccionamiento IP que se configuró en cada una de las interfaces del dispositivo.



GuestAP WiFi Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static	Hardware: GuestAP	
LAN LAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	172.16.255.253/255.255.0.0 Static	Hardware: Port1	
Internet_MC_300Mb... WAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	179.43.90.2/255.255.255.224 Static 179.43.90.40/255.255.255.224 (Port2:0)	Hardware: Port2	
MZ MZ Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	10.0.1.1/255.255.255.0 Static	Hardware: Port3	
DMZ DMZ Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	10.0.5.1/255.255.255.0 Static	Hardware: Port4	
CAM CAM Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	10.100.12.2/255.255.255.0 Static	Hardware: Port5	
ASBANC ASBANC Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	10.10.10.3/255.255.255.0 Static	Hardware: Port6	
MASTERCARD MASTERCARD Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	10.80.48.102/255.255.255.252 Static	Hardware: Port7	
VISA VISA Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	10.202.0.170/255.255.255.252 Static	Hardware: Port8	
HA DMZ Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	20.20.20.2/255.255.255.252 Static	Hardware: PortA1	
PortA2 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortA2	
PortA3 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortA3	
PortA4 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortA4	
PortA5 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortA5	

PortA6 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortA6	
PortA7 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortA7	
PortA8 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortA8	
PortF1 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortF1	
PortF2 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortF2	
PortF3 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortF3	
PortF4 Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortF4	
PortMGMT Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortMGMT	

Paso 2 - Configuración: Enrutamiento:

En la siguiente grafica se muestran los enrutamientos realizados, red destino, interface y Gateway.

10.21.0.0 / 255.255.0.0	172.16.3.50	LAN	0	
192.168.51.0 / 255.255.255.0	172.16.3.50	LAN	0	
10.80.67.11 / 255.255.255.255	10.80.48.101	MASTERCARD	0	
10.80.67.29 / 255.255.255.255	10.80.48.101	MASTERCARD	0	
10.118.253.101 / 255.255.255.255	10.202.0.169	VISA	0	
10.100.1.0 / 255.255.255.0	10.100.12.1	CAM	0	
10.100.3.0 / 255.255.255.0	10.100.12.1	CAM	0	
10.100.10.0 / 255.255.255.0	10.100.12.1	CAM	0	
192.168.200.0 / 255.255.255.0	10.100.12.1	CAM	0	
192.168.221.0 / 255.255.255.0	10.100.12.1	CAM	0	
192.168.203.0 / 255.255.255.0	10.100.12.1	CAM	0	
10.100.13.0 / 255.255.255.0	10.100.12.1	CAM	0	
10.100.9.0 / 255.255.255.0	10.100.12.1	CAM	0	

192.168.100.0 / 255.255.255.0	10.100.12.1	CAM	0		
192.168.201.0 / 255.255.255.0	10.100.12.1	CAM	0		
192.168.202.0 / 255.255.255.0	10.100.12.1	CAM	0		
192.168.204.0 / 255.255.255.0	10.100.12.1	CAM	0		
192.168.210.0 / 255.255.255.0	10.100.12.1	CAM	0		
192.168.211.0 / 255.255.255.0	10.100.12.1	CAM	0		
192.168.212.0 / 255.255.255.0	10.100.12.1	CAM	0		
10.100.8.0 / 255.255.255.0	10.100.12.1	CAM	0		
10.100.6.0 / 255.255.255.0	10.100.12.1	CAM	0		
192.165.1.0 / 255.255.255.0	10.100.12.1	CAM	0		
10.100.14.0 / 255.255.255.0	10.100.12.1	CAM	0		
10.100.2.0 / 255.255.255.0	10.100.12.1	CAM	0		
192.168.222.0 / 255.255.255.0	10.100.12.1	CAM	0		
192.168.220.0 / 255.255.255.0	10.100.12.1	CAM	0		
192.168.220.0 / 255.255.255.0	10.100.12.1	CAM	0		
10.100.5.0 / 255.255.255.0	10.100.12.1	CAM	0		
172.18.0.0 / 255.255.0.0	172.16.3.50	LAN	0		
172.17.0.0 / 255.255.0.0	172.16.3.50	LAN	0		
172.23.0.0 / 255.255.0.0	172.16.3.50	LAN	0		
172.22.0.0 / 255.255.0.0	172.16.3.50	LAN	0		
172.24.0.0 / 255.255.255.0	172.16.3.50	LAN	0		

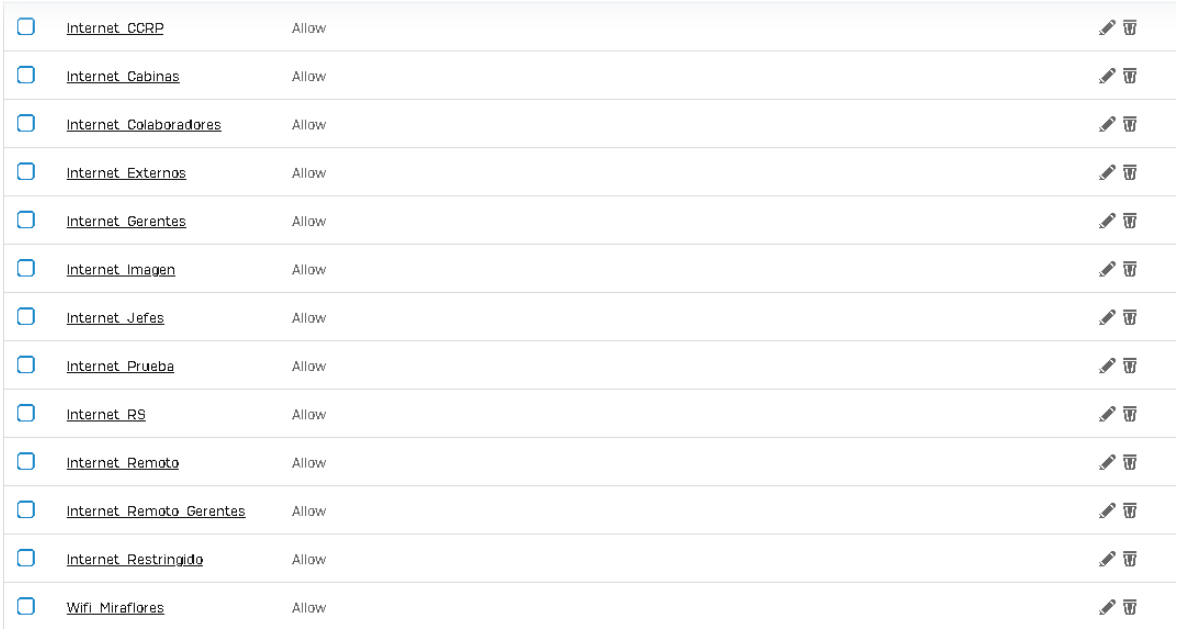
Paso 3 - Configuración: Filtrado web

A continuación, se observan los perfiles de filtrado web creados, estos son aplicados a las políticas de firewall dependiendo si el usuario es restringido o de libre acceso a internet**.**

Default Workplace Policy	Deny access to categories most commonly unwanted in professional environments	0 ⚠	
Internet_Cabinas		1	
Internet_Colaboradores		8	
Internet_Externos		1	
Internet_Imagenes		1	
Internet_Jefes		1	
Internet_Prueba	WebFilter de Prueba	1	
Internet_Remoto		2	
Internet_gerentes		1	
No Ads or Explicit Content	Deny access to advertisements and sexually explicit sites	0 ⚠	
No Explicit Content	Deny access to sexually explicit sites	8	
No Games Ads or Explicit Content	Deny access to games, advertisements, and sexually explicit sites	0 ⚠	
No Online Chat	Deny access to online chat sites	0 ⚠	
No Web Mail	Deny access to web mail sites	0 ⚠	
No Web Mail or Chat	Deny access to web mail and online chat sites	0 ⚠	
No web uploads	Restrict users from uploading content to any site	0 ⚠	
internet_RS		1	

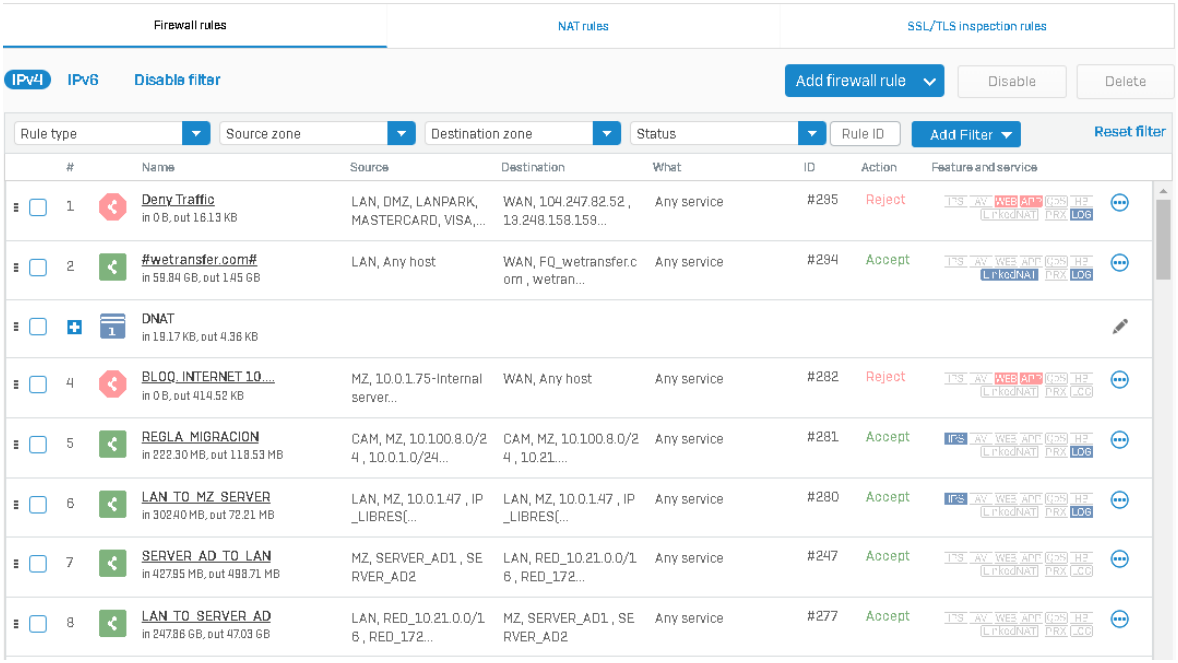
Paso 4 - Configuración: Control de aplicaciones

Con el control de aplicaciones se bloqueó el software no productivo instalado en los equipos de cómputo y dispositivos móviles según su requerimiento, por motivos de seguridad se aplica restricción a todos los usuarios sin excepción del software tipo proxy y túnel.

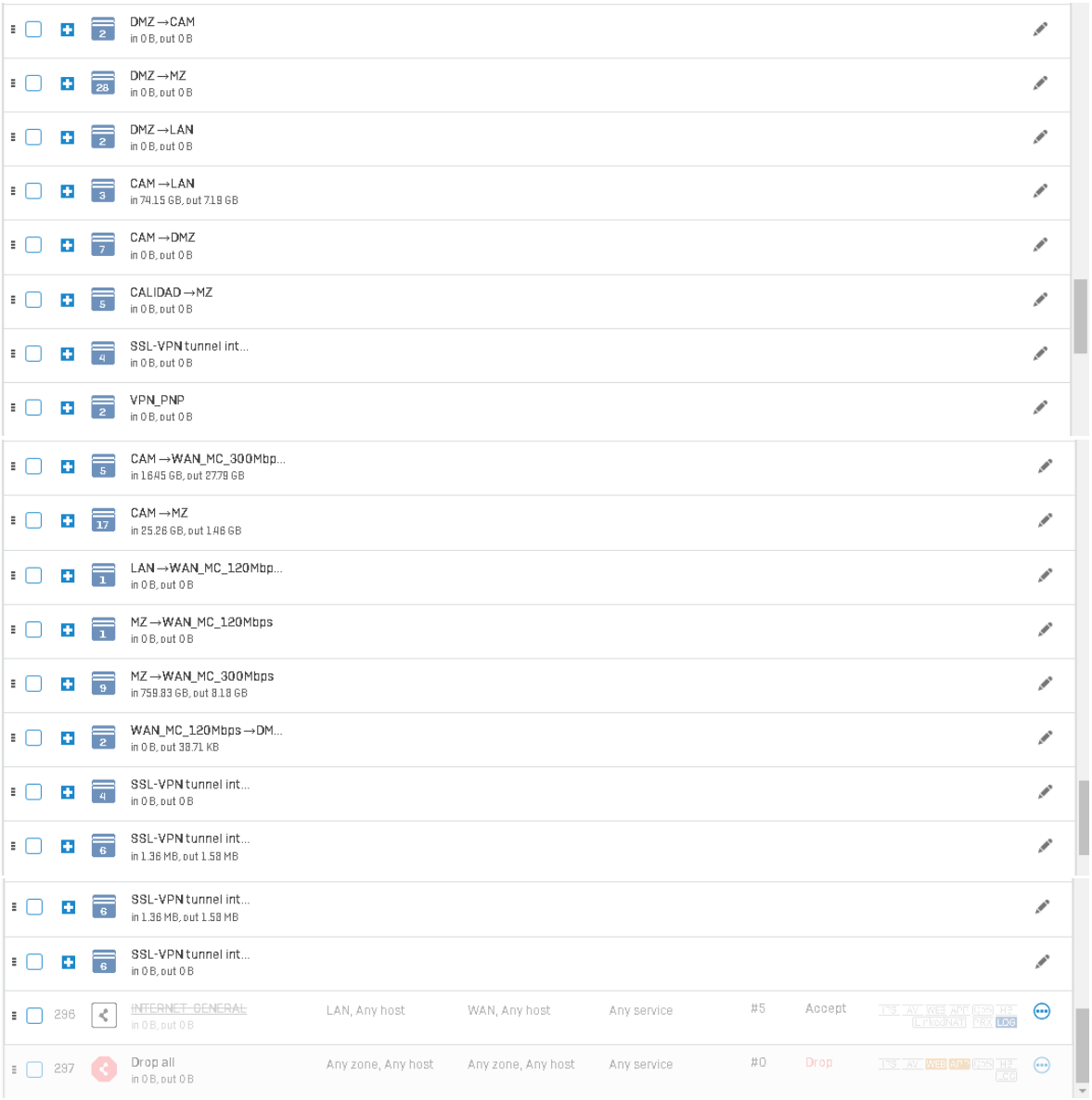


Paso 5- Configuración: Políticas de firewall

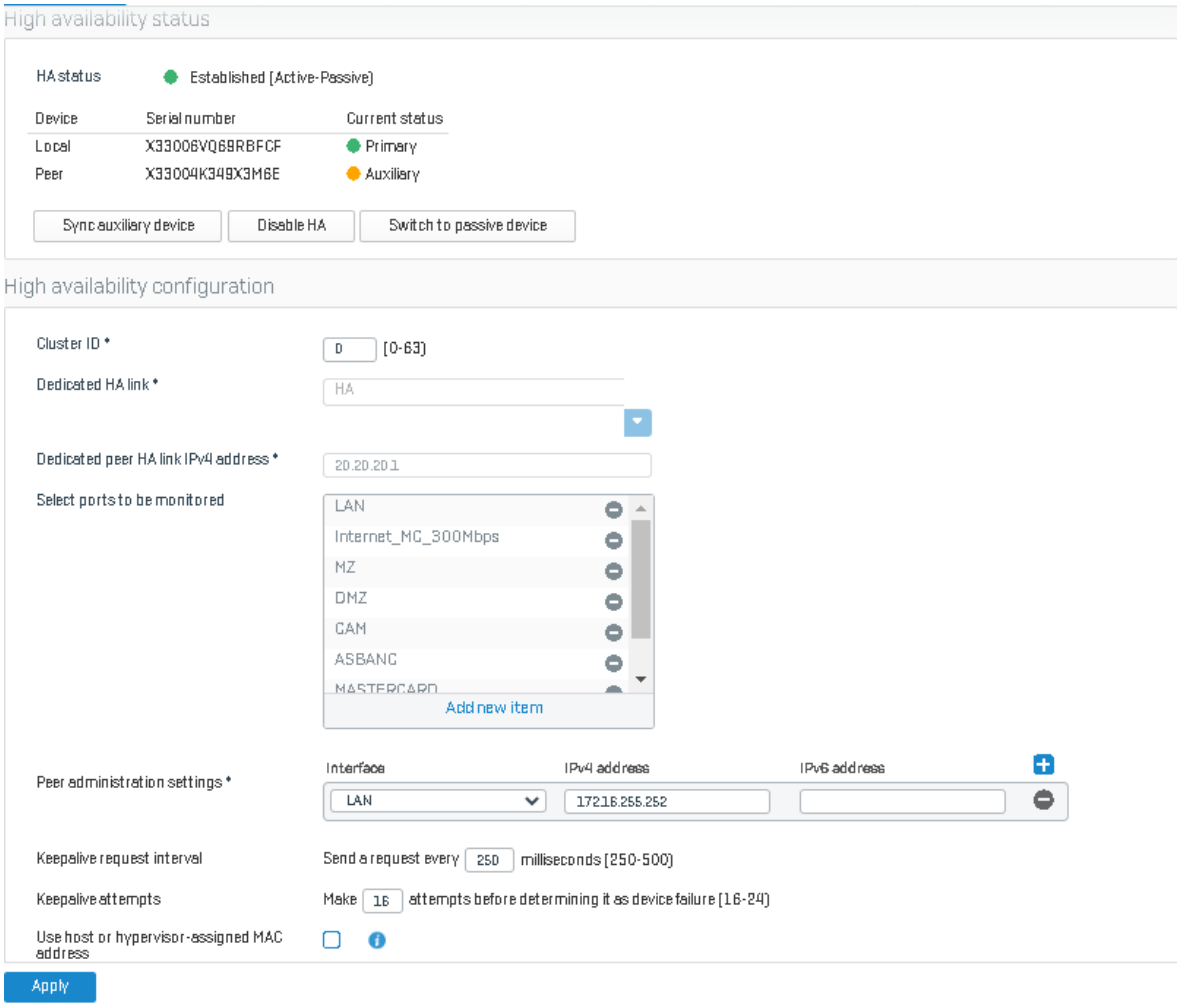
A continuación, se observan las políticas de firewall configuradas, en todas las políticas se aplicó el respectivo control IPS, filtro WEB y de aplicaciones para la seguridad perimetral contra el Ransomware y otros ataques que afectan algún tipo de vulnerabilidad de la red.



		18	WAN_MC_300Mbps→DM... in 751.55 GB, out 15.92 GB						
		18	WAN_MC_300Mbps→MZ in 31.09 GB, out 4.89 GB						
	45		DMZ_TO_MZ---MZ_TO_... in 259.52 GB, out 162.41 GB	DMZ, MZ, Any host	DMZ, MZ, Any host	Any service	#276	Accept	TLS AV WEB APP QOS H3 L7 modNAT PRX LOG
	46		DMZ_TO_CAM---CAM_T... in 5.79 GB, out 4.56 GB	DMZ, CAM, Any host	DMZ, CAM, Any host	Any service	#274	Accept	TLS AV WEB APP QOS H3 L7 modNAT PRX LOG
	47		VPN_to_LAN in 23.70 GB, out 4.65 GB	VPN, Any host, Any live user	LAN, DMZ, CAM, MZ, Any host	Any service	#271	Accept	TLS AV WEB APP QOS H3 L7 modNAT PRX LOG
	48		LAN_to_VPN in 98.42 MB, out 88.10 MB	LAN, MZ, Any host, Any live user...	VPN, Any host	Any service	#270	Accept	TLS AV WEB APP QOS H3 L7 modNAT PRX LOG
		5	ASBANC→MZ in 26.76 MB, out 28.42 MB						
		12	DMZ→WAN_MC_300Mbp... in 1.72 GB, out 64.93 MB						
		2	ASBANC→WAN_MC_300... in 0 B, out 0 B						
		2	WIFI→MZ in 0 B, out 0 B						
		32	LAN→WAN_MC_300Mbp... in 4.97 TB, out 795.22 GB						
		1	MZ→LAN-PARK in 0 B, out 0 B						
		10	MZ→LAN in 13.75 TB, out 640.73 GB						
		13	MZ→DMZ in 0 B, out 0 B						
		4	MZ→CAM in 1.77.41 MB, out 188.37 MB						
		4	MZ→ASBANC in 4.15 MB, out 4.15 MB						
		1	LAN→VISA in 0 B, out 1.38 KB						
		34	LAN→MZ in 3.50 TB, out 1.26 TB						
		1	LAN→MASTERCARD in 0 B, out 0 B						
		1	LAN→LAN-PARK in 0 B, out 0 B						
		12	LAN→DMZ in 96.83 GB, out 1.842 GB						
		7	LAN→CAM in 786.83 GB, out 13.35 GB						
		1	LAN→CALIDAD in 0 B, out 0 B						
		1	LAN→ASBANC in 0 B, out 71.22 KB						


DMZ→CAM
in 0 B, out 0 B
DMZ→MZ
in 0 B, out 0 B
DMZ→LAN
in 0 B, out 0 B
CAM→LAN
in 74.15 GB, out 7.19 GB
CAM→DMZ
in 0 B, out 0 B
CALIDAD→MZ
in 0 B, out 0 B
SSL-VPN tunnel int...
in 0 B, out 0 B
VPN_PNP
in 0 B, out 0 B
CAM→WAN_MC_300Mbp...
in 1.645 GB, out 27.79 GB
CAM→MZ
in 25.26 GB, out 1.46 GB
LAN→WAN_MC_120Mbp...
in 0 B, out 0 B
MZ→WAN_MC_120Mbps
in 0 B, out 0 B
MZ→WAN_MC_300Mbps
in 759.83 GB, out 8.18 GB
WAN_MC_120Mbps→DM...
in 0 B, out 38.71 KB
SSL-VPN tunnel int...
in 0 B, out 0 B
SSL-VPN tunnel int...
in 1.36 MB, out 1.58 MB
SSL-VPN tunnel int...
in 1.36 MB, out 1.58 MB
SSL-VPN tunnel int...
in 0 B, out 0 B
296
INTERNET-GENERAL
in 0 B, out 0 B
LAN, Any host
WAN, Any host
Any service
#5
Accept
297
Drop all
in 0 B, out 0 B
Any zone, Any host
Any zone, Any host
Any service
#0
Drop

Paso 6 - Configuración: En alta disponibilidad del hardware



HA (alta disponibilidad

ETAPA 3: Evaluación De La Seguridad De La Información

Confidencialidad:

nuestro marco de trabajo se ha desarrollado básicamente en las áreas comunes que manejan todas las municipalidades por ejemplo alcaldía, consejo municipal, gerencia municipal y áreas que gerencian el servicio a la sociedad que tienen como objetivo la tributación, la seguridad, fiscalización, catastro, entro otros. en base a esas áreas comunes lo que nosotros hemos hecho es trabajar este marco de trabajo utm para que se conecten a estas áreas directamente de acuerdo a sus políticas que están como base central y así las áreas manejen sus riesgos en función a la documentación y facilita el acceso a los datos de personas y organizaciones con los cuales se puede trabajar mediante la autenticación basada en el UTM

- **Velocidad**: gracias a datos oportunos, verídicos y confidenciales que aporten valor al proceso.
- **Seguridad**: a través de canales y vías seguras que garanticen solo el acceso a quienes tengan las credenciales necesarias.
- **Sin límites**: que permita acceso total sin tope a los colaboradores para agilizar los procesos, operaciones y servicios.

Integridad:

La **integridad de los datos** alude a ese atributo o cualidad que es inherente a la información cuando se considera exacta, completa, homogénea, sólida y coherente con la intención de los creadores de los datos que la conforman. La municipalidad mantendrá la integridad en las áreas específicas tras la implementación del UTM que garantiza la fidelidad de la información a todos los usuarios y contribuyentes y de esta manera se garantiza la originalidad de toda documentación

Disponibilidad:

La gerencia de sistema y tecnología de la información pone determinados mecanismos que garantizan que los interesados que estén autorizados a acceder a esta información puedan hacer de forma segura y sencilla. Es clave que el informático garantice que se pueda acceder tanto a estos datos como a procesos

en sí en cualquier momento de forma rápida y sencilla y solucionar posibles problemas cuando puedan surgir.

Con la implementación del marco de trabajo la seguridad de la información mantendrá la disponibilidad en cualquier momento que el usuario o contribuyente lo requiera las 24 horas al día los 365 días al año

Areas comunes:

GAF: Es el órgano de apoyo, responsable de conducir el proceso de la **administración** a través de los sistemas de logística, personal, tesorería y contabilidad.

GAT: Es un órgano de línea, responsable de dirigir, ejecutar, controlar y supervisar las acciones relacionadas con la recaudación y captación de tributos; así como la obtención de rentas municipales; estableciendo adecuados sistemas de fiscalización, recaudación y control; que garantice cumplir con la ejecución del presupuesto de ingresos en cada ejercicio fiscal, debiendo establecer políticas de gestión y estrategias para simplificar los procesos tributarios de fiscalización y recaudación.

GPP: La Gerencia de Participación Vecinal promueve la participación organizada de la ciudadanía, a fin de generar una cultura cívica, responsable y vigilante de los asuntos de la gestión local, así como, de un sistema de comunicación e información a los ciudadanos sobre los objetivos, metas, acciones de la gestión municipal, a través de los distintos medios y canales para hacer llegar los mensajes en forma oportuna y eficaz.

GAJ: Es el órgano de asesoramiento que desarrolla funciones consultivas en materia jurídica, encargado de organizar, coordinar, evaluar y supervisar la ejecución de carácter jurídico; así como brindar asesoramiento sobre la adecuada interpretación, aplicación y difusión de las normas de competencia municipal.

GSC: Es el órgano de línea responsable de conducir y supervisar los procesos vinculados con la seguridad ciudadana, contribuyendo a asegurar la convivencia pacífica, el control de la violencia urbana y la prevención de delitos y faltas

ALCALDIA: Asesorar legalmente a entidades públicas para llevar un control en sus planes y proyectos, supervisa que los proyectos este de acuerdo a la ley y no permitir que haya falta en la parte legal de la entidad.

GM: Es un órgano de más alto nivel jerárquico, responsable de la Dirección Administrativa General de la Municipalidad, su función básica es el de planear, organizar, dirigir, coordinar y controlar la ejecución de las actividades y/o proyectos de los órganos de Administración Municipal

GDH: La Gerencia de Desarrollo Humano busca contribuir con el desarrollo integral de los miraflorinos en cada etapa de vida, en relación con su familia y comunidad, a través del fortalecimiento de capacidades por medio de la creación de entornos que le brinden las oportunidades para tener una vida sana, productiva y creativa.

GPV: Es el órgano de línea responsable de promover, facilitar, articular y fortalecer espacios de participación para la ciudadanía en general, en la provincia de Lima y en la gestión y desarrollo de acciones en beneficio de la comunidad, dentro del marco de los dispositivos legales aplicables.

GDU: Es el órgano de línea responsable de conducir y supervisar los procesos de autorizaciones, certificaciones, adjudicaciones, asentamientos humanos, renovación urbana, saneamiento legal y físico de predios tugurizados, concernientes al desarrollo urbano dentro del marco de los dispositivos legales aplicables.

GDF: Es el órgano de línea responsable de conducir y supervisar los procesos de gestión del riesgo de desastres en la jurisdicción de la provincia de Lima, de conformidad con la normatividad que regula la materia.