UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

==========

SEGURIDAD PERIMETRAL INFORMÁTICA Y LA GESTION DE SERVICIOS DE TI EN LAS UNIVERSIDADES PÚBLICAS DE LA AMAZONÍA PERUANA, 2021

==========

Tesis

Para optar el título profesional de:

INGENIERO DE SISTEMAS

TESISTAS : **Bach. Jack Junior Torres Reategui**

Bach. Erick Erasmo Loli Romero

ASESOR : **MSc. Oscar Amado Ruiz Torres**

PUCALLPA - PERÚ

2022

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL
ESCUELA PROFESIONAL DE INGENIERÍA CIVIL
COMISIÓN DE GRADOS Y TÍTULOS

ACTA DE EVALUACIÓN DE SUSTENTACIÓN DE TESIS N° 019-2022

GRADUANDO : **Bach. ERICK ERASMO LOLI ROMERO**
Bach. JACK JUNIOR TORRES REÁTEGUI

TEMA : **"SEGURIDAD PERIMETRAL INFORMÁTICA Y LA GESTION DE SERVICIOS DE TI EN LAS UNIVERSIDADES PÚBLICAS DE LA AMAZONÍA PERUANA ,2021".**

ASESOR : **MG. OSCAR AMADO RUIZ TORRES**

CRITERIOS	PUNTAJE			
	3	2	1	0
I- PRESENTACION				
* MOTIVACION		x		
* TONO DE VOZ		x		
* CALIDAD DE MATERIAL AUDIOVISUAL		x		
II- DESARROLLO DE CONTENIDO				
* SECUENCIA	x			
* DOMINIO DE VOZ		x		
* USO ADECUADO DEL MATERIAL		x		
* VALIDEZ DE LOS HALLAZGOS	x			
III- ABSOLUCION DE PREGUNTAS				
* RESPONDE A LAS PREGUNTAS FORMULADAS POR EL JURADO		x		
IV- APORTE CIENTIFICO Y TECNOLOGICO				
* AL DESARROLLO DE LA COMUNIDAD		x		
* A LA PROFESION		x		

EVALUACION

- EXCELENCIA 26 A 30 PUNTOS
- UNANIMIDAD 21 A 25 PUNTOS
- MAYORIA 16 A 20 PUNTOS
- DESAPROBADO 15 A MENOS

CALIFICACION FINAL:

PUNTAJE : 22 / 30

CONCLUSIONES:

APROBADO POR : UNANIMIDAD
DESAPROBADO POR :

JURADO EVALUADOR

- DR. NILTON CESAR AYRA APAC — Presidente
- MG. ARTURO YUPANQUI VILLANUEVA — Miembro
- MG. CESAR AUGUSTO AGURTO CHERRE — Miembro

SECRETARIA ACADÉMICA: M.SC. CLOTILDE RÍOS HIDALGO DE CERNA

PUCALLPA, 07 DE DICIEMBRE DEL 2022

"SEGURIDAD PERIMETRAL INFORMÁTICA Y LA GESTION DE SERVICIOS DE TI EN LAS UNIVERSIDADES PÚBLICAS DE LA AMAZONÍA PERUANA, 2021"

Elaborado por:

Bach. Jack Junior Torres Reategui.

Bach. Erick Erasmo Loli Romero.

Aprobado por:

Dr. Nilton Cesar Ayra Apac.
Presidente

Ing. Mg. Arturo Yupanqui Villanueva.
Miembro

Ing. Mg. Cesar Augusto Agurto Cherre.
Miembro

Asesor:

MSc. Oscar Amado Ruiz Torres.

UNIVERSIDAD NACIONAL DE UCAYALI
VICERRECTORADO DE INVESTIGACION
DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACION

SISTEMA ANTIPLAGIO URKUND

Nº V/0633-2022

La **Dirección de Producción Intelectual**, hace constar por la presente, que el Informe Final de Tesis, **titulado:**

"SEGURIDAD PERIMETRAL INFORMÁTICA Y LA GESTIÓN DE SERVICIOS DE TI EN LAS UNIVERSIDADES PÚBLICAS DE LA AMAZONÍA PERUANA, 2021".

Autor (es)	:	**TORRES REATEGUI, JACK JUNIOR** **LOLI ROMERO, ERICK ERASMO**
Facultad	:	INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL
Escuela Profesional	:	ING. SISTEMAS
Asesor (a)	:	M.Sc. Ruiz Torres, Oscar Amado

Después de realizado el análisis correspondiente en el Sistema Antiplagio URKUND, dicho documento presenta un **porcentaje de similitud de 9%.**

En tal sentido, de acuerdo a los criterios de porcentaje establecidos en el artículo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO URKUND, el cual indica que no se debe superar el 10%. Se declara, que el trabajo de investigación: SI Contiene un porcentaje aceptable de similitud, por lo que SI se aprueba su originalidad.

En señal de conformidad y verificación se firma y se sella la presente constancia.

FECHA 03/10/2022

Mg. JOSÉ MANUEL CÁRDENAS BERNAOLA
Director de Producción Intelectual

AUTORIZACIÓN DE PUBLICACIÓN DE TESIS

REPOSITORIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI

Yo, Jack Junior Torres Reategui

Autor(a) de la TESIS de pregrado titulada:

"SEGURIDAD PERIMETRAL INFORMATICA Y LA GESTION DE SERVICIOS DE TI EN LAS UNIVERSIDADES PUBLICAS DE LA AMAZONIA PERUANA, 2021"

Sustentada el año: 2022

Con la asesoría de: Msc. Oscar Amado Ruiz Torres

En la Facultad: Ingeniería de Sistemas e Ingeniería Civil

Escuela profesional: Ingeniería de Sistemas

Autorizo la publicación:

PARCIAL ☐ Significa que se publicará en el repositorio institucional solo La caratula, la dedicatoria y el resumen de la tesis. Esta opción solo es válida marcar **si su tesis o documento presenta material patentable**, para ello deberá presentar el trámite de CATI y/o INDECOPI cuando se lo solicite la DGPI UNU.

TOTAL ☒ Significa que todo el contenido de la tesis y/o documento será publicada en el repositorio institucional.

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali **licencia no exclusiva** para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la **tesis es una creación de mi autoría** y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 07 / 12 / 2022

Email: jackjtr21@gmail.com
Teléfono: 993935342

Firma:
DNI: 72814818

AUTORIZACIÓN DE PUBLICACIÓN DE TESIS

REPOSITORIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI

Yo, ERICK ERASMO LOLI ROMERO

Autor(a) de la TESIS de pregrado titulada:

"SEGURIDAD PERIMETRAL INFORMATICA Y LA GESTION DE SERVICIOS DE TI EN LAS UNIVERSIDADES PÚBLICAS DE LA AMAZONIA PERUANA, 2021"

Sustentada el año: 2022

Con la asesoría de: Msc Oscar Amado Ruiz Torres

En la Facultad: Ingenieria de Sistemas e Ingenieria Civil

Escuela profesional: Ingenieria de Sistemas

Autorizo la publicación:

PARCIAL [ ] Significa que se publicará en el repositorio institucional solo La caratula, la dedicatoria y el resumen de la tesis. Esta opción solo es válida marcar **si su tesis o documento presenta material patentable**, para ello deberá presentar el trámite de CATI y/o INDECOPI cuando se lo solicite la DGPI UNU.

TOTAL [X] Significa que todo el contenido de la tesis y/o documento será publicada en el repositorio institucional.

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali **licencia no exclusiva** para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la **tesis es una creación de mi autoría** y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 07/12/2022

Email: ERICKLOLI_RE3@GMAIL.COM Firma:

Teléfono: 956965466 DNI: 46471896

DEDICATORIA

El presente trabajo lo dedicamos a Dios, por ser el inspirador y darnos fuerza para continuar en este proceso de obtener uno de los anhelos más deseados.

Los autores

AGRADECIMIENTO

Gracias a nuestros padres, por ser los principales promotores de nuestros sueños, por confiar y creer en nuestras expectativas, por los consejos, valores y principios que nos han inculcado.

Los autores

INDICE DE CONTENIDO

DEDICATORIA vii
AGRADECIMIENTO viii
INDICE DE CONTENIDO ix
INDICE DE ANEXOS xvi
RESUMEN xvii
INTRODUCCIÓN xix
CAPITULO I 21
PLANTEAMIENTO DEL PROBLEMA 21
1.1. DESCRIPCIÓN Y FUNDAMENTACIÓN DEL PROBLEMA 21
1.2. FORMULACIÓN DEL PROBLEMA 22
1.2.1. Problema general 22
1.2.2. Problemas específicos 22
1.3. OBJETIVOS 23
1.3.1. Objetivo general 23
1.3.2. Objetivo específico 23
1.4. JUSTIFICACIÓN, IMPORTANCIA Y LIMITACIONES 24
1.4.1. JUSTIFICACIÓN 24
1.4.2. IMPORTANCIA. 24
1.4.3. LIMITACIONES. 25
1.5. HIPÓTESIS 25
1.5.1. Hipótesis General. 25
1.5.2. Hipótesis Específica. 25
1.6. DELIMITACIONES DE LA INVESTIGACIÓN 26
1.6.1. Delimitación Espacial. 26
1.6.2. Delimitación Social. 26
1.6.3. Delimitación Temporal. 26
1.6.4. Delimitación Conceptual. 27
1.7. VARIABLES 27
1.7.1. Variable independiente: 27
1.7.2. Variable dependiente: 27
1.7.3. Variable interviniente: 27

1.8. SISTEMA DE VARIABLES, DIMENSIONES E INDICADORES. 28
CAPITULO II 31
MARCO TEÓRICO.....31
2.1. ANTECEDENTES DEL PROBLEMA.....31
2.2. BASES TEÓRICAS 37
2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS 44
CAPITULO III 46
METODOLOGÍA DE LA INVESTIGACIÓN 46
3.1. METOGOLOGÍA Y TÉCNICAS UTILIZADAS. 46
3.1.1. Tipo de investigación. 46
3.1.2. Nivel de investigación. 46
3.1.3. Método de investigación. 46
3.1.4. Diseño de la investigación.....47
3.2. POBLACIÓN Y MUESTRA DE LA INVESTIGACIÓN.....48
3.2.1. Población 48
3.2.2. Muestra 48
3.3. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS 49
3.4. PROCEDIMIENTO DE RECOLECCIÓN DE DATOS 49
3.5. TRATAMIENTO DE DATOS. 49
CAPITULO IV 50
SEGURIDAD PERIMETRAL 50
4.1. UNIVERSIDAD NACIONAL DE UCAYALI.....50
4.1.1. INSTITUCIÓN 50
4.1.2. HISTORIA. 50
4.1.3. DESCRIPCIÓN ACTUAL DE LA ARQUITECTURA.....51
4.1.4. PROPUESTA DE SOLUCIÓN E IMPLEMENTACIÓNES DE SOLUCIONES.....66
4.2. UNIVERSIDAD NACIONAL INTERCULTURAL DE LA AMAZONIA -UNIA 89
4.2.1. INSTITUCIÓN 89
4.2.2. HISTORIA 89
4.2.3. DESCRIPCIÓN ACTUAL DE LA ARQUITECTURA.....89
4.2.4. PROPUESTA DE SOLUCIÓN E IMPLEMENTACIÓN DE SOLUCIÓN. 96

CAPITULO V RESULTADOS Y DISCUSIÓN.....118
5.1 Procesamiento de datos de la Variable Seguridad Perimetral.....118
5.1.1. Procesamiento de datos de la Dimensión Políticas 119
5.1.2. Procesamiento de datos de la Dimensión Aspectos organizativos 120
5.1.3 Procesamiento de datos de la Dimensión Control de Accesos.....121
5.1.4. Procesamiento de datos de la Dimensión Seguridad en la Operación 122
5.1.5. Procesamiento de datos de la Dimensión Seguridad en las Telecomunicaciones 123
5.1.6. Procesamiento de datos de la Dimensión Adquisición y Desarrollo 124
5.1.7. Procesamiento de datos de la Dimensión Gestión de incidentes .125
5.2. Procesamiento de datos de la Variable Gestión de Servicios de TI. 126
5.2.1. Procesamiento de datos de la Dimensión Personal y Organización 127
5.2.2. Procesamiento de datos de la Dimensión Información y Tecnología 128
5.2.3. Procesamiento de datos de la Dimensión Proveedores y Socios.129
5.2.4. Procesamiento de datos de la Dimensión Flujo de Valor 130
5.3. Prueba de hipótesis.....131
5.3.1. Prueba de hipótesis general.....131
5.3.2. Prueba de hipótesis especifica 1.....134
5.3.3. Prueba de hipótesis especifica 2.....135
5.3.4. Prueba de hipótesis especifica 3.....137
5.3.5. Prueba de hipótesis especifica 4.....139
CONCLUSIONES.....142
RECOMENDACIONES 144
REFERENCIAS BIBLIOGRÁFICAS.....145
ANEXOS 147

INDICE DE FIGURAS

Figura 1: Cortafuego 39
Figura 2: Honeynet.....40
Figura 3: Gestión de Servicios TI 40
Figura 4: Proceso de Gestión ITSM 44
Figura 5: Esquema.....47
Figura 6: UNU – Copias de seguridad.....59
Figura 7: UNU – Actividades de IP.....61
Figura 8: UNU – Actividades de IP Destino.....62
Figura 9: UNU – Actividades de IP Origen 62
Figura 10: UNU – Aplicaciones utilizadas 63
Figura 11: UNU – Niveles y permisos de internet.....65
Figura 12: UNU – Registro de proveedores 67
Figura 13: UNU – Flujo de actividades.....68
Figura 14: UNU – Registro de control de cuentas de acceso a dispositivos 71
Figura 15: UNU – Registro de control de acceso personal interno.....72
Figura 16: UNU – Registro backup.....73
Figura 17: UNU – Configuración proxy.....85
Figura 18: UNU – Registro de control de acceso a personal externo.....87
Figura 19: UNU – Registro de incidencias de copias de seguridad.....88
Figura 20: UNU – Registro de incidencias de equipos de telecomunicaciones88
Figura 21: UNIA – Sophos 91
Figura 22: UNIA – Respaldos.....93
Figura 23: UNIA – Firewall Internet 94
Figura 24: UNIA – Kaspersky.....95
Figura 25: UNIA – Firewall kaspersky 95
Figura 26: UNIA – Registro de proveedores 97
Figura 27: UNIA – Flujo de actividades.....100
Figura 28: UNIA – Registro de cuentas de acceso a dispositivos de comunicación 101
Figura 29: UNIA – Registro de control de acceso personal interno.....102
Figura 30: UNIA – Registro backup.....102
Figura 31: UNIA – Registro de control de acceso personal externo.....116
Figura 32: UNIA – Registro de incidencias de copias de seguridad.....117
Figura 33: UNIA – Registro de incidencias en equipos de telecomunicaciones 117
Figura 34: UNIA – Barras porcentuales de la Variable Seguridad Perimetral de TI.....118
Figura 35: UNIA – Barras porcentuales de la dimensión Políticas 119
Figura 36: UNIA – Barras porcentuales de la dimensión Aspectos Organizativos 120
Figura 37: UNIA – Barras porcentuales de la dimensión Aspectos Organizativos 121

Figura 38: UNIA – Barras porcentuales de la dimensión Seguridad en la Operación.....122
Figura 39: UNIA – Barras porcentuales de la dimensión Seguridad en las Telecomunicaciones 123
Figura 40: UNIA – Barras porcentuales de la dimensión Adquisición y Desarrollo 124
Figura 41: UNIA – Barras porcentuales de la dimensión Adquisición y Desarrollo 125
Figura 42: UNIA – Barras porcentuales de la Variable Gestión de Servicios de TI.....126
Figura 43: UNIA – Barras porcentuales de la dimensión Personal y Organización 127
Figura 44: UNIA – Barras porcentuales de la dimensión Información y Tecnología 128
Figura 45 UNIA – Barras porcentuales de la dimensión Proveedores y Socios 129
Figura 46: UNIA – Barras porcentuales de la dimensión Flujo de Valor.....130

INDICE DE TABLAS

Tabla N° 1: Operacionalización de variable I 28
Tabla N° 2: Operacionalización de variable II 30
Tabla N° 3: Población de estudio 48
Tabla N° 4: Población de estudio 49
Tabla N° 5: Personal de TI 51
Tabla N° 6: UNU- Servidor Web Dedicado.....56
Tabla N° 7: UNU - Hardware centro de datos 57
Tabla N° 8: UNU - Características control de acceso.....72
Tabla N° 9:UNIA - Personal de TI 89
Tabla N° 10: UNIA - Servidor 90
Tabla N° 11: UNIA – Hardware Centro de datos 90
Tabla N° 12: UNIA – Características del control de acceso. 102
Tabla N° 13: Distribución de frecuencia de la Variable Seguridad Perimetral .118
Tabla N° 14: Distribución de frecuencia de la dimensión dimensión Políticas 119
Tabla N° 15: Distribución de frecuencia de la dimensión Aspectos Organizativos 120
Tabla N° 16: Distribución de frecuencia de la dimensión Control de Accesos 121
Tabla N° 17: Distribución de frecuencia de la dimensión Seguridad en la Operación.....122
Tabla N° 18: Distribución de frecuencia de la dimensión Seguridad en las Telecomunicaciones 123
Tabla N° 19: Distribución de frecuencia de la dimensión Adquisición y Desarrollo 124
Tabla N° 20: Distribución de frecuencia de la dimensión Gestión de Incidentes 125
Tabla N° 21: Distribución de frecuencia de la Variable Gestión de Servicios de TI 126
Tabla N° 22: Distribución de frecuencia de la dimensión Personal y Organización 127
Tabla N° 23: Distribución de frecuencia de la dimensión Información y Tecnología 128
Tabla N° 24: Distribución de frecuencia de la dimensión Proveedores y Socios 129
Tabla N° 25: Distribución de frecuencia de la dimensión Flujo de Valor 130
Tabla N° 26: Prueba de normalidad de la prueba de hipótesis general 132
Tabla N° 27: Toma de decisión de la hipótesis general 133
Tabla N° 28 Prueba de correlación de Rho Spearman de la hipótesis general 133
Tabla N° 29: Prueba de normalidad de la prueba de hipótesis especifica 1 ...134
Tabla N° 30: Toma de decisión de la hipótesis especifica 1 134

Tabla N° 31 Prueba de correlación de Rho Spearman de la hipótesis especifica 1 135
Tabla N° 32: Prueba de normalidad de la prueba de hipótesis especifica 2 ...136
Tabla N° 33: Toma de decisión de la hipótesis especifica 2 136
Tabla N° 34 Prueba de correlación de Rho Spearman de la hipótesis especifica 2 137
Tabla N° 35: Prueba de normalidad de la prueba de hipótesis especifica 3 ...138
Tabla N° 36: Toma de decisión de la hipótesis especifica 3 138
Tabla N° 37 Prueba de correlación de Rho Spearman de la hipótesis especifica 3 139
Tabla N° 38: Prueba de normalidad de la prueba de hipótesis especifica 4 ...140
Tabla N° 39: Toma de decisión de la hipótesis especifica 4 140
Tabla N° 40 Prueba de correlación de Rho Spearman de la hipótesis especifica 4 141
Tabla N° 41: Reseña de recolección de datos 155
Tabla N° 42: Recolección de datos 156

INDICE DE ANEXOS

Anexos N° 1: Matriz de consistencia. 148
Anexos N° 2: Base de datos 148
Anexos N° 3: Cuestionario de preguntas para la recolección de datos.....155
Anexos N° 4: Validación de los instrumentos por expertos 159
Anexos N° 5: Evidencias en la Universidad Nacional de Ucayali 160
Anexos N° 6: Evidencias en la Universidad Nacional Intercultural de la Amazonia 161
Anexos N° 7: Constancias de ejecución de proyecto 162

RESUMEN

La principal ventaja de las organizaciones que cuentan con seguridad perimetral, es que tienen una barrera virtual que les permite protegerse ante los diferentes ataques. La seguridad perimetral se conforma de varios sistemas de defensa que son para detectar y prevenir la presencia de amenazas externas. Esto se puede lograr con la implementación de una serie de métodos, que nos alertan en el caso de que la seguridad esté siendo transgredida.

Todos estos métodos o herramientas van registrando todo lo que ocurre y se reporta el ataque para que se puedan ejecutar tareas de defensa del sistema.

En esta investigación se pretende identificar la relación de la SEGURIDAD PERIMETRAL INFORMÁTICA Y LA GESTION DE SERVICIOS DE TI EN LAS UNIVERSIDADES PÚBLICAS DE LA AMAZONÍA PERUANA, para lograrlo se tendrá que realizar una serie de visitas a la Universidad Nacional de Ucayali y a la Universidad Intercultural de la Amazonia Peruana.

Palabras clave: Seguridad, perímetro, servicios, gestión

ABSTRACT

The main advantage of organizations that have perimeter security is the virtual barrier that allows them to protect themselves against different attacks. Perimeter security is confirmed by several defense systems to detect and prevent the presence of external threats. This can be achieved by implementing a series of methods, which alert us in the event that security is being breached.

All these methods or tools record everything that happens and the attack is reported so that system defense tasks can be executed.

This research aims to identify the relationship between IT PERIMETER SECURITY AND IT SERVICES MANAGEMENT IN PUBLIC UNIVERSITIES OF THE PERUVIAN AMAZON. To achieve this, a series of visits will be made to the National University of Ucayali and the Intercultural University of the Peruvian Amazon.

Key words: Security, perimeter, services, management.

INTRODUCCIÓN

En la actualidad, debido a la gran evolución de las tecnologías, las computadoras son accesibles para cualquier persona. Asimismo, estos equipos no solo se interconectan entre computadoras dentro de un mismo espacio local, sino que también lo realizan a través del Internet, y con otros tipos de equipos como: los Teléfonos inteligentes, Tvs inteligentes, etc.

Las organizaciones hacen uso de los equipos informáticos interconectados para agilizar sus procesos y/o actividades el cual les proporciona, por una parte, la ventaja competitiva, y por otra la vulnerabilidad en la seguridad de su información; en tal sentido, es indispensable que se implementen controles a fin de garantizar que la información y los sistemas computacionales no sufran ataques ni accesos desde redes informáticas no confiables, que se encuentren fuera de su perímetro.

La presente investigación busca determinar en qué medida la Seguridad Perimetral Informática se relaciona con la Gestión de TI en la oficina de Informática de la Universidad Nacional de Ucayali y de la Universidad Nacional Intercultural de la Amazonia.

Se presenta a continuación la distribución de los capítulos correspondiente a la presente investigación.

En el **Capítulo I** – Planteamiento del problema, c**apítulo II** – Marco Teórico, **Capítulo III** - Hipótesis y Variables: Contiene la hipótesis general, hipótesis específicas y las variables, **Capítulo IV** – Metodología de la investigación: Contiene el tipo y nivel de investigación, método y diseño,

población, muestra, fuentes, técnicas e instrumentos de recolección de datos de la investigación, **Capítulo V** – Administración del proyecto de investigación: Contiene los recursos, presupuesto y cronograma de actividades.

Los anexos conteniendo: la matriz de identificación de problema instrumentos de recolección de datos.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN Y FUNDAMENTACIÓN DEL PROBLEMA

La tecnología avanza a pasos cada vez más acelerados, las organizaciones tienen la necesidad de conseguir e implementar tecnología para mejorar sus sistemas informáticos, procedimientos, actividades con el fin de asegurar y garantizar su funcionamiento de forma oportuna.

Estos mismos avances, en manos de personas inadecuadas, permite que se investigue y se crean formas de vulnerarlos, haciendo que los sistemas de información sean blanco de frecuentes ataques cibernéticos. Las organizaciones realizan muchos esfuerzos para invertir e implementar mecanismos de detección y control.

La seguridad perimetral es un método que permite la defensa de las redes informáticas, consiste en la instalación de equipos relacionados con las comunicaciones, a los cuales se les debe establecer políticas que garanticen la seguridad y su insuperable funcionamiento. (Marina, 2021).

La Universidad Nacional de Ucayali (UNU) y la Universidad Nacional Intercultural de la Amazonía (UNIA), cuentan con soluciones informáticas, como soporte de sus procesos y/o actividades, asimismo, como toda entidad, vienen implementado y/o mejorando su infraestructura tecnológica, tales como: la infraestructura de comunicaciones que son la base para los servicios web, sistemas de matrícula, sistemas de registro

de notas, correo electrónico, web service, acceso a internet, interconexión entre las oficinas administrativas, facultades, etc.

Por lo mencionado en el párrafo anterior, y por razones de seguridad, estas universidades están obligadas a implementar los controles adecuados para reducir el impacto del riesgo que podrían ser ocasionados por ataques externos como son: Ataque DoS, Ping Flood, Ping de muerte, escaneo de puertos, etc. Ataques internos como: Virus, Gusanos, Phishing, etc. Cada uno de estos posibles ataques son riesgos que, al materializarse, impactarían de forma negativa comprometiendo a cada uno de los procesos vinculados.

Ante esta posible situación de inseguridad, es necesario descubrir como la Seguridad Perimetral Informática implica en la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana: 2021

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema general

¿De qué manera la Seguridad Perimetral Informática se relaciona con la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana: 2021?

1.2.2. Problemas específicos

1. ¿Cómo la Seguridad Perimetral Informática se relaciona con el Personal y Organización de las Universidades Públicas de la Amazonía Peruana: 2021?
2. ¿En qué medida la Seguridad Perimetral Informática se relaciona con la Información y Tecnología en las Universidades Públicas de la Amazonía Peruana: 2021?

3. ¿De qué manera la Seguridad Perimetral Informática se relaciona con los Proveedores y Socios en las Universidades Públicas de la Amazonía Peruana: 2021?
4. ¿En qué medida la Seguridad Perimetral Informática se relaciona con el Flujo de valor y Procesos en las Universidades Públicas de la Amazonía Peruana: 2021?

1.3. OBJETIVOS

1.3.1. Objetivo general

Determinar en nivel de relación entre la Seguridad Perimetral Informática y la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana: 2021.

1.3.2. Objetivo específico

1. Identificar el nivel de relación entre la Seguridad Perimetral Informática con el Personal y la Organización en las Universidades Públicas de la Amazonía Peruana: 2021.
2. Establecer el nivel de relación entre la Seguridad Perimetral Informática y la Información y tecnología en las Universidades Públicas de la Amazonía Peruana: 2021.
3. Conocer el nivel de relación entre la Seguridad Perimetral Informática y los Proveedores y Socios en las Universidades Públicas de la Amazonía Peruana: 2021
4. Determinar el nivel relación entre la Seguridad Perimetral Informática y el Flujo de valor y Procesos en las Universidades Públicas de la Amazonía Peruana: 2021

1.4. JUSTIFICACIÓN, IMPORTANCIA Y LIMITACIONES

1.4.1. JUSTIFICACIÓN

Justificación teórica.

La presente investigación obtiene su justificación teórica, por el aporte de teorías a través de la validación de un instrumento que permita medir el nivel de Seguridad Perimetral Informática y la Gestión de Servicios de TI que será analizada y diseñada por un equipo conformado por los investigadores y el personal de TI de las Universidades Públicas de la Amazonia Peruana.

Justificación práctica.

La principal finalidad de esta investigación es descubrir la percepción de Seguridad Perimetral Informática, en el espacio referido a la Gestión de Servicios de TI en las Universidades Públicas de la Amazonia Peruana, los hallazgos, apoyan en la elaboración e implementación de proyectos que permiten alcanzar el estado recomendado.

Justificación metodológica.

La presente investigación forma parte de las líneas de investigación aprobadas en la Universidad Nacional de Ucayali, específicamente en la escuela profesional de Ingeniería de Sistemas, cumpliendo con los reglamentos establecidos, y de esta manera sentar la influencia de la Seguridad Perimetral Informática y la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana.

1.4.2. IMPORTANCIA.

La presente investigación sustenta su importancia, **Primero** por tratar un tema muy importante para las organizaciones, debido a

que en la actualidad toda o casi toda organización se encuentra conectado a la gran red de redes, y deben buscar estrategias para minimizar los riesgos de ataque externos y así no sufrir impactos negativos sobre su información. **Segundo**, presenta un gran aporte a la carrera de ingeniería de sistemas de nuestra universidad, debido a que es la primera en tratar sobre el tema de la Seguridad Perimetral, y así servirá como guía o referencia para futuras investigaciones. **Tercero**, presenta un aporte a la comunidad en el sentido que las Universidades deben garantizar la seguridad de la información del personal docente, estudiantes, administrativos, etc.

1.4.3. LIMITACIONES.

El acceso a la información de los sistemas de telecomunicaciones de las Universidades, por ser uno de los activos más importantes, y de no fácil acceso para externos.

1.5. HIPÓTESIS

1.5.1. Hipótesis General.

La Seguridad Perimetral Informática se relaciona con la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana: 2021.

1.5.2. Hipótesis Específica.

1. La Seguridad Perimetral Informática se relaciona con el Personal y Organización en las Universidades Públicas de la Amazonía Peruana: 2021.

2. La Seguridad Perimetral Informática se relaciona con la Información y tecnología en las Universidades Públicas de la Amazonía Peruana: 2021.
3. La Seguridad Perimetral Informática se relaciona con los Proveedores y Socios en las Universidades Públicas de la Amazonía Peruana: 2021.
4. La Seguridad Perimetral Informática se relaciona con el Flujo de valor y Procesos en las Universidades Públicas de la Amazonía Peruana: 2021.

1.6. DELIMITACIONES DE LA INVESTIGACIÓN

1.6.1. Delimitación Espacial.

Esta investigación se centra en evaluar la Seguridad Perimetral y la Gestión del Servicio las dos Universidades Públicas como son: La Universidad Nacional de Ucayali y La Universidad Intercultural de la Amazonia Peruana.

1.6.2. Delimitación Social.

En la presente investigación se encuentran relacionados los estudiantes de la Escuela Profesional de Ingeniería de Sistema de la Facultad de Ingeniería de Sistemas e Ingeniería Civil quienes, con su investigación, evalúan la Seguridad Perimetral involucrando al personal de TI de cada Universidad.

1.6.3. Delimitación Temporal.

Esta investigación cumple con los requisitos de tiempo propuestos por la Oficina de Grados y Títulos de la FISeIC.

1.6.4. Delimitación Conceptual.

Esta investigación hace uso de teorías, conceptos relacionados a la carrera de Ingeniería de sistemas, asimismo, toma como referencia información de bibliografías, revistas, información WEB.

1.7. VARIABLES

1.7.1. Variable independiente:

Seguridad Perimetral de TI (Enetic, 2021)

Es el aseguramiento de la infraestructura tecnológica de las organizaciones, fortifica los accesos, implementando un entorno de soluciones integradas para la detección y gestión de amenazas, desplegando una vigilancia activa que previene las intrusiones e infecciones.

1.7.2. Variable dependiente:

Gestión de Servicios de TI. (Alvarado, 2019).

Las dimensiones de Gestión de Servicios de TI, son: 1. Personal y Organización, 2. Información y tecnología, 3. Proveedores y Socios, 4. Flujo de valor y Procesos.

1.7.3. Variable interviniente:

Oficina General de Tecnología de la Información, Sistemas y Estadística en las Universidades Públicas de la Amazonía Peruana: 2021.

1.8. SISTEMA DE VARIABLES, DIMENSIONES E INDICADORES.

Variable: Seguridad Perimetral

Tabla N° 1: Operacionalización de variable I

Dimensión	Indicadores	Preguntas	Escala valorativa	Instrumento
Políticas	Documentos	1. La OGTISE cuenta con políticas de seguridad perimetral.	1.-Muy malo 2.-Malo 3.-Regular 4.-Bueno 5.-Muy bueno	Cuestionario
	Difusión	2. La OGTISE realiza reuniones de difusión de las políticas y/o procedimientos sobre seguridad perimetral.		
Aspectos Organizativos de la Seguridad de la Información	Comité de Gestión de Seguridad	3. La Universidad brinda las posibilidades necesarias para iniciar y controlar la implementación de políticas de seguridad.		
	Coordinaciones	4. Las responsabilidades del personal OGTISE, con respecto a la seguridad perimetral están definidas de forma clara y precisa.		
Control de accesos	Identificación y control de usuarios	5. Las OGTISE lleva el registro de acceso como parte de la seguridad perimetral.		
	Gestión de claves de acceso	6. Las OGTISE gestiona las claves de acceso como parte de la seguridad perimetral (Registros).		
	Sistemas biométricos	7. Las OGTISE hace uso de los sistemas biométricos de acceso a las instalaciones que deben estar aseguradas como la sala de servidores, gabinetes como parte de la seguridad perimetral.		
	Registros de acceso al personal y terceros	8. Las OGTISE lleva el registro de los accesos del personal interno a las instalaciones que salvaguardan los activos más importantes de TI.		
Seguridad en la Operación	Respaldo de información y contingencia	9. Las OGTISE realiza respaldo de la información de base de datos 10. Las OGTISE realiza registro de los respaldos de las bases de datos. 11. Las OGTISE gestiona los sistemas de contingencia a nivel físico y lógico de los sistemas.		
Seguridad en las Telecomunicaciones	Internet, intranet y extranet	12. La Universidad posee acceso a internet con respaldo 13. La Universidad cuenta con Intranet 14. La Universidad cuenta con extranet	1.-Muy malo 2.-Malo 3.-Regular 4.-Bueno	

	Sistemas de detección y/o prevención de intrusos (IDS/IPS)	15. Se realizan verificaciones de IP entrantes salientes y de aplicaciones 16. La frecuencia monitorización de tráfico en la LAN es 17. La frecuencia monitorización de tráfico en la red Wireless es.. 18. La cantidad de implementaciones de pasarelas antivirus y antispan es. 19. El nivel de detección y bloqueo de SPAM es. 20. El nivel de testeo basado en DNS, DNS Block list.	5.-Muy bueno
	Pasarelas antivirus y antispam	21. La cantidad de implementaciones de pasarelas antivirus y antispan 22. El nivel de detección y bloqueo de SPAM. 23. El nivel de testeo basado en DNS, DNS Block list.	
Adquisición, desarrollo y mantenimiento de los sistemas de información	Participación	24. La OGTISE forma parte del comité de evaluación y adquisiciones de soluciones relacionados a la seguridad perimetral.	
	Registro	25. La OGTISE registra los datos de personal externo que ingresa a las instalaciones para el trabajo de mantenimiento de las soluciones de TI.	1.-Muy malo 2.-Malo 3.-Regular 4.-Bueno 5.-Muy bueno
Gestión de incidentes en la seguridad de la información	Registro	26. Las OGTISE lleva el registro de incidencias de copias de seguridad de datos y aplicaciones. 27. Las OGTISE lleva el registro de incidencias en las telecomunicaciones, clasificados por tipo o medio.	

Variable: Gestión de Servicios de TI

Tabla N° 2: Operacionalización de variable II

Dimensión	Indicadores	Preguntas	Escala valorativa	Instrumento
Personal y Organización	Cultura Organizacional	28. Se tiene definido la cultura organización a nivel de la OGTISE.	1.-Muy malo 2.-Malo 3.-Regular 4.-Bueno 5.-Muy bueno	Cuestionario
Información y tecnología	Hardware	29. La OGTISE cuenta con servidores adecuados para la necesidad de la Universidad 30. La OGTISE cuenta con sistemas de almacenamiento adecuando para necesidad de la Universidad.		
Proveedores y Socios	Registro	31. La OGTISE cuenta con la cantidad de proveedores de TI de acuerdo a sus necesidades. 32. La OGTISE cuenta con una base de datos de proveedores de TI.		
Flujo de valor y Procesos	Registro	33. La OGTISE cuenta con interconexiones estrategias con otras Instituciones 34. La OGTISE cuenta con flujos de trabajo aprobados		

CAPITULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DEL PROBLEMA

(MARCEL, 2017). “DISEÑO DE UN SISTEMA DE SEGURIDAD PERIMETRAL EN LAS INSTALACIONES DEL CONSORCIO EXPANSION PTAR SALITRE, SEDE BOGOTÁ D.C”, con el objetivo: Proponer un sistema de seguridad perimetral con características de protección en la infraestructura física y lógica de las instalaciones del consorcio, PTAR salitre, llegando a las siguientes conclusiones: Realizar la implementación de un sistema de seguridad perimetral por anillos, permitirá al Consorcio Expansión PTAR Salitre, ir generando la puesta en marcha de cada uno de ellos a medida que se quieran ir ejecutando. Generar el aseguramiento de la capa de red, tomando en cuenta el modelo OSI, ampliara el aseguramiento de la información que se maneja en el consorcio, ya que esta brindara el primer bloque de seguridad. Manejar la información por roles y perfiles de acceso, y asegurar las aplicaciones que se manejan en el consorcio, brindará un control más amplio en el uso cotidiano de la información, y el personal de tecnología tendrá a capacidad de encontrar cualquier brecha adicional. Asegurar la periferia de la edificación, apoyara la gestión realizada por el personal de seguridad, tanto físico, como el del personal de tecnología encargado de asegurar la información. El presente trabajo tomo como punto de partida los planos arquitectónicos avalados para la construcción de la edificación, esto permitirá que, desde el inicio de la obra, se de apertura al aseguramiento.

(GARCIA, 2016). “ESTUDIO DE LAS TECNOLOGIAS DE SEGURIDAD PERIMETRAL INFORMÁTICAS Y PROPUESTA DE UN PLAN DE IMPLEMENTACIÓN PARA LA AGENCIA NACIONAL DE TRÁNSITO", con el objetivo de: Analizar las principales tecnologías de seguridad perimetral informática y propuesta de un plan de implementación para la Agencia Nacional de Tránsito, tomando en cuenta las características técnicas y económicas, llegando a las siguientes conclusiones: Se identificó que la infraestructura tecnológica de la Agencia Nacional de Tránsito presenta vulnerabilidades y existen falencias en torno a la transferencia de información entre sucursales ya que no se utiliza ninguna herramienta de encriptación que permita dar confidencialidad a la información. La red de ANT posee mecanismos de seguridad como el software antivirus Kaspersky y el dispositivo Astaro Security Gateway (punto único de protección y de falla), los mismos que constituyen una herramienta muy fuerte para la protección de la red, pero que no permiten ejercer controles. La mayoría de los ataques de suplantación de identidad y programas maliciosos se llevan a cabo a través de Internet, al restringir el acceso a determinados sitios web utilizando tecnología de filtrado de direcciones o contenido web permite que las empresas puedan reducir los riesgos de que los usuarios se conviertan en víctimas de estos ataques. El establecimiento de Redes Privadas Virtuales basadas en protocolos de tunelización (IPSec SSL, PPTP y L2TP) permite que oficinas pequeñas puedan establecer comunicaciones privadas sobre redes públicas garantizando la confidencialidad e integridad de los datos trasmitidos por Internet. Utilizar técnicas de autenticación a través de políticas de Firewall

(Interfaces de entrada y salida, direcciones IP origen y destino, protocolo, servicio o puertos TCP/UDP) permitirán llevar un mejor control del tráfico que circula por nuestra red. Contar con sistema de seguridad que maneje un esquema de alta disponibilidad permitirá que la Agencia Nacional de Tránsito cuente siempre con las aplicaciones que apoyan sus operaciones principales, pues la falta de disponibilidad de las mismas puede repercutir en costos, tiempos, esfuerzos y por supuesto en la confianza e insatisfacción de los usuarios.

Una adecuada gestión de calidad de servicio nos permitirá la utilización de aplicaciones susceptibles a retardos (voz y aplicaciones multimedia) sin recurrir a una ampliación innecesaria del ancho de banda, reservando el ancho de banda necesario y priorizando este tipo de tráfico ante otros menos sensibles al retardo como pueda ser el correo o el tráfico ftp.

(BOLAÑOS BOTINA, 2018). “DISEÑO DE LA ARQUITECTURA DE SEGURIDAD PERIMETRAL DE LA RED INFORMATICA EN LA INDUSTRIA DE LICORES DEL VALLE”, con el objetivo: Diseñar una arquitectura de seguridad perimetral de la red de informática de la ILV (Industria de Licores del Valle) que permita optimizar el esquema de seguridad y privacidad de la información, garantizando la protección de sus activos, llegando a la conclusión de: Como la más importante conclusión, se debe resaltar la importancia de darle continuidad a este trabajo, estableciendo las políticas de control de riesgo, enmarcadas dentro del Modelo de Seguridad y Privacidad de la Información [MSPI] en su fase de implementación, que le permitirá a la Industria de Licores del

Valle ILV, el desarrollo, la implantación y la puesta en marcha del diseño y la planificación de la arquitectura de seguridad perimetral propuesto. Una conclusión complementaria y no menos importante, es considerar las graves consecuencias de la no implementación de una estrategia operativa, representada en la arquitectura de seguridad perimetral, enmarcada dentro del plan de seguridad y privacidad de la información en la organización objeto de estudio que evite la exposición integral de sus activos de información, a las evidentes vulnerabilidades de su infraestructura de red informática. La etapa subsiguiente de implementación de la arquitectura de seguridad perimetral propuesta, consiste en establecer políticas de seguridad y documentarlas con el fin de gestionar el plan de riesgos identificado. Estas políticas y su debida documentación, permitirán definir los comportamientos aceptables, la selección de las herramientas y los procedimientos necesarios, y definirán una serie de responsabilidades divulgando a las unidades responsables, la manera correcta de cómo responder ante la aparición de incidencias de seguridad, entre otras tareas, evitando así las vulnerabilidades asociadas a las políticas. Todos los proyectos orientados a la seguridad de la información corporativa deberían empezar con el mismo paso, determinar cuál es la información sensible, descubrir dónde está alojada además del centro de datos, si está diseminada en computadoras de escritorio, dispositivos móviles y en la nube; y revisar cómo y quién accede a ella. Tras identificar la información sensible, se debe determinar cómo se utiliza, quién accede a ella, quién la utiliza, quién la crea, dónde se envía, y así identificar los procesos del negocio en los cuales participan estos

datos, para poder asegurarlos y plasmarlos en políticas corporativas, e incluir algunos casos de excepción que sean necesarios como en el caso de los socios de negocios.

(RUIZ VIEIRA, 2018). “IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL OPEN SOURCE EN LA RED TELEMÁTICA DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO”, con el objetivo: Incrementar la seguridad de los servicios académicos en la red telemática de la Universidad Nacional Pedro Ruiz Gallo, llegando a la conclusión de: El objetivo de esta tesis fue incrementar significativamente la seguridad de base de datos y aplicaciones en la red telemática de la Universidad Nacional Pedro Ruiz Gallo, implementando un firewall basado en FreeBSD (pfSense), habiéndose cumplido el objetivo general y luego de hacer análisis y comparaciones entre los antecedentes encontrados, los resultados son los siguientes: Se pudo encontrar la existencia de ataques a cada uno de los 7 servicios que la red telemática de la UNPRG ofrece. Se detectaron vulnerabilidades con un promedio de 113 por servicio siendo el mayor acceso no deseado al “SISTEMA ACADÉMICO” con 287 y el menor “SIGA” con 10. Se implementó y configuró el sistema pfSense para la gestión de la seguridad perimetral tal como consta en el Acta de Instalación. Después de la instalación y puesta en producción el firewall pfSense se pudo detectar un significativo descenso de las vulnerabilidades en la red siendo un promedio de 5.14 y el servicio de “SISTEMA ACADEMICO” con 10 y el menor “SIGA” con 1. Con esto podemos afirmar que la implementación del firewall pfSense aumentó la

seguridad perimetral dentro de la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

(Humberto, 2019). “Implementación de un modelo de seguridad perimetral para la Comisión Nacional para el Desarrollo y Vida sin Drogas”, En el presente proyecto está desarrollado para lograr la implementación de una solución de seguridad perimetral segmentada para la Comisión Nacional para el Desarrollo y Vida sin Drogas. En el primer capítulo se expondrán los aspectos generales del proyecto, que incluyen el árbol de problemas, que será el punto de inicio para la identificaron de los problemas específicos que adolece la organización dentro las cuales están principalmente las deficiencias existentes en el consumo del ancho de banda y las constantes interrupciones de la red LAN. Luego se establecerán los objetivos del presente proyecto que básicamente son el planteamiento de la solución a desarrollar. Dentro de este capítulo también se mencionará los alcances que son básicamente la implementación de zonas de red, establecer políticas de control de seguridad y control del tráfico y finalmente establecer un modelo jerárquico y VLANS. En esta capitulo también se menciona los alcances del proyecto que establece hasta dónde llega el proyecto y sus limitaciones. En el segundo capítulo del proyecto está referido al marco teórico donde se establecen las tesis de referencia que se emplearon como una guía de referencia y serán la base del presente proyecto. También dentro del segundo capítulo encontraremos el marco conceptual que es la definición de los términos empleados dentro del proyecto.

Finalmente se incluyó la normativa empleada como base legal que es la ISO/IEC 27001. En el tercer capítulo del proyecto se establecerá el marco metodológico que se empleara para el desarrollo de la solución propuesta, para la cual se ha utilizado la metodología de CISCO denominado TOP DOWN NETWORK, cuyo objetivo es hacer un proyecto manejable que se divide en cuatro módulos o fases que son: el análisis del requerimiento, el diseño lógico, el diseño físico, y las pruebas de optimización. También encontramos dentro del tercer capítulo como se va desarrollando la implementación del proyecto etapa por etapa bajo la metodología establecida. Luego se mencionarán los resultados obtenidos luego del desarrollo de la implementación del proyecto, resultados que deberán satisfacer los requerimientos iniciales es decir la solución a sus problemas identificados. Finalmente se mencionarán las conclusiones basadas en los resultados obtenidos dentro la implementación de un modelo basado en zonas para la Comisión Nacional para el Desarrollo y Vida sin Drogas.

2.2. BASES TEÓRICAS

¿Qué es la seguridad perimetral? (Unir, 2020)

Viene a ser la agrupación de componentes y métodos relacionados con el control para el acceso físico de los individuos a las infraestructuras, también es la identificación y la prevención de intromisiones. Para que se implementen tiene mucho que ver la forma y cultura de cada organización y los requisitos del mismo.

Objetivos de seguridad perimetral (Rubi, 2019)**.**

Establecer la primera línea de defensa contra los accesos externos no autorizados a los sistemas informáticos de la empresa. Se enfoca en:

- Admitir y/o rechazar enlaces.
- Limitar el tráfico de red
- Disminuir el tráfico de red producido por los equipos
- Proveer un punto único de acceso con el o los servidores
- Gestionar tráfico entre la red interna y la red externa.

Herramientas de seguridad perimetral informática (Accensit_admin, 2017)**.**

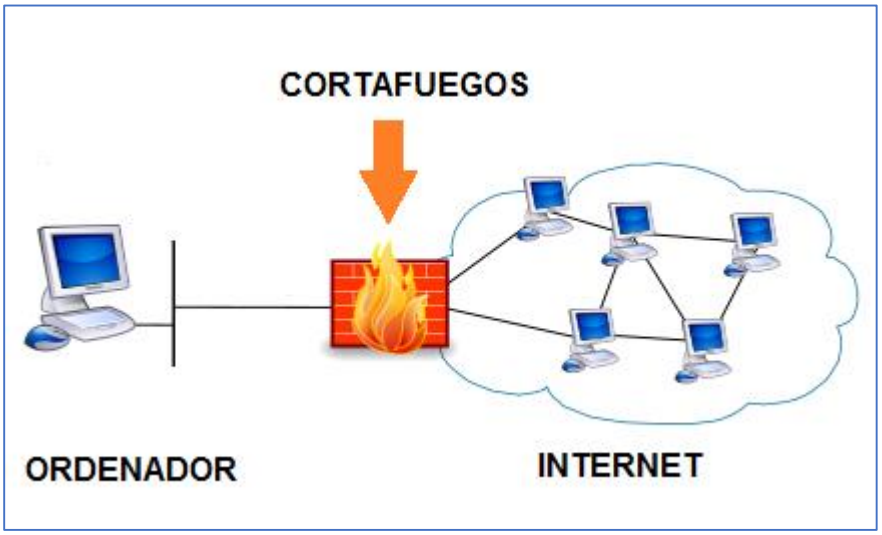
En el campo de la informática se pueden encontrar varias formas de instaurar una seguridad perimetral, como, por ejemplo:

- **Cortafuegos:** Permite definir, a través de políticas de accesos, qué tipo de tráfico se admite o se restringe en la red.

  Tipos:

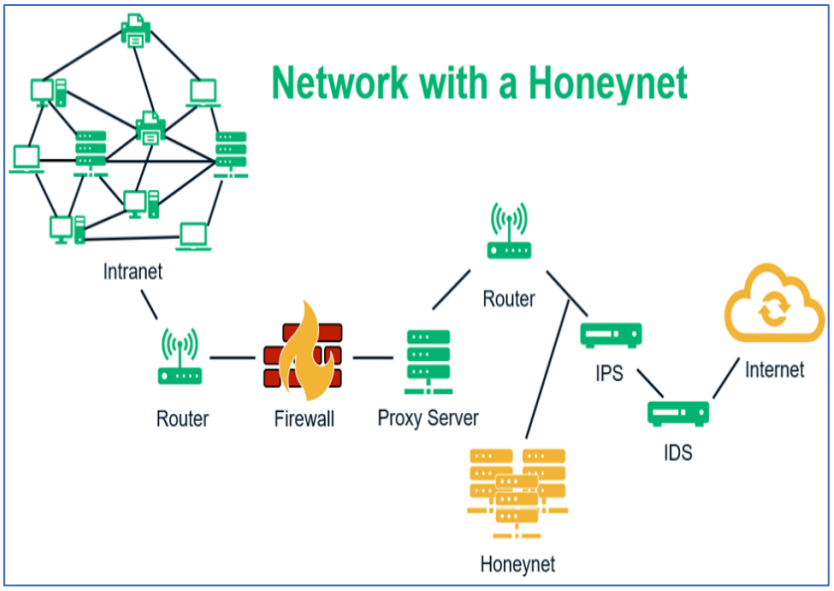
  – A nivel de pasarela: para aplicaciones específicas.
  – Configurados en la capa de red: filtra por IP origen/destino.
  – Para la capa de aplicación: Filtran según el protocolo.
  – Personal: Utilizados en los equipos personales como PC o móviles.

Figura 1: Cortafuego



- **Sistemas de Detección y Prevención de Intrusos**: Son dispositivos que monitorizan y generan alarmas cuando hay alertas de seguridad. Su actuación sigue estos pasos:
  - Identificación y detección de un probable ataque.
  - Registrar logs.
  - Bloqueo del ataque.
  - Informar a los administradores y a los sistemas de seguridad.
- **Honeypots:** Denominados como “sistema trampa” o “señuelo”, se configuran en una red con el objetivo de evitar posibles ataques al sistema. Su objetivo es identificar y obtener información sobre el ataque informático, cual es su procedencia procede, con la finalidad de que se tomen las medidas de seguridad necesarias.

Figura 2: Honeynet



Gestión de servicios de TI (ITSM). (Bailon, 2019)

La Gestión de servicios de TI consiste en organizar la entrega de servicios de TI con las necesidades organizacionales. Su forma completa es la gestión de servicios de TI. El enfoque de las herramientas tiene como finalidad de proporcionar un servicio grato a los usuarios finales.

Es la composición de un grupo de políticas, procesos, actividades y métodos precisos para conceder productos y servicios de TI. Busca mejorar, así como admitir servicios de TI centrados en el cliente.

Figura 3: Gestión de Servicios TI



Beneficios. (ServiceDesk, 2020)

Sin tomar en cuenta el tamaño de la organización, cada una está envuelta en la gestión de servicios de TI de una u otra forma. ITSM garantiza que se gestionen de forma simplificada las incidencias, los requerimientos de servicio, los problemas, los cambios y los activos de TI, además como otros relacionados con los servicios de TI.

El personal de TI en una organización puede emplear distintos flujos de trabajo y las mejores prácticas en ITSM, como se describe en ITIL.

Los procesos de ITSM pueden proporcionar efectos positivos en la función general de una organización de TI.

A continuación, se presenta los 10 beneficios clave de ITSM:

- Disminución de los costos de las operaciones de TI.
- Mayores retornos de las inversiones en TI.
- Mínima cantidad de Interrupciones del servicio.
- Capacidad para configurar procesos de TI correctamente definidos, que sean repetibles y adaptables.
- Promover un análisis eficiente de los problemas de TI con la finalidad de reducir la reproducción de incidentes.
- Mayor eficiencia del personal de la mesa de ayuda de TI.
- Roles y responsabilidades correctamente definidos.
- Expectativas claras sobre los niveles de servicio y la disponibilidad del servicio.
- Implementación de cambios de TI con el minino o nada de riesgos.
- Mayor transparencia en los procesos y servicios de TI.

Procesos de gestión de ITSM. (Motadata, 2020)

Los procesos de ITSM se clásica y componen de 05 etapas efectivas que el personal de TI puede hacer uso de una combinación de flujos de trabajo y las mejores prácticas involucradas en ITSM.

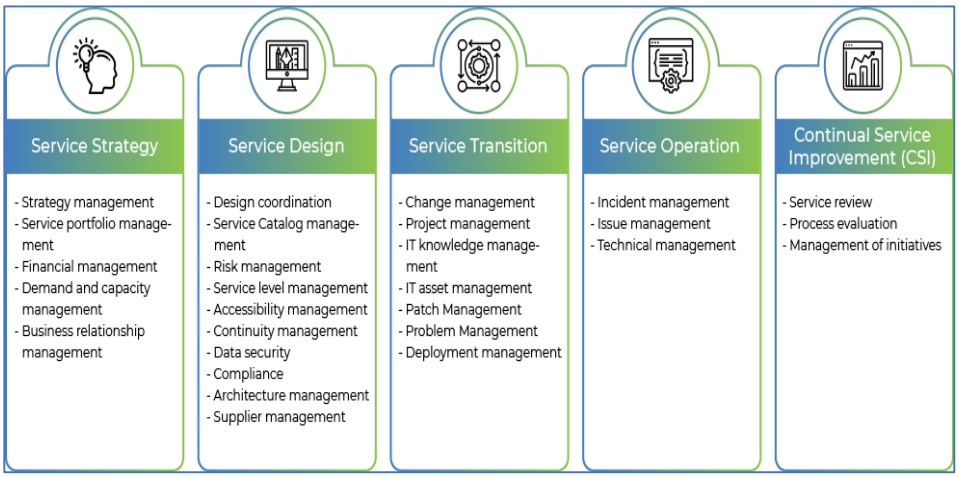
1. **Estrategia de servicio:** Se configuran y definen los servicios que proporciona la organización. Planifica estrategias de los procesos y la construcción de activos. Cuenta con los siguientes elementos:
    - Gestión de estrategia.
    - Gestión de cartera de servicio.
    - Gestión financiera.
    - Gestión de demanda y capacidad.
    - Gestión de relaciones comerciales.
2. **Diseño de servicio**: Se planifican y diseñan los servicios de TI que ofrece la organización, aplicados para satisfacer los requerimientos. Mejoran los servicios que se encuentran en proceso y se diseñan otros nuevos. A continuación, se muestran algunos componentes:
    - Coordinación de diseño.
    - Gestión del catálogo de servicios.
    - Gestión de riesgos.
    - Gestión de nivel de servicio.
    - Gestión de accesibilidad.
    - Gestión de continuidad.
    - Seguridad de datos.
    - Cumplimiento.

- Gestión de arquitectura.
- Administración de suministros.

3. **Transición de servicio.** Permite asegurar que los procesos respondan de la forma como fueron diseñados. En este punto la gestión de cambios, la evaluación y el manejo de riesgos están en escena. Posee los siguientes componentes:
   - Gestión del cambio.
   - Gestión del conocimiento de TI.
   - Gestión de activos de TI.
   - Gestión de despliegue.
   - Manejo de parches.
   - Manejo de parches.
4. **Operación de servicio.** Se implementan los diseños. Se debe monitorear los procesos con el fin de enfrentar problemas. Aquí algunos de sus componentes:
   - Administración de incidentes.
   - Gestión de problemas.
   - Manejo técnico.
5. **Mejora continua del servicio.** En esta etapa los KPIs y las métricas desempeñan una gran importancia para identificar áreas que requieran mejorar o transformarse.
   - Revisión de servicio.
   - Evaluación de proceso.
   - Gestión de iniciativas

.

Figura 4: Proceso de Gestión ITSM



2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS

Eficiencia: (Gestion, 2021)**.** Viene a ser la relación entre los recursos empleados en un proyecto y los logros obtenidos. Se produce en la utilización de menos recursos al alcanzar el miso objetivo o cuando se obtienen mayor cantidad de objetivos con cantidades iguales o con menos recursos.

Eficacia. (Eude, 2019)**.** Involucra el nivel del logro de metas y objetivos, hace referencia a la capacidad que tienen las personas para obtener o alcanzar lo que se proponen, independientemente del número de recursos empleados.

Gestión. (Huergo, 2019)**.** Es una acción integral, entendida como un proceso de trabajo y organización en el que se coordinan diferentes miradas, perspectivas y esfuerzos, para avanzar eficazmente hacia objetivos asumidos institucionalmente y que desearíamos que fueran adoptados de manera participativa y democrática.

KPIs. (Eserp, 2020)**.** Son indicadores clave de rendimiento utilizados para evaluar el éxito de las acciones y/o procesos aplicados para alcanzar los objetivos, permite determinar si está obteniendo lo esperado o será necesario aplicar correcciones.

Seguridad. (INSPQ, 2021)**.** Es un estado donde los peligros y las condiciones que pueden provocar daños son controlados para reducir su impacto.

Servicio. (DELSOL, 2019)**.** Es la prestación que satisface alguna necesidad humana y que no consiste en la producción de bienes materiales.

Tecnología. (UNL, 2021)**.** La tecnología no es una cosa sino un proceso, una capacidad de transformar o combinar algo ya existente para construir algo nuevo o bien darle otra función.

CAPITULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. METOGOLOGÍA Y TÉCNICAS UTILIZADAS.

3.1.1. Tipo de investigación.

(Rodríguez, 2020) . Investigación básica o fundamental, de acuerdo con el propósito de la investigación, no se busca la aplicación práctica de los descubrimientos, sino más bien la ampliación de los conocimientos para responder interrogantes o aplicarlos en investigaciones futuras.

3.1.2. Nivel de investigación.

(Nicomedes, 2017). La investigación descriptiva se encarga de puntualizar las características de la población que está estudiando. Esta metodología se centra más en el “qué”, en lugar del “por qué” del sujeto de investigación.

3.1.3. Método de investigación.

Método deductivo.

(GOMEZ, 2004). El método deductivo viene a ser las reglas y procesos en su totalidad, que nos permite deducir las conclusiones finales desde los enunciados denominados premisas si de una hipótesis se sigue una consecuencia y esa hipótesis se da, entonces, necesariamente, se da la consecuencia.

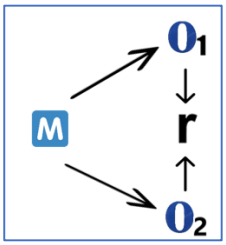
Método cuantitativo.

(Salas & Héctor, 2011). Los métodos cuantitativos, metodologías cuantitativas o investigaciones cuantitativas son el conjunto de estrategias de obtención y procesamiento de información que emplean magnitudes numéricas y técnicas formales y/o estadísticas para llevar a cabo su análisis, siempre enmarcados en una relación de causa y efecto.

3.1.4. Diseño de la investigación

(Hernandez, 2001). **Investigación correlacional** que es un tipo de investigación no experimental en el cual un investigador mide dos variables. Entiende y evalúa la relación estadística entre ellas sin influencia de ninguna variable extraña.

Esquema



Dónde:

Figura 5: Esquema

Icono	Significado
M	Muestra
O1	Seguridad Perimetral
O2	Gestión de Servicios de TI
r	Relación entre variables

3.2. POBLACIÓN Y MUESTRA DE LA INVESTIGACIÓN

3.2.1. Población

La población de estudio está conformada por el personal administrativo, personal docente y estudiantes, como se puede ver en la siguiente tabla.

Tabla N° 3: Población de estudio

Lugar	Estratos	Cantidad
UNU	Estudiantes	5439
	Docentes	254
	Administrativos	183
UNIA	Estudiantes	2155
	Docentes	90
	Administrativos	100
	TOTAL	**8221**

3.2.2. Muestra

Para obtener el tamaño de la muestra se empleó el método no probabilístico, con muestra intencionada que es aquella que el "investigador selecciona según su propio criterio sin ninguna regla matemática o estadística" (Carrasco Díaz, 2010, pág. 243)

Durante el periodo del año 2021, como efecto de la pandemia se propuso el trabajo remoto en las universidades públicas, por ello el acceso y contacto con el número de estudiantes, docentes y administrativos era muy limitado, dificultando contar con el número de muestra establecido en el método probabilístico. Bajo este criterio se optó por emplear el método no probabilístico considerando que el muestreo estará conformado de acuerdo a la muestra por cuotas.

Tabla N° 4: Población de estudio

Lugar	Estratos	Cantidad
UNU	Estudiantes	100
	Docentes	4
	Administrativos	3
UNIA	Estudiantes	73
	Docentes	4
	Administrativos	3
	TOTAL	**187**

3.3. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Instrumentos de recolección de datos

Como instrumento de recolección de datos se usó el cuestionario que está conformado por 02 partes: La primera de preguntas generales y la segunda de preguntas relacionada con las 02 variables de estudio como son: La Seguridad Perimetral y la Gestión de servicios de TI. Este instrumento posee un total de 34 preguntas (ver en el anexo 2).

3.4. PROCEDIMIENTO DE RECOLECCIÓN DE DATOS

La recolección de los datos se realizó de forma presencial y de forma virtual a través de formularios WEB, que fueron remitidos al personal de OGTISE para su llenado.

3.5. TRATAMIENTO DE DATOS.

El tratamiento se efectuó a través de la herramienta IBM SPSS Stadistics versión 26.

Para medir el grado de confiabilidad de los datos se utilizó el Alfa de Cronbach.

CAPITULO IV

SEGURIDAD PERIMETRAL

4.1. UNIVERSIDAD NACIONAL DE UCAYALI

4.1.1. INSTITUCIÓN

La Universidad Nacional de Ucayali conforma una de las más importantes universidades del Perú, se encuentra ubicada en la ciudad de Pucallpa en el departamento de Ucayali. Su creación fue a través del decreto Ley N.º 22804 con fecha del 18/12/1979.

4.1.2. HISTORIA.

En el año de 1981, el Congreso de la república del Perú le otorgó la legalización / ratificación de la creación por Ley No. 23261 de la Universidad Nacional de Ucayali, dos años posteriores, en 1983 se cambió a su designación como actualmente se la conoce: con la Ley No. 23733.3 las carreras iniciales fueron: agronomía, enfermería e ingeniería forestal. En el año 2016 se contaban con 8 facultades y sus 18 carreras profesionales convirtiéndose en una de las universidades con representaciones que muestran sostenibilidad para el desarrollo a nivel científico como tecnológico.

4.1.3. DESCRIPCIÓN ACTUAL DE LA ARQUITECTURA

- **Personal de TI.**

Tabla N° 5: Personal de TI

Área	Cargo	Nombres y Apellidos	Grado de Estudio	Funciones
Dirección de la Oficina General de Tecnología de la Información, Sistemas y Estadística	Director de la Oficina General de Tecnología de la Información, Sistemas y Estadística			Diseñar planear y ejecutar los sistemas de acuerdo a las necesidades de las dependencias y supervisar el trabajo en el desarrollo de las aplicaciones. Conducir estudios de factibilidad e investigaciones recomendando cursos de acción. Controlar la estructura de la documentación de los sistemas informáticos que utiliza la UNU, estableciendo los mecanismos adecuados de control y seguridad para cada uno de ellos. Investigar la utilización del potencial de computadores y formular planes de trabajo para el desarrollo de sistemas. Evaluar el Hardware y Software y otros mecanismos similares y preparar los estimados de tiempo y costos para el trabajo de desarrollo de sistemas. Planear la disponibilidad de recursos en la cantidad adecuada, a fin de cumplir los requerimientos los requerimientos de los proyectos de desarrollo de sistemas. Asesorar en asuntos de su especialidad. Otras que le asigne su jefe inmediato superior de acuerdo a la naturaleza de sus funciones.
Oficina ejecutiva de Estadística	Jefe de la Oficina Ejecutiva de Estadística	Secretaria de la Oficina General de Tecnología de la Información, Sistemas y Estadística Margarita Tang de Hidalgo	Ingeniero de Sistemas Secretaria	Oficina ejecutiva de desarrollo de software. Centro de cómputo y soporte técnico. Desarrollar plataformas para optimizar los procesos informáticos de la UNU. Prestar soporte técnico a todas las dependencias, mantenimiento preventivo y reparaciones. Administrar redes corporativas y los equipos de telecomunicaciones. Administrar el registro de recursos informáticos. Supervisión de unidades de procesamiento de datos de las diferentes Facultades para descentralizar el sistema. Otras labores inherentes de acuerdo a su naturaleza. Atención al público en general Gestión de la agenda de Dirección Gestión de documentos Organización de la Oficina Manejo de información sensible (interna y externa) Vigilancia Administrativa Elaboración de presentaciones Organización de desplazamientos La comunicación entre otras áreas y/o oficinas Proponer anualmente la metodología para la construcción de indicadores de desempeño, así como coordinar y brindar asesoría en el proceso de llenado de los formatos de los indicadores de desempeño
		Miguel Ángel Torres Pizarro	Economista	

Oficina ejecutiva de Desarrollo de Software			Recolectar, integrar, procesar, analizar y sistematizar la información estadística por programa educativo (PE), dependencia de educación superior (DES), área académica, región y a nivel Institucional con el propósito de generar información y alimentar la base de datos del Sistema de Información para la Planeación institucional, con base en la información que proporcione cada entidad académica o dependencia responsable de la misma Elaborar documentos, informes, reportes, etc., para responder a los requerimientos de información que formulan diversos usuarios internos y externos, al mismo tiempo de difundir a la comunidad universitaria los indicadores por programa educativo (PE), dependencia de educación superior (DES), área académica, región y a nivel Institucional Contribuir en todas aquellas actividades contempladas en la Legislación Universitaria para el logro de los objetivos de la Dirección de Planeación Institucional y del Plan General de Desarrollo de la Universidad Veracruzana
Analista de la Oficina Ejecutiva de Encargado de la Oficina Ejecutiva de Desarrollo de Software Desarrollo de Software	Luis Alfredo Huarcaya Villalobos	Bachiller en Ingeniería de Sistemas	Instalar y mantener aplicaciones clave para el negocio y solucionar problemas. Esto incluye servidores de aplicaciones, hardware asociado, dispositivos conectados, y bases de datos Reunirse y coordinar con los interesados internos y externos, para establecer el alcance del proyecto, los objetivos del sistema y los requerimientos Desarrollar, analizar, establecer prioridades y organizar las especificaciones de requerimientos, mapeo de los datos, diagramas y gráficas de flujo a seguir por desarrolladores y probadores Traducir especificaciones altamente técnicas a requerimientos claros y no técnicos Dirigir la puesta a punto y configuración de los sistemas
	Darwin Oliver Ramos Zapata	Ingeniero de Sistemas	Organizar y gestionar el área de desarrollo de sistemas informáticos de la institución, procurando un uso óptimo y eficiente de los recursos tecnológicos y humanos mediante definición de estándares y metodologías de trabajo apropiadas Responsable de la construcción de una plataforma de sistemas informáticos institucionales robusta, homogénea, integrada, documentada y escalable Crear y gestionar un modelo de datos institucional integrado, consistente, confiable, robusto, seguro, modelado y documentado Gestionar el proceso de investigación y desarrollo del área, así como las buenas prácticas de desarrollo y gestión del conocimiento, para asegurar el uso de tecnologías de vanguardia en la institución Elaborar el plan de trabajo del área de Desarrollo, con un enfoque en gestión (KPI's) Proponer, aplicar y controlar buenas prácticas en el proceso de desarrollo de sistemas Asegurar el cumplimiento de los procesos y el flujo de tareas establecidos Velar por la correcta asignación de personas por proyecto Velar por el éxito de los proyectos de desarrollo de sistemas (alcance, tiempo, costo) Supervisar al personal y las actividades del departamento bajo su responsabilidad

Centro de Cómputo y Soporte Técnico			
Técnico del Centro de Cómputo y	Encargado del Centro de Cómputo y Soporte Técnico	Programador de la Oficina Ejecutiva de Desarrollo de Software	Definir y coordinar la ejecución de procedimientos de prueba y desarrollar casos de prueba que sirvan al proceso general de garantía de calidad Proporcionar documentación de todos los procesos y la capacitación cuando sea necesaria Desarrollar e implementar procedimientos de mantenimiento, monitorizar la salud de los sistemas, recopilar estadísticas, y solucionar los errores y alarmas de los que se informe Realizar el diseño, implementación y la actualización de los sistemas de información para cumplir con las necesidades del negocio y el usuario Implementar las mejores prácticas para la escalabilidad, mantenimiento, facilidad del mismo, y rendimiento del sistema Colaborar con los miembros del equipo para determinar las mejores prácticas y los requisitos del cliente para el software Desarrollar un software intuitivo que satisfaga y supere las necesidades de la empresa Llevar un mantenimiento profesional de todo el software y crear actualizaciones regularmente para atender las inquietudes de los clientes y de la empresa. Analizar y someter a prueba los programas y productos antes de su lanzamiento oficial al mercado Solucionar problemas de programación de forma rápida y eficaz para garantizar un lugar de trabajo productivo
José Daniel Balarezo Perea	Warren Klaus Rojas García	Matt Again Moncada Abisrror	Garantizar la seguridad del software desarrollando programas para monitorizar activamente el intercambio de información privada Buscar activamente formas de mejorar los procesos y las interacciones del software empresarial Ayudar y respaldar en la formación y la capacitación de otros miembros del equipo para garantizar que todos los empleados se sientan seguros con el uso de las aplicaciones de software Atender las consultas y solucionar problemas técnicos realizado por los usuarios Administración de software y herramientas de asistencia técnica Derivar o escalar las consultas a el canal de apoyo apropiado Diagnosticar y solucionar de problemas de los usuarios Mantenimiento de la red local Administración de usuarios, creación y baja de cuentas Instalación, configuración, administración y mantenimiento de equipos informáticos (estaciones de trabajo, teléfonos ip, impresoras, scanner, Notebooks, tabletas, teléfonos, etc.) Resolver problemas técnicos de Hardware y Software
Técnico	Técnico Electrónico	Estudiante de Ing. De Sistemas	Armar, instalar, configurar y realizar tareas preventivas o correctivas sobre equipos informáticos Monitorear y supervisar la ejecución de los backups para poder resguardar toda la información de la compañía acorde a las políticas y procedimientos vigentes Ejecutar las políticas definidas respecto al movimiento, prestamos de los equipos y los medios de backup y su correspondiente almacenamiento Realizar el inventario de los equipos de cómputos desplegados en la institución o empresa Instalar y configurar la tecnología a ser empleada en la empresa, es decir, los equipos, sistemas operativos, programas y aplicaciones;

	Carlos Manuel Días Tuesta	Técnico	Realizar el mantenimiento periódico de sistemas; Brindar asistencia a los empleados o clientes acerca de tecnología; Detectar las averías en los sistemas y aplicaciones; Realizar diagnósticos del mal funcionamiento del hardware y el software; Encontrar soluciones a cualquier falla e implementarlas; Reemplazar las partes dañadas o con averías en los equipos cuando sea necesario; Realizar la solicitud de las piezas nuevas cuando falten en el inventario; Elaborar informes sobre el estado de los equipos y sistemas de la empresa; Implementar y orientar a los diferentes equipos en la ejecución de nuevas aplicaciones o sistemas operativos;
	Ricardo Herrera Sulca	Técnico	Aprender sobre nuevas aplicaciones o sistemas operativos; Realizar pruebas y evaluar nuevas aplicaciones antes de su implementación en los sistemas; Configurar perfiles, correos electrónicos y accesos para los nuevos ingresos, además de brindar asistencia en todo lo relacionado con contraseñas; Realizar revisiones de seguridad en todos los sistemas.

- **Producción y Desarrollo.**

  La Universidad Nacional de Ucayali, cuenta con la Oficina Ejecutiva de Desarrollo de Software que hace las veces de producción de soluciones de software cumpliéndose con todas las etapas del ciclo de desarrollo.

  Asimismo, es la encargada de realizar estudios de factibilidad, evaluar y proponer la aplicación de Sistemas Informáticos recomendables para la institución; está a cargo de un profesional no docente.

  Cuenta con las siguientes funciones:

  - Elaborar estudios de factibilidad para la aplicación de sistemas de información.
  - Programar y supervisar la implementación de sistemas de procesamiento electrónico de datos.

- Implementar el Registro de Recursos Informáticos de la UNU de acuerdo a lo dispuesto en el numeral 6.1 y 6.6 de la Directiva N° 004-2003-INEI/DTNP.
- Monitorear los Softwares Instalados.
- Formular, proponer y evaluar el Plan Operativo Informático y el Plan de Desarrollo Informático de la UNU, de acuerdo a lo dispuesto en la Directiva N° 004-2003-INEI/DTNP.
- Asesorar en asuntos de su especialidad.
- Custodiar el banco de preguntas del Examen de Admisión de la UNU.
- Otras tareas que se le encargue según la naturaleza de las funciones.

- **Servidores.**

  Cuenta con los siguientes tipos de servidores Web

  - **Servidor Web Compartido**

    Se entiende como Servidor Web Compartido corresponde al uso de una o más personas utilizaran el mismo servidor con tu sitio web.

    Dentro de los sistemas o sitios web que se encuentran implementados dentro de los servidores web compartido tenemos los siguientes:

    - Sitio web de la UNU que tiene como dominio web www.unu.edu.pe, y dos dominios.edu.pe extras, cuenta con 70 Gb de hosting para almacenamiento, transferencia de datos de 2000Gb, con 30 dominios

alojados, memoria RAM de 4 Gb, cuentas de correo ilimitados, programación en HTML, JavaScript, Flash y PHP, así como motor de base de datos MySQL.

- **Servidor Web VPS**

Se entiende como Servidor Web VPS corresponde a un servidor virtual que consiste en la habilitación de una máquina virtual con recursos específicos para el sitio o sistema web en específico. La UNU no cuenta con un servidor VPS.

- **Servidor Web Dedicado**

Tabla N° 6: UNU- Servidor Web Dedicado

Sistemas	Características
○ Matricula Virtual ○ Registro de nota Virtual ○ Sistema de caja ○ Sistema de Investigación ○ Sistema de soporte técnico ○ Sistema de bienestar Universitario ○ Sistema de Post Grado ○ Sistema de Segunda Especialidad ○ Sistema de CepreUnu ○ Sistema de Admisión	- Sistema Operativo: WINDOWS SERVER - Lenguaje de Programación: JAVA - Framework: NETBEANS - Memoria RAM Asignado en el Servidor: 16 gb. - Base de Datos: ORACLE 12 G - Velocidad de Transferencia de Datos 100/1000 - Compatibilidad: Es multiplataforma, pero no responsive. - Dominio: unu.edu.pe y sus sub dominios.

- **Hardware del centro de datos.**

Tabla N° 7: UNU - Hardware centro de datos

Marca	Modelo	Procesador	RAM	HDD
HP	DL380 GEN10	Xeon Gold 5118 - 2,3Ghz	262 GB	5,45 TB
HP	DL380 GEN9			
IMB	X3550 M4	Xeon E5-2640 - 2,5Ghz	64 GB	900 GB
IBM	X3650 M4	Xeon E5-2640 - 2,5Ghz	256 GB	1,2 TB
IBM	X3650 M3			
IBM	X3550 M3	Xeon X5650 - 2,67Ghz	32 GB	557,74 GB - 1,2 TB
IBM	X3100 M4			
HP	ML110 G7	Xeon E31220 - 3,1Ghz	14 GB	500 GB
HP	ML110 G9	Xeon E5-2603 v4 - 1,7Ghz	16 GB	2 TB
HP	ML110 G9	Xeon E5-2603 v4 - 1,7Ghz		
HP	ML110 G9	Xeon E5-2603 v4 - 1,7Ghz	65 GB	2 TB
HP	ML110 G9	Xeon E5-2603 v4 - 1,7Ghz		

- **Servidor proxy**

  La UNU cuenta con el servidor proxy palo alto, que permite obtener información de todas las actividades de Internet y conservar actualizados de los eventos de seguridad, este dispositivo mantiene una gran cantidad de registros de seguridad y tráfico.

  Lo que no posee es una configuración de políticas para restringir algunos accesos.

- **Sistema de Almacenamiento.**

  La Universidad Nacional de Ucayali, con almacenamiento local en sus servidores, pero no posee configuraciones de acceso por filtrado de archivos.

- **Proveedores y socios.**

  La UNU posee una gran alianza con cada uno de sus proveedores de las marcas de los equipos de TI, estos son consultados en casos que requiera ese nivel de atención, no se cuenta con un registro digital, ni físico de los proveedores.

- **Interconexión estratégica con otras instituciones.**

  No posee servicios de interconexión con otras entidades.

- **Flujos de trabajo.**

  La OGTISE, no cuenta con el diagrama de flujos de trabajo respecto a la seguridad perimetral.

- **Políticas, procedimiento de seguridad perimetral.**

  La UNU no cuenta con políticas y/o procedimientos sobre seguridad perimetral.

- **Reuniones de difusión de políticas.**

  Al no contar con políticas y/o procedimientos, no se realiza esta actividad.

- **Reuniones sobre Gestión de la Seguridad.**

  No se realizan estas actividades por no contar con un Sistema de Gestión de la Seguridad de la Información.

- **Cooperación de los gerentes sobre Seguridad de la Información.**

  No se realiza esta actividad por no contar con un Sistema de Gestión de la Seguridad de la Información.

- **Registro y control de acceso sobre la seguridad perimetral.**

  No se lleva un registro para el control de acceso.

- **Gestión de claves de acceso para la seguridad perimetral.**

  No existe una política y/o procedimiento para la gestión de claves de acceso

- **Sistema biométrico para acceso.**

  No se cuenta con este tipo se sistema.

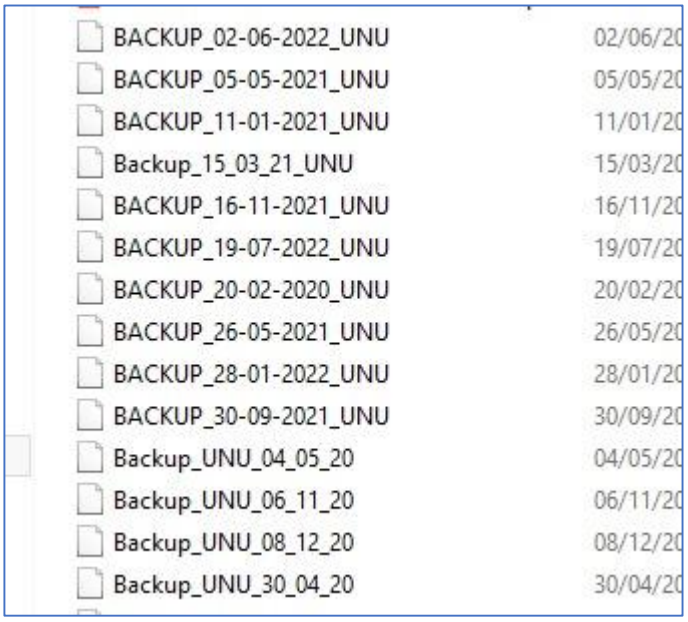
- **Registro de acceso al personal interno.**

  No se lleva el registro.

- **Respaldo de base de datos.**

  Se realizan respaldos de base de datos, pero no se lleva el control en registros.

Figura 6: UNU – Copias de seguridad



No se lleva el registro de control de las copias de seguridad.

- **Contingencias a nivel físico.**

  Únicamente redundancia de UPS.

- **Contingencias a nivel lógico.**

  Solo se realizan copias de seguridad, mas no se cuenta con una solución de contingencia.

- **Acceso a Internet.**

  Cuenta con servicio de internet dedicado, de 100 Mb de velocidad, es decir al 100% de su velocidad de transferencia, con alimentación por fibra óptica por parte del proveedor hasta la cabecera del centro de datos de la UNU, este servicio es brindado por la empresa Viettel Telecom S.A.C. (Bitel); dentro del paquete ofrecido por el proveedor se cuenta con Seguridad Perimetral Compartida.

- **Acceso a Intranet**

  Cuenta con una red de uso exclusivo, donde se puede publicar y compartir todo tipo de información y documentos siempre actualizados, nos permite la carga y descarga de información y documentos en una red común y privada, también se puede potenciar el trabajo colaborativo entre los empleados, el trabajo de protección se realiza mediante procedimientos seguros, aumentando la productividad y disminuyendo el coste de productividad.

  Se implementó una red LAN dentro del campus Universitario con salida de fibra óptica desde la cabecera del centro de datos de tipo de cable holgado, Monotubo Armado Dieléctrico OM3 de seis (06) fibras con velocidad de 10 Gbps. La distribución hasta los switchs principales por pabellón, facultades y edificios

de las oficinas administrativas, están siendo alimentados por Fibra óptica.

No se cuenta con un sistema alterno de tipo backup.

- **Extranet.**

  No cuenta con extranet, porque no existe un repositorio de archivos entre cliente y proveedor, ni mucho menos podemos acceder a base de datos de otras entidades sean públicas o privadas.

- **Verificación de IP salientes, entrantes.**

  Si se cuenta con un módulo a través de la herramienta PALO ALTO.

ACTIVIDADE DE IP

Figura 7: UNU – Actividades de IP

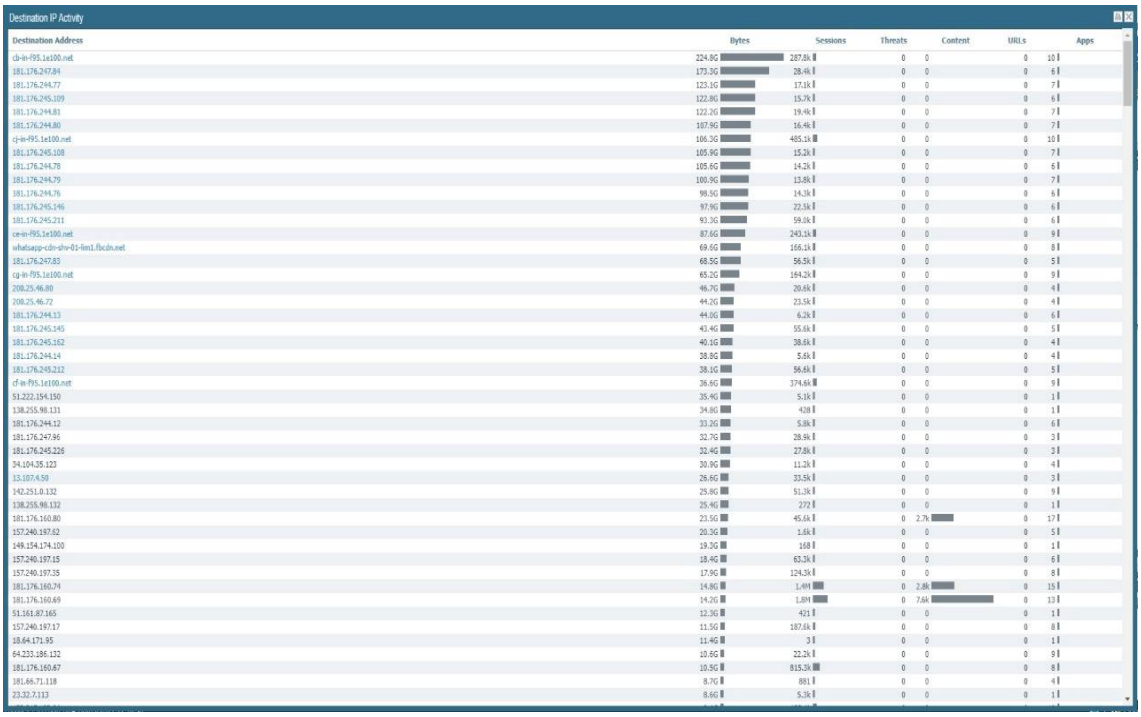
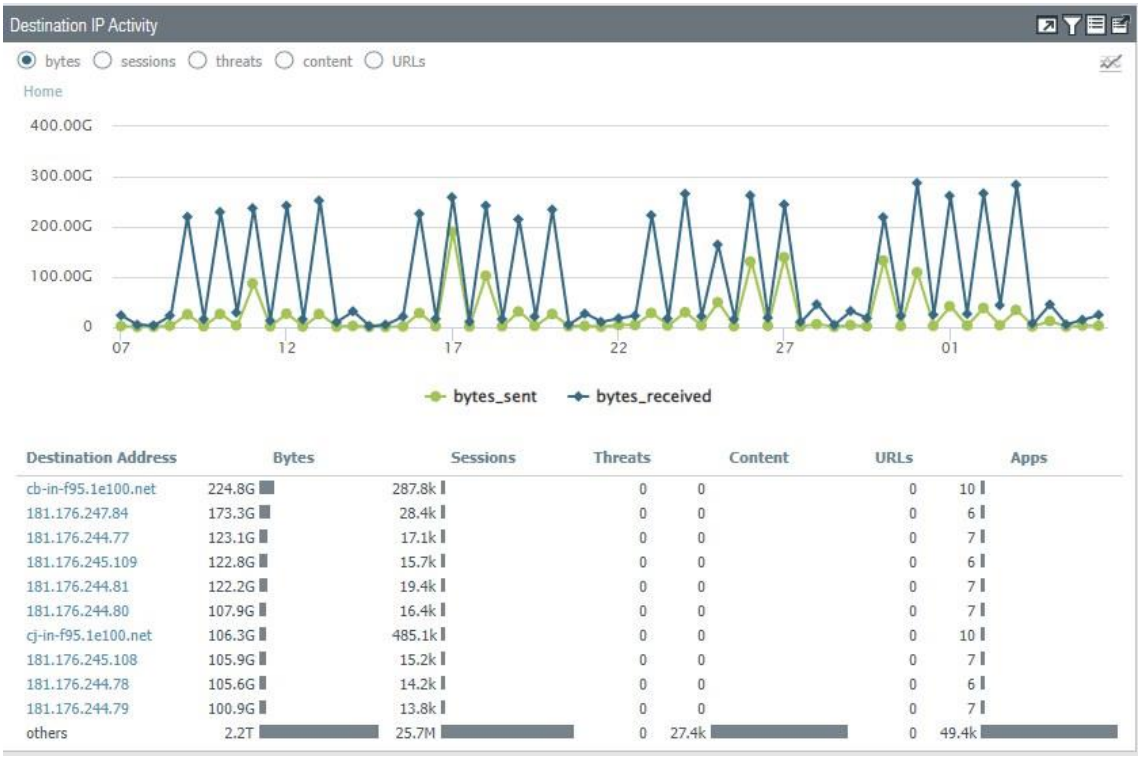


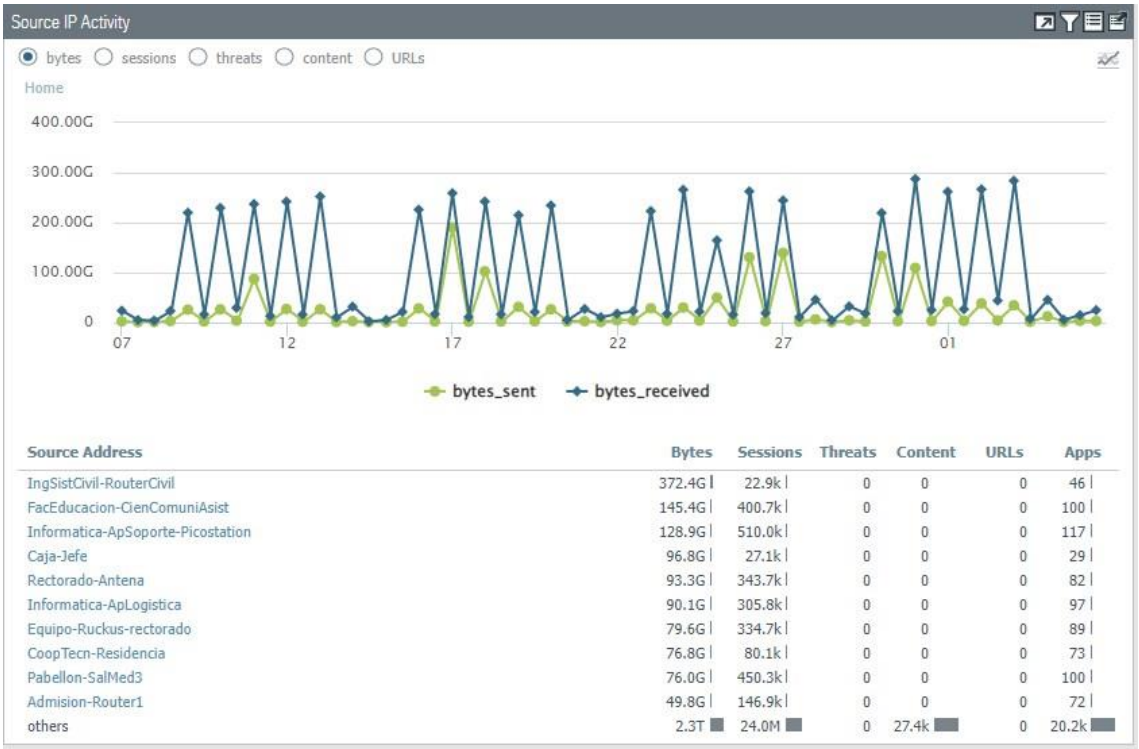
Figura 8: UNU – Actividades de IP Destino



Destination Address	Bytes	Sessions	Threats	Content	URLs	Apps
cb-in-f95.1e100.net	224.8G	287.8k	0	0	0	10
181.176.247.84	173.3G	28.4k	0	0	0	6
181.176.244.77	123.1G	17.1k	0	0	0	7
181.176.245.109	122.8G	15.7k	0	0	0	6
181.176.244.81	122.2G	19.4k	0	0	0	7
181.176.244.80	107.9G	16.4k	0	0	0	7
cj-in-f95.1e100.net	106.3G	485.1k	0	0	0	10
181.176.245.108	105.9G	15.2k	0	0	0	7
181.176.244.78	105.6G	14.2k	0	0	0	6
181.176.244.79	100.9G	13.8k	0	0	0	7
others	2.2T	25.7M	0	27.4k	0	49.4k

ACTIVIDADE DE IP ORIGEN

Figura 9: UNU – Actividades de IP Origen



Source Address	Bytes	Sessions	Threats	Content	URLs	Apps
IngSistCivil-RouterCivil	372.4G	22.9k	0	0	0	46
FacEducacion-CienComuniAsist	145.4G	400.7k	0	0	0	100
Informatica-ApSoporte-Picostation	128.9G	510.0k	0	0	0	117
Caja-Jefe	96.8G	27.1k	0	0	0	29
Rectorado-Antena	93.3G	343.7k	0	0	0	82
Informatica-ApLogistica	90.1G	305.8k	0	0	0	97
Equipo-Ruckus-rectorado	79.6G	334.7k	0	0	0	89
CoopTecn-Residencia	76.8G	80.1k	0	0	0	73
Pabellon-SalMed3	76.0G	450.3k	0	0	0	100
Admision-Router1	49.8G	146.9k	0	0	0	72
others	2.3T	24.0M	0	27.4k	0	20.2k

ACTIVIDADE A APLICACIONES MAS USADAS

Figura 10: UNU – Aplicaciones utilizadas



Application Usage

Application	Risk	Bytes	Sessions	Threats	Content	URLs	Users
quic	1	2.1T	5.2M	0	0	0	384
ssl	4	692.2G	3.6M	0	0	0	816
google-base	4	517.8G	739.4k	0	0	0	412
facebook-base	4	294.9G	496.6k	0	0	0	290
ms-update	4	273.2G	193.2k	0	0	0	406
web-browsing	4	139.0G	2.1M	0	32.4k	0	10.4k
whatsapp-base	1	127.8G	237.7k	0	0	0	306
youtube-base	4	95.2G	76.7k	0	0	0	350
facebook-video	4	71.0G	74.8k	0	0	0	128
tiktok	2	68.9G	176.6k	0	0	0	105
ms-rdp	4	37.9G	6.3M	0	0	0	1.0k
rtcp	1	36.1G	1.1k	0	0	0	42
gmail-base	4	31.2G	128.0k	0	0	0	281
ms-teams-audio-video	2	30.0G	3.0k	0	0	0	39
whatsapp-file-transfer	3	26.1G	29.7k	0	0	0	295
telegram-base	2	20.0G	7.5k	0	0	0	38
sharepoint-online	3	18.0G	4.2k	0	0	0	97
netflix-base	3	17.4G	6.1k	0	0	0	40
mega-base	3	15.2G	6.8k	0	0	0	48
whatsapp-web	2	11.4G	40.4k	0	0	0	308
unknown-udp	1	10.5G	16.6k	0	0	0	281
ms-onedrive-base	4	8.7G	16.7k	0	0	0	135
google-update	3	6.7G	485	0	0	0	213
stun	2	6.3G	17.8k	0	0	0	86
zoom-meeting	2	6.3G	136	0	0	0	7
http-video	4	5.6G	132	0	0	0	7
outlook-web-online	3	5.1G	43.6k	0	0	0	216
windows-azure-base	1	5.0G	6.6k	0	0	0	221
zoom-base	1	4.6G	1.2k	0	0	0	22
samsung-updates	1	3.2G	498	0	0	0	20
ms-teams	3	3.1G	78.3k	0	0	0	290
dailymotion	4	3.0G	879	0	0	0	18
itunes-base	3	2.7G	9.2k	0	0	0	20
speedtest	2	2.6G	481	0	0	0	21
dns	3	2.4G	7.7M	0	0	0	185
udemy-base	2	1.9G	446	0	0	0	10
hotmail	4	1.9G	8.4k	0	0	0	67
web-crawler	4	1.7G	7.1k	0	450	0	245
traceroute	2	1.2G	35.1k	0	0	0	90

- **Firewall Internet.**

  El elemento de control del firewall de próxima generación (NGFW) basado en ML de la serie PA-800 es PAN-OS®, que clasifica de forma nativa todo el tráfico, incluidas las aplicaciones, las amenazas y el contenido, y luego vincula ese tráfico al usuario independientemente de ubicación o tipo de dispositivo. La aplicación, el contenido y el usuario, en otras palabras, los elementos que hacen funcionar su negocio, luego sirven como la base de sus políticas de seguridad, lo que da como resultado una postura de seguridad mejorada y un tiempo de respuesta a incidentes reducido. Cuenta con puerto de administración fuera de banda 10/100/1000, alta disponibilidad 10/100/1000 (4) Gigabit SFP (8), un puerto de consola RJ-45,

puerto USB y puerto de consola Micro USB, con SSD de 240 GB de almacenamiento, cuenta con dos fuentes de alimentación de CA de 500 W. Una fuente de alimentación es redundante. La seguridad que utiliza es cCSAUS, CB, con una interfaz de administración FCC clase A, CE Clase A y VCCI Clase A.

Implementa políticas coherentes para usuarios locales y remotos que se ejecutan en las plataformas Windows, Mac OS X, Linux, Android o Apple Ios, así como también permite la integración sin agentes con Microsoft Active Directory y Terminal Services, LDAP, Novell eDirectory y Citrix e integra fácilmente sus políticas de firewall con 802.1X inalámbrico, proxies, soluciones NAC y cualquier otra fuente de información de identidad del usuario.

- **Firewall Extranet.**

  La Universidad Nacional de Ucayali al no contar con Extranet esta no cuenta con firewall de extranet, porque no existe un repositorio de archivos entre cliente y proveedor ni mucho menos podemos acceder a base de datos de otras entidades sean públicas o privadas.

- **Sistema de auditoría.**

  No cuenta con un componente de auditoria como Netwrix, Firemon u otros que haga las veces.

- **Monitorización de tráficos en la LAN.**

  Esta actividad no se realiza.

- **Monitorización de tráficos en la red Wireless.**

  Esta actividad no se realiza.

- **Pasarelas y antivirus.**

  No se cuenta con pasarelas antivirus y antispam.

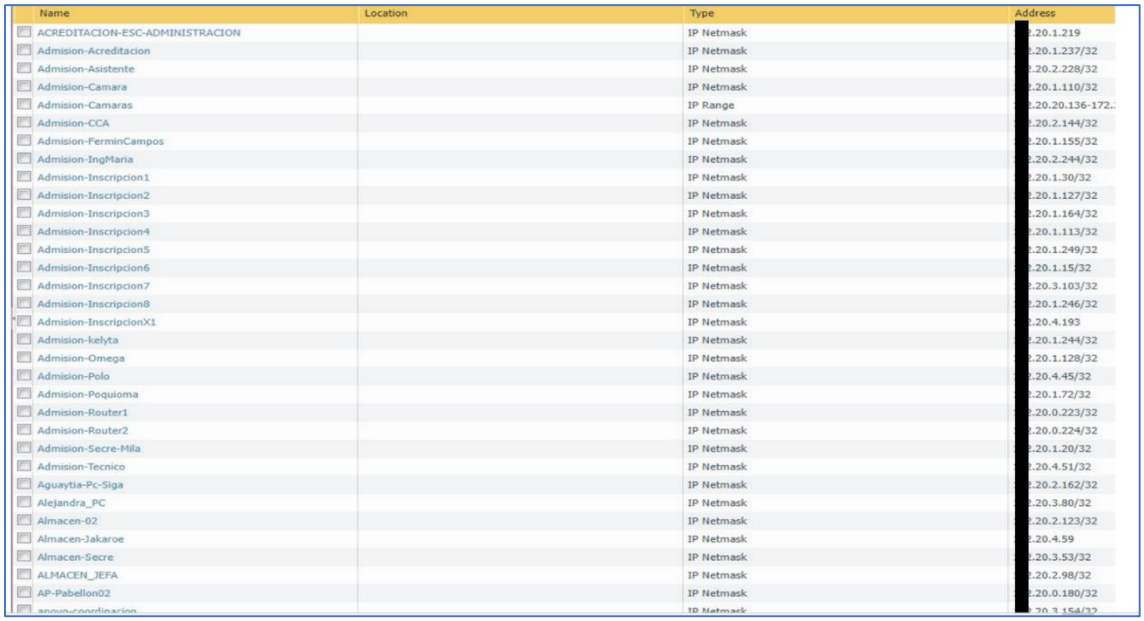
- **Testeo de DNS y DNS Blocklist.**

  Se realiza a nivel intermedio a través de las listas negras de DNS a través de Firewall PALO ALTO y el Antivirus.

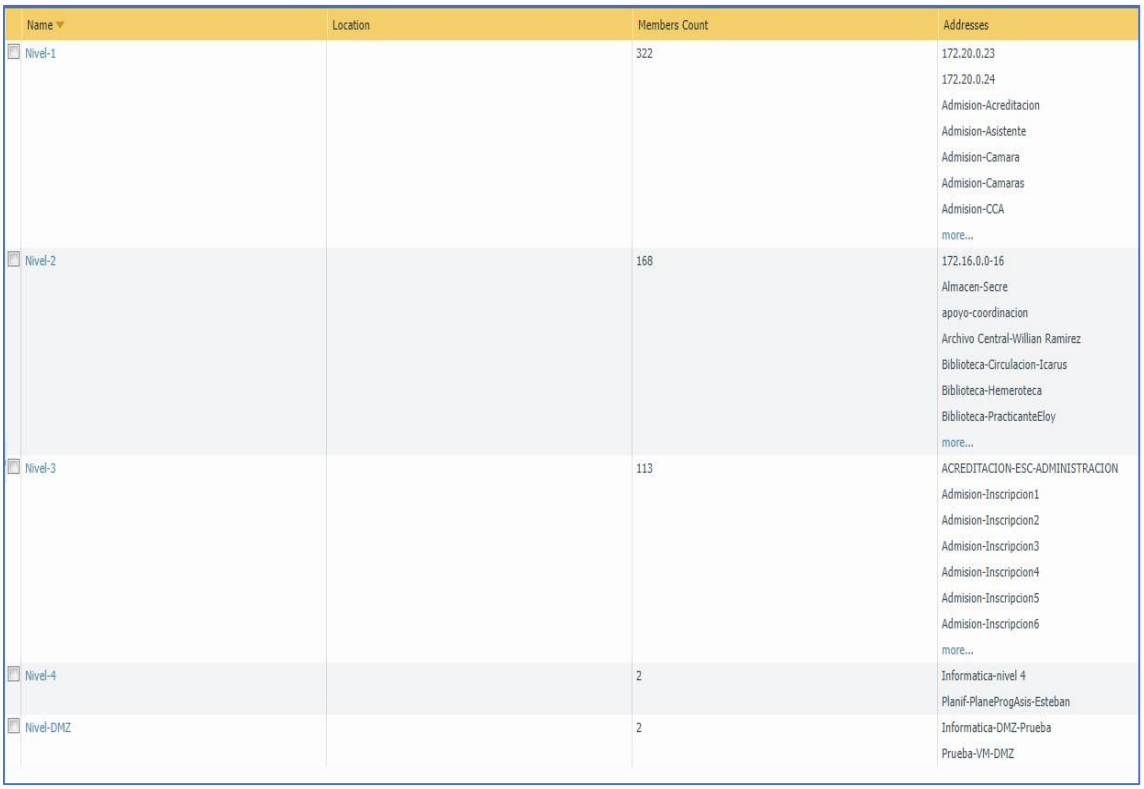
- **Servidores proxy.**

  La Universidad Nacional de Ucayali cuenta con el Firewall Palo Alto PA-800 que desde su plataforma administrable se ejecutan las configuraciones proxys. No se implementó un servidor proxy dedicado, ya que gracias a las funcionalidades del Firewall PA-800 estas son gestionadas dentro del software. Se adjunta imágenes de los niveles y permisos del internet.

Figura 11: UNU – Niveles y permisos de internet



Name	Location	Type	Address
ACREDITACION-ESC-ADMINISTRACION		IP Netmask	[redacted].20.1.219
Admision-Acreditacion		IP Netmask	[redacted].20.1.237/32
Admision-Asistente		IP Netmask	[redacted].20.2.228/32
Admision-Camara		IP Netmask	[redacted].20.1.110/32
Admision-Camaras		IP Range	[redacted].20.20.136-172.[redacted]
Admision-CCA		IP Netmask	[redacted].20.2.144/32
Admision-FerminCampos		IP Netmask	[redacted].20.1.155/32
Admision-IngMaria		IP Netmask	[redacted].20.2.244/32
Admision-Inscripcion1		IP Netmask	[redacted].20.1.30/32
Admision-Inscripcion2		IP Netmask	[redacted].20.1.127/32
Admision-Inscripcion3		IP Netmask	[redacted].20.1.164/32
Admision-Inscripcion4		IP Netmask	[redacted].20.1.113/32
Admision-Inscripcion5		IP Netmask	[redacted].20.1.249/32
Admision-Inscripcion6		IP Netmask	[redacted].20.1.15/32
Admision-Inscripcion7		IP Netmask	[redacted].20.3.103/32
Admision-Inscripcion8		IP Netmask	[redacted].20.1.246/32
Admision-InscripcionX1		IP Netmask	[redacted].20.4.193
Admision-kelyta		IP Netmask	[redacted].20.1.244/32
Admision-Omega		IP Netmask	[redacted].20.1.128/32
Admision-Polo		IP Netmask	[redacted].20.4.45/32
Admision-Poquioma		IP Netmask	[redacted].20.1.72/32
Admision-Router1		IP Netmask	[redacted].20.0.223/32
Admision-Router2		IP Netmask	[redacted].20.0.224/32
Admision-Secre-Mila		IP Netmask	[redacted].20.1.20/32
Admision-Tecnico		IP Netmask	[redacted].20.4.51/32
Aguaytia-Pc-Siga		IP Netmask	[redacted].20.2.162/32
Alejandra_PC		IP Netmask	[redacted].20.3.80/32
Almacen-02		IP Netmask	[redacted].20.2.123/32
Almacen-Jakaroe		IP Netmask	[redacted].20.4.59
Almacen-Secre		IP Netmask	[redacted].20.3.53/32
ALMACEN_JEFA		IP Netmask	[redacted].20.2.98/32
AP-Pabellon02		IP Netmask	[redacted].20.0.180/32
anoyo-coordinacion		IP Netmask	[redacted].20.3.154/32



Name	Location	Members Count	Addresses
Nivel-1		322	172.20.0.23 172.20.0.24 Admision-Acreditacion Admision-Asistente Admision-Camara Admision-Camaras Admision-CCA more...
Nivel-2		168	172.16.0.0-16 Almacen-Secre apoyo-coordinacion Archivo Central-Willian Ramirez Biblioteca-Circulacion-Icarus Biblioteca-Hemeroteca Biblioteca-PracticanteEloy more...
Nivel-3		113	ACREDITACION-ESC-ADMINISTRACION Admision-Inscripcion1 Admision-Inscripcion2 Admision-Inscripcion3 Admision-Inscripcion4 Admision-Inscripcion5 Admision-Inscripcion6 more...
Nivel-4		2	Informatica-nivel 4 Planif-PlaneProgAsis-Esteban
Nivel-DMZ		2	Informatica-DMZ-Prueba Prueba-VM-DMZ

- **Registro del personal externo.**

  No se lleva el registro del personal externo que ingresas a las instalaciones relacionados con la seguridad perimetral.

- **Registro de indecencias de copias de seguridad.**

  No se lleva el registro de incidencias de copias de seguridad.

- **Registro de incidencias en telecomunicaciones.**

  No se lleva el registro de incidencias en telecomunicaciones.

4.1.4. PROPUESTA DE SOLUCIÓN E IMPLEMENTACIÓNES DE SOLUCIONES.

- **Políticas de servidor proxy.**

  Si la institución cuenta con un servidor proxy, lo que carece es de la configuración de políticas de bloque de algunos sitios web, para ello se ha implementado políticas de bloqueo las

cuales se detallan en el punto denominado Políticas para proxy puntos más adelante.

- **Almacenamiento adecuado.**

  Se cuenta con almacenamiento como se indica antes, pero no se cuenta con servicios de bloqueo por tipos de archivos, este servicio se implementó y se detalla en el punto titulado Intranet – filtrado de tipos de archivos

- **Implementación registros de proveedores.**

Figura 12: UNU – Registro de proveedores



UNIVERSIDAD NACIONAL DE UCAYALI

OFICINA GENERAL DE TI SISTEMAS E INFORMATIVA

FORMATO: REGISTRO DE PROVEEDORES

NRO	RAZON SOCIAL	REPRESENTANTE	SERVICIO	TELEFONO FIJO	NROS CELULAR	PAGINA WEB	H. ATENCION	CIUDAD
1								
2								
3								

- **Interconexión con otras instituciones.**

  Reniec: Servicios como:

  - Consulta en línea, vía internet.
  - Verificación Biométrica.
  - Cotejo Masivo.

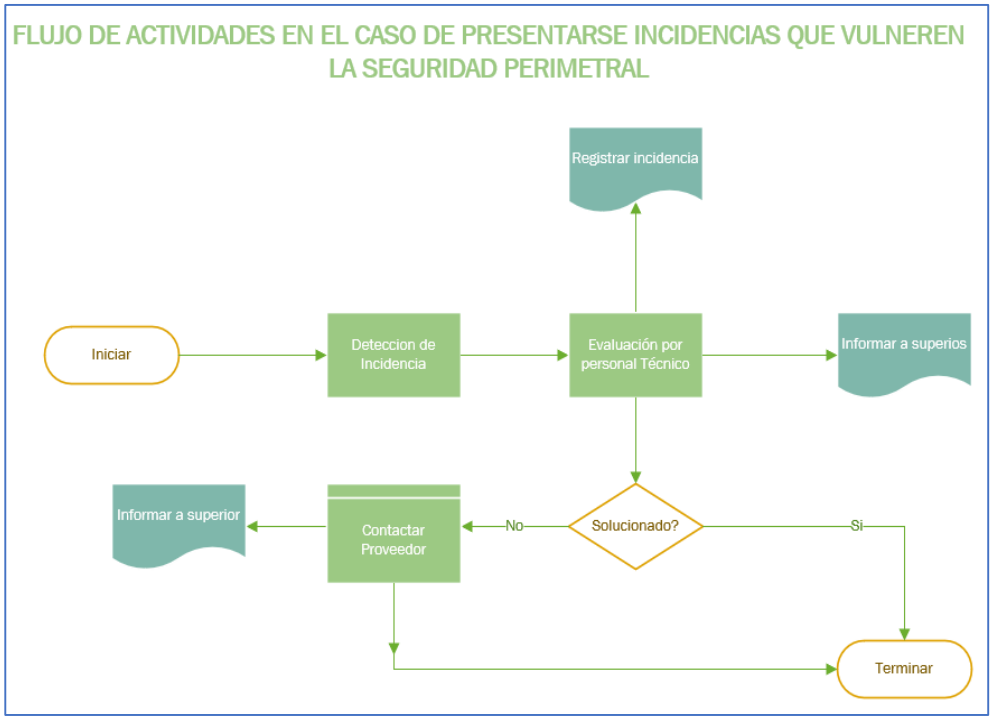
  Servicios de Bancos.

  - Para pagos de los servicios de UNU a través de la plataforma online.
  - Pagos de servicios de UNU a través de tarjetas de crédito o débito.

- **Flujos de trabajo, procedimiento.**

  Flujo de trabajo

Figura 13: UNU – Flujo de actividades



- **Procedimiento para control perimetral.**

  El procedimiento implementado posee las siguientes características:

PROCEDIMIENTO SEGURIDAD PERIMETRAL

Código del proceso	
Nombre del proceso	
Objetivo del proceso	
Nombre del proceso relacionado	
Responsable	

	Órgano / Unidad Orgánica	**Firma y sello**
Elaborado por:		
Revisado por:		
Aprobado por:		
Fecha:		

DESCRIPCIÓN DEL PROCEDIMIENTO:

1: Gestión de acceso a los Cuartos de Comunicaciones:

N°	Descripción de la actividad	Responsable	Puntos de Control / Observaciones	Documentos que se generan
1	Otorgar, al personal, roles de Administración de los Cuartos de Comunicaciones.	Jefe	**Punto de Control:** Definir funciones de acuerdo a perfiles y competencias.	Informe
2	Registrar el permiso diligenciado en el "Formato de acceso permanente al Centro de Datos y los Cuartos de Comunicaciones" (anexo 1).	Jefe	Punto de Control: Verifica que se asignen privilegios según las funciones	Informe.
3	Comunicar a la OGA y la RRHH , la autorización de ingreso en horario no laboral en casos de emergencia a los Cuartos de Comunicaciones.	Jefe		Informe
4	Realizar las tareas de administración, monitoreo, mantenimiento en los Cuartos de Comunicaciones de acuerdo al rol. Registrar en "Bitácora de Acceso" (Anexo 2)	Personal de TI	**Punto de Control:** Director/a de la Oficina de Tecnologías de la Información debe verificar periódicamente el diligenciamiento de la Bitácora de Acceso y los fines de los accesos.	Bitácora
5	Solicitar autorización de acceso al a los Cuartos de Comunicaciones a personal no autorizado, (funcionario, tercero, y/o contratista), diligenciar el formato "Autorización Acceso a los Cuartos de Comunicaciones" **(Anexo 3)**.	Personal de TI		
6	Autorizar o denegar el ingreso de personal previa evaluación.	Jefe		Bitácora
7	Elaborar informe mensual de actividades realizadas en los Cuartos de Comunicación y gestión de aseguramiento de los servicios de red.	Personal de TI		

FORMATO DE PROCEDIMIENTO

ANEXO 1. Formato de acceso permanente a los Cuartos de Comunicaciones

Fecha de autorización:	**Día:**	**Mes:**	**Año:**
Firma:	**Firma:**		
Nombre:	**Nombre:**		
Oficina General de Estadística e Informática	**Oficina de Tecnología de la Información**		

Nº	**Datos del personal autorizado**
	Nombre completo: DNI: **Cargo:** **Rol: Teléfono Móvil:** **Anexo:**

ANEXO 2. Bitácora de acceso al Centro de Datos y Cuartos de Comunicaciones

Fecha	DNI/RUC	Nombre y Apellidos	Empresa / Oficina	Labor a realizar	Hora de Ingreso	Hora de Salida	Autoriza	Firma

- **Reuniones de difusión de políticas y/o procedimientos.**

  Es recomendable realizar reuniones de difusión de políticas y/o procedimiento en los siguientes casos:

  - Personal nuevo en el área.
  - Posterior a la una actualización del procedimiento y/o política.
  - Al crearse una nueva política y/o procedimiento.
  - Dos veces por año en los siguientes meses:
    - Marzo.
    - Octubre.

- **Conformación de un comité de seguridad de la información (SGSI).**

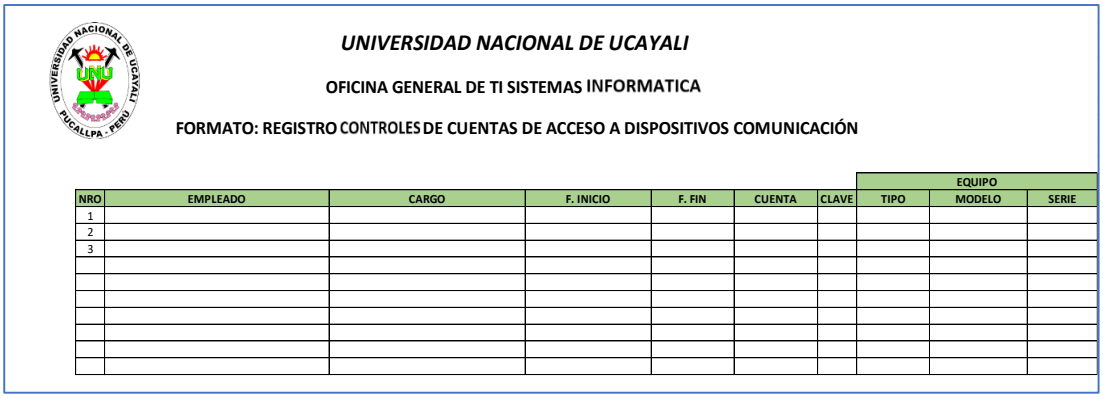
  Este Comité estará comprometido en la elaboración de las estrategias y mejoras en lo que concierne la seguridad de la información. Estará integrado por personal de alta dirección jefaturas o direcciones.

  Funciones:

  - Precisar las políticas sobre seguridad de la información alineados con el Plan Estratégico Organizacional.
  - Mantenimiento de los productos del SGSI
  - Identificación de riesgos respecto al SGSI.
  - Adecuación del SGSI.
  - Suministrar los recursos relacionados con el SGSI.
  - Evaluación de las vulnerabilidades sobre lo implementado.
  - Monitorear el SGSI.
  - Concientización sobre el SGSI.

- **Registro de control de cuentas de acceso sobre equipos seguridad perimetral.**

Figura 14: UNU – Registro de control de cuentas de acceso a dispositivos



UNIVERSIDAD NACIONAL DE UCAYALI

OFICINA GENERAL DE TI SISTEMAS INFORMATICA

FORMATO: REGISTRO CONTROLES DE CUENTAS DE ACCESO A DISPOSITIVOS COMUNICACIÓN

NRO	EMPLEADO	CARGO	F. INICIO	F. FIN	CUENTA	CLAVE	EQUIPO		
							TIPO	MODELO	SERIE
1									
2									
3									

- **Sistema biométrico para acceso a las instalaciones.**

  Se propone implementar un control de acceso físico, de tipo biométrico, a las instalaciones donde se ubican los equipos informáticos críticos de la institución, las características de control podrían ser las siguientes:

Tabla N° 8: UNU - Características control de acceso

Características	Valores
Biométrico	Huella
Tarjeta y Protocolo LF/HF	Dual RFID, MultiCLASS SE y Dual RFID
Max Usuarios	10 000
Tcp/Ip	Si
Usb	No
CPU	1,0Ghz
Memoria	8Gb
LED	Multicolor
Alimentación	12VDC
Tecnología	Huella dactilar

- **Registro de acceso al personal interno**

Figura 15: UNU – Registro de control de acceso personal interno

UNIVERSIDAD NACIONAL DE UCAYALI

OFICINA GENERAL DE TI SISTEMAS E INFORMATICA

FORMATO: REGISTRO DE CONTROL DE ACCESO A PERSONAL INTERNO

NRO	EMPLEADO	CARGO	H. Ingreso	H. Finalizacion	Tareas Realizadas	Autorizado por
1						
2						
3						

- **Registro de copias de seguridad.**

  Se implementó un registro para llevar el control de las copias de seguridad realizados.

Figura 16: UNU – Registro backup



UNIVERSIDAD NACIONAL DE UCAYALI

OFICINA GENERAL DE TI SISTEMAS E INFORMATICA

FORMATO: REGISTRO BACKUPS

NRO	RESPONSABLE	FECHA	HORA	MARCA	MODELO	DATOS	ARCHIVO	TAMAÑO	OBSERVACIONES
1									
2									
3									

- **Contingencia a nivel Físico.**

  Se recomienda adquirir un servidor de las mismas características del servidor principal.

  - Adquirir bancos de baterías redundantes.
  - Sistemas de climatización redundante.
  - Sistema contra incendio redundante.

  Switchs Core, de acceso, Firewall para contingencia.

  UPS a nivel de piso.

  Generador de energía eléctrica.

- **Contingencia a nivel lógico.**

  Se recomienda los siguiente:

  Licencia para replicación del sistema de virtualización, como Citrix XenServer u otro.

  - Licencias para software de replicación de aplicaciones en tiempo real a nivel de aplicaciones y de base de datos

- **Respaldo de conexión de internet.**

  Para garantizar el acceso a internet es recomendable que se instale una redundancia de interconexión, reescribiendo un nuevo contrato con el operador.

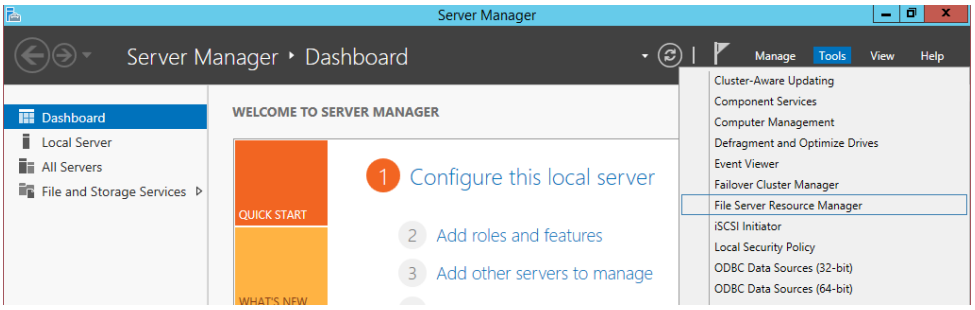
  La conexión de backup deberá tener las siguientes características.

  - El sistema Back up debe ser de Fibra Óptica y/o 4G.
  - Permite la conexión a internet a todos los equipos y/o dispositivos.
  - El ancho de banda debe ser el mismo que de la interconexión principal, así como los valores para subir y descargar.

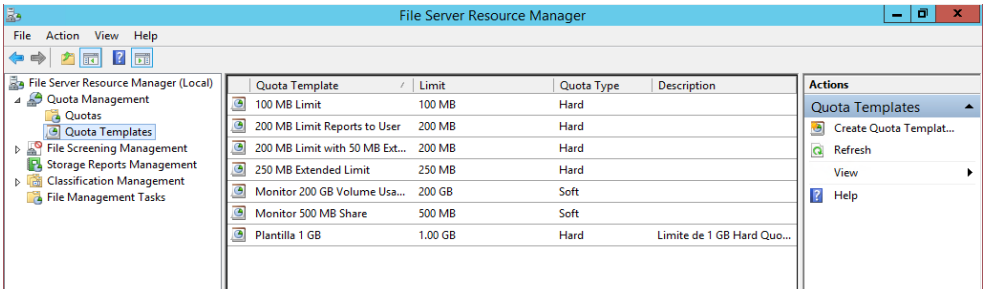
- **Intranet – filtrado de tipos de archivos.**

  Debido a la carencia de la configuración del filtrado por tipos de archivos, se determinó realizar las configuraciones necesarias a fin de que el sistema de almacenamiento cuente con esta importante restricción, cuyos pasos se detallan a continuación:
  Como el SO es Windows 2012 R2, se procedió con efectuar la configuración del filtrado de archivos (Imágenes, ejecutables, Audio y Video), tal como a continuación se muestra:

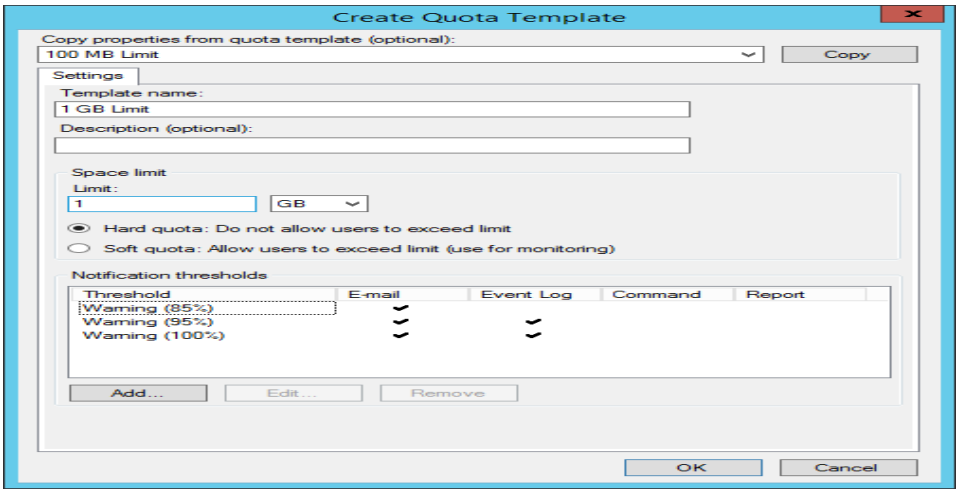
- Desde Server Manager iniciar la consola File Server Resource Manager.



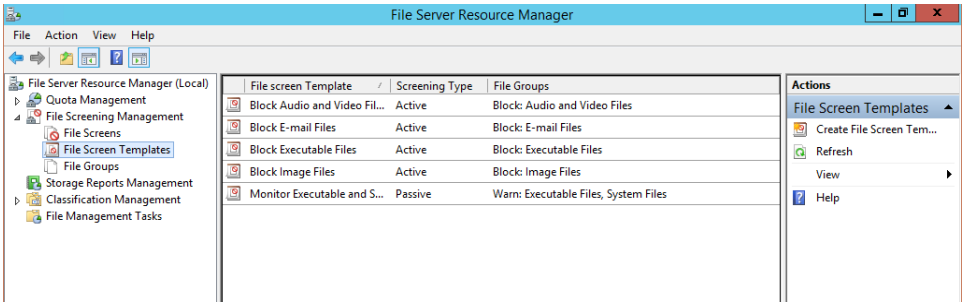
- Expandir el nodo Quota Management luego hacer clic sobre Quota Templates, luego hacer clic sobre la opción Create Quota Template



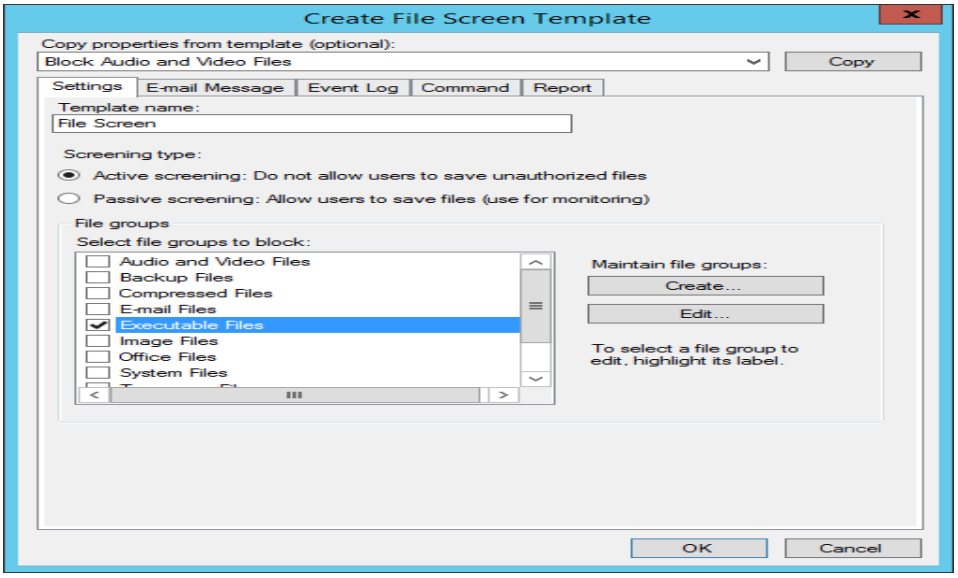
- En la ventana Create Quota Template, especificar el nombre en el campo Template name luego en la sección Space limit seleccionar la unidad de medida y la cantidad de espacio por último presionar el botón OK.



- Expandir el nodo File Screening Management luego hacer clic sobre File Screen Templates, luego hacer clic sobre la opción Create File Screen Templat



- En la ventana Create File Screen Template, especificar el nombre en el campo Template name luego en la sección Screening Type seleccionar el modo activo o pasivo, en la sección File Groups seleccionar los grupos de archivos que queremos filtrar por último presionar el botón OK.



- **Extranet – características.**

  Debido a la finalidad de la UNU se recomienda implementar una extranet académica con los siguientes requerimientos mínimos:

  - Ingreso al sistema: Generar su acceso mediante el ingreso de su correo personal - Actualizar sus datos personales - Cambiar su contraseña El personal administrativo ingresará mediante su cuenta de dominio.
  - Acceso a la información académica del estudiante: Notas - Unidades didácticas matriculadas - Inasistencias - Horario de clases - Record Académica - Avance curricular.
  - Acceso a deudas y pagos: Realizar pagos en línea, mediante una pasarela con visa - Visualizar sus pagos efectuados y pagos pendientes.

- Gestión de la información del docente: Visualizar sus unidades didácticas - Visualizar su horario - Visualizar su asistencia - Visualizar documentos.
- Capacitación docente: Realizar la gestión de flyers - Gestión docentes - Gestión estudiantes - Gestión Documentos.
- Medio de comunicación académica: El personal administrativo podrá realizar el envío de mensajes y notificaciones a los estudiantes y profesores.
- Gestión de documentos, capacitaciones y eventos.

- **Firewall para Extranet.**

  Se recomienda un firewall que cumpla con las siguientes características mínimas:

  - Filtrado de las direcciones de IP de destino y de origen.
  - Gestión de protocoles TCP o UDP.
  - Filtrado de puertos.
  - Uso de flags en las cabeceras de TCP.

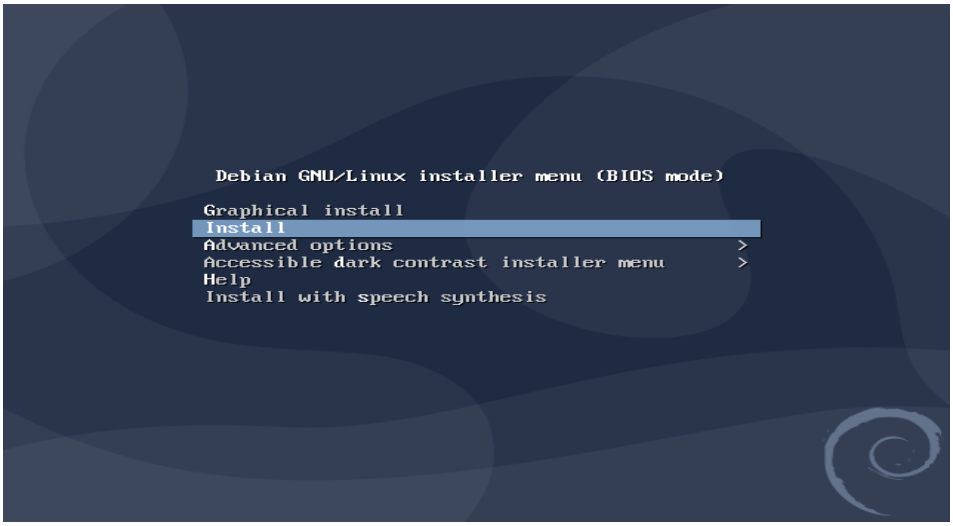
    Filtrado de direcciones

- **Sistema para auditoria.**

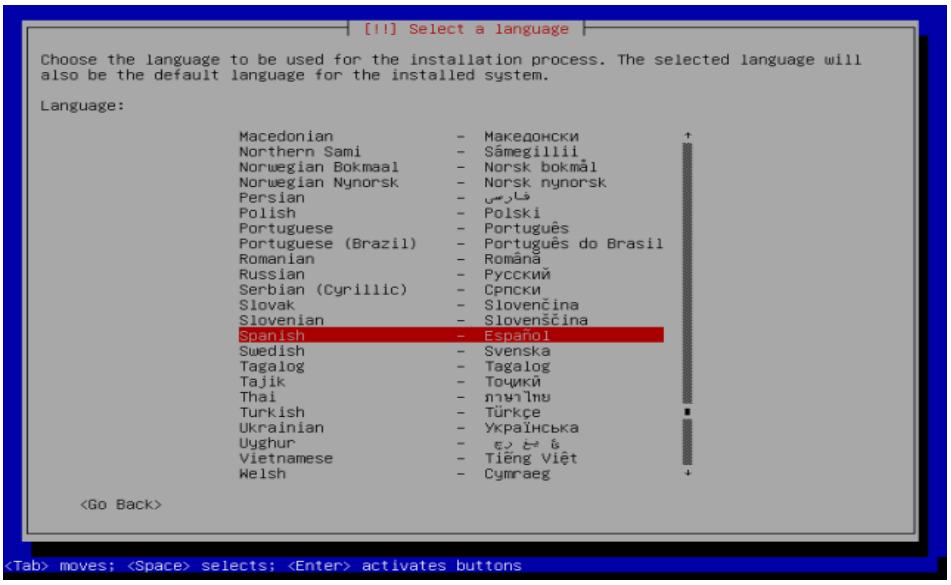
  Se implementó un pc con software libre de SO Debian y el software de auditoria Open-Audit. A continuación, se presentan capturas del proceso de instalación realizado.

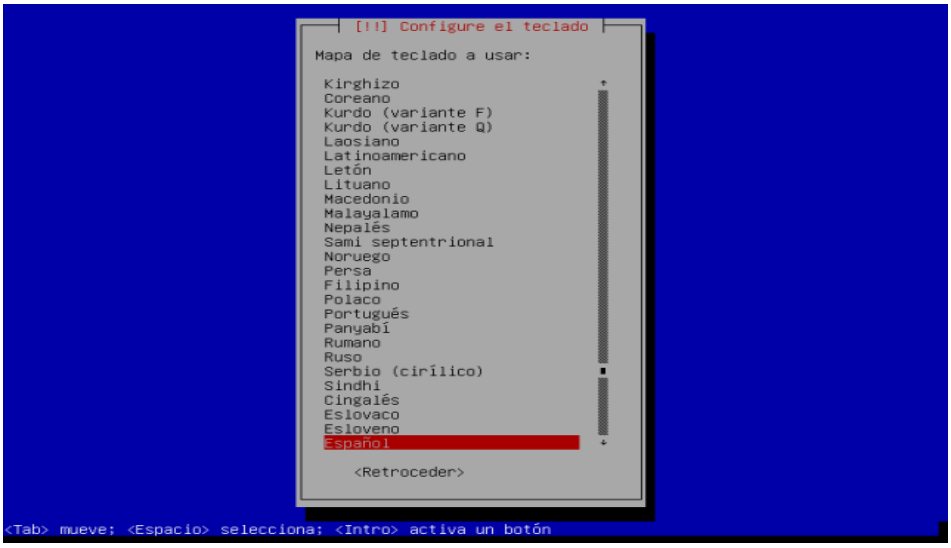
  Instalación de Debian.

  - Modo de instalación.

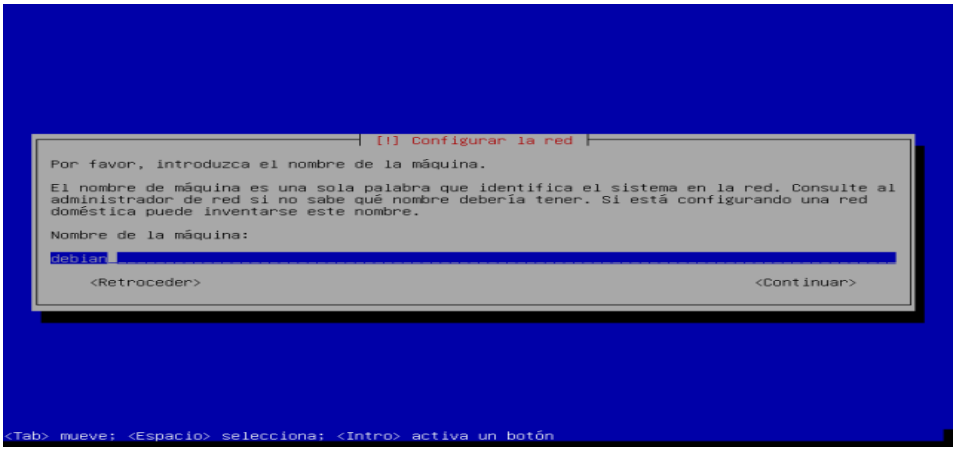


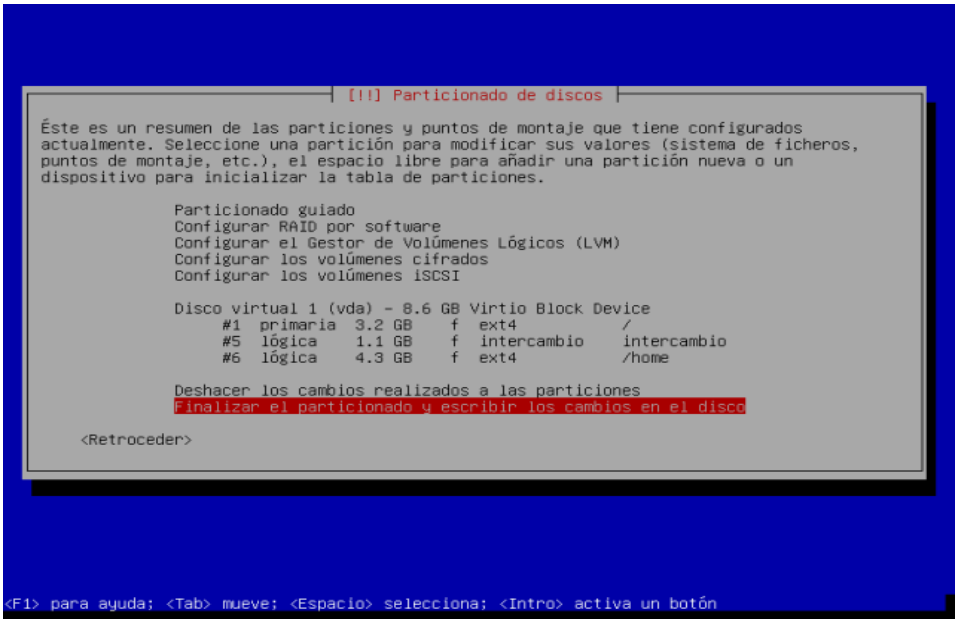
- Idioma, ubicación y teclado





- Máquina, el dominio y el superusuario y otros





- Configurando Sudo.

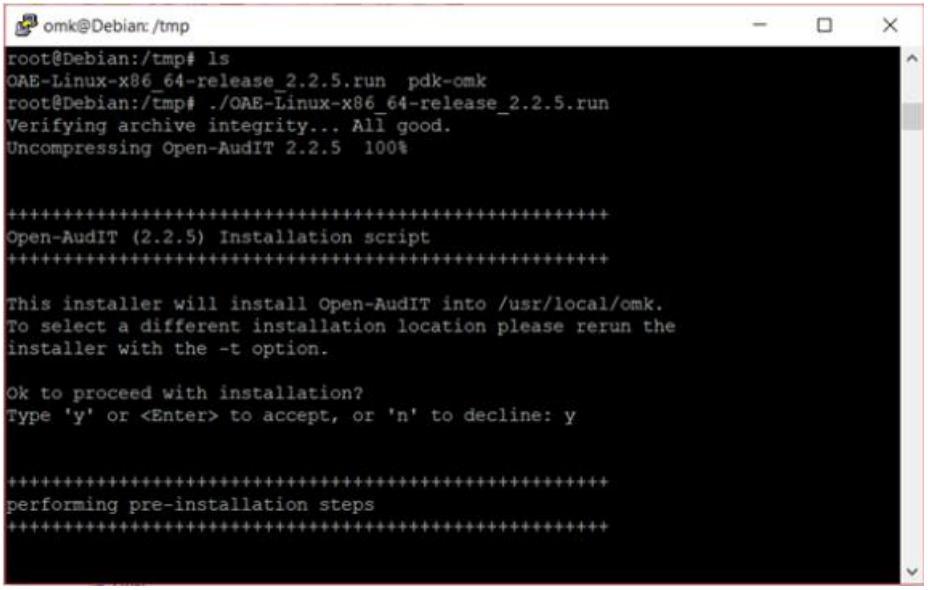
  proxyUNU@debian:~$ su –

  Contraseña:

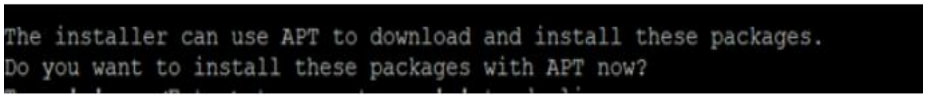
  root@debian:~# chmod +r+w /etc/sudoers

Instalación de OAE.

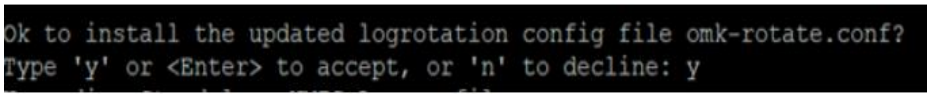
Se ejecuta el instalador con el siguiente comando ./OAE-Linux-x86_64-release_2.2.5.run.



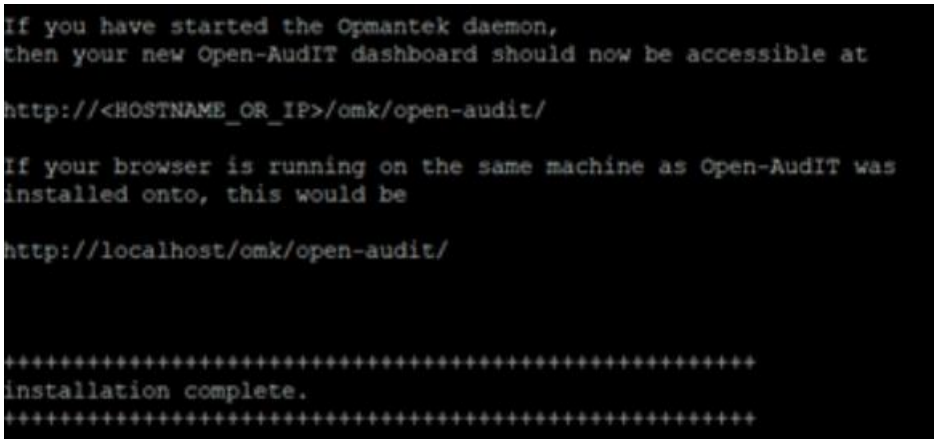
Open-AudIT se requiere los paquetes APT, pregunta si se desea instalar estos paquetes con APT ahora. escribir para aceptar.



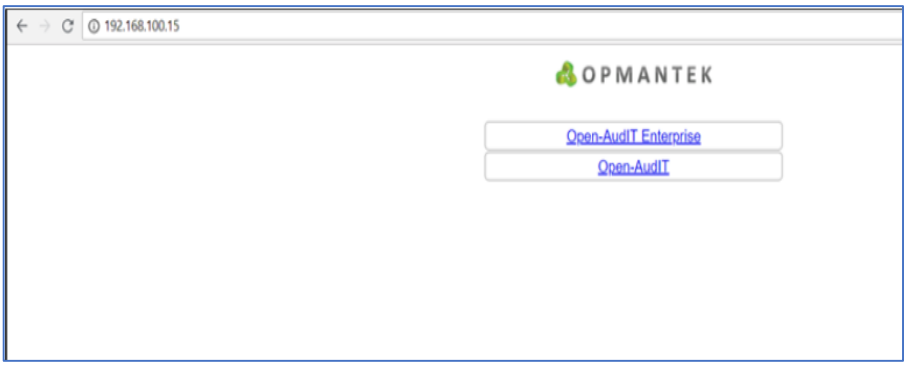
Pregunta si se desea instalar el archivo de configuración de actualizado omk-rotate.conf, escribir para aceptar.

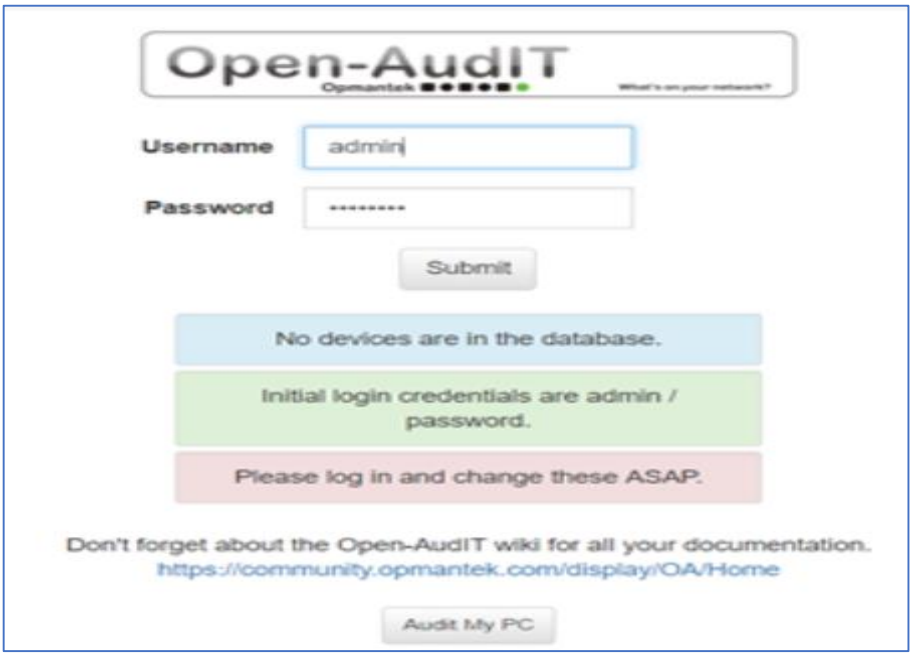


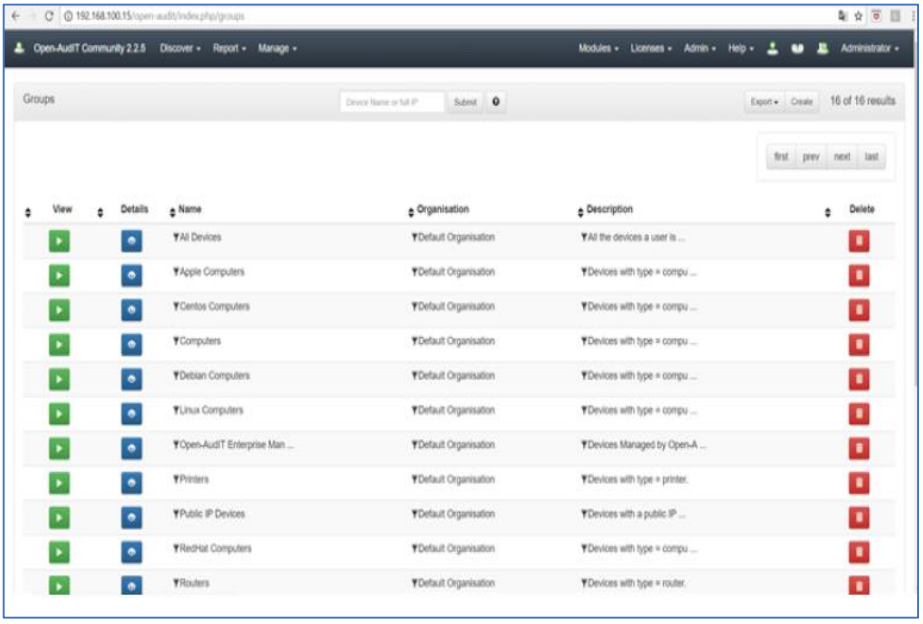
Finalmente aparece un mensaje donde dice que la instalación se completó.



Login:


192.168.100.15
OPMANTEK
Open-AudIT Enterprise
Open-AudIT


Open-AudIT
Username
admin
Password
Submit
No devices are in the database.
Initial login credentials are admin / password.
Please log in and change these ASAP.
Don't forget about the Open-AudIT wiki for all your documentation.
https://community.opmantek.com/display/OA/Home
Audit My PC


Open-AudIT Community 2.2.5
Discover
Report
Manage
Modules
Licenses
Admin
Help
Administrator
Groups
16 of 16 results
first
prev
next
last
View
Details
Name
Organisation
Description
Delete
All Devices
Default Organisation
Apple Computers
Centos Computers
Computers
Debian Computers
Linux Computers
Open-AudIT Enterprise Man ...
Printers
Public IP Devices
RedHat Computers
Routers

- **Monitorización de red LAN y Wireless.**

  Se vio conveniente implementar un procedimiento para el monitoreo, el cual se detalla a continuación:

  Modelo de procedimiento de monitoreo de redes

  Fundamentos: Se describirá el uso de las herramientas actuales para efectuar una constante vigilancia de la red, con la finalidad de detectar componentes defectuosos, e informar al inmediato superior.

  Objetivo: Asegurar que las redes funcionen en su óptimo rendimiento.

  Características:

  - **Administración:** Consiste en la planeación, diseño de la red, selección de infraestructura, instalación y administración de software y las políticas de seguridad.

    La administración del rendimiento se divide en 2 etapas: la de análisis y la de monitoreo.

  Procedimiento:

  - **Identificación de dispositivos:** Tales como: Routers, Modems, Servidores, Switchs, etc.
  - **Herramientas de monitores:** Se hará uso de las herramientas actuales como el programa PALO ALTO, con la configuración de alertas, seguimiento y evaluación permanente.
  - **Resultados:**
    - Reducir los tiempos de atención de los usuarios.

- Eliminación de la documentación física.
- Mayor control sobre los servicios.
- Mejorar tiempos de respuesta.
- Minimizar solicitudes de atención.

- **Proceso de Gestión de Incidencias:**
  - Primer nivel: Telefónico, remoto o presencial.
  - Segundo nivel: Asistencia de un proveedor.
- **Soluciones y cierre.**
  - **Pasarelas (gateway) y antivirus.**

    Se propone las siguientes características mínimas:
  - Capacidad de interconexión de redes heterogéneas.
  - Tipo asíncrono.
  - Traducción de direcciones (IP Maquerading)
  - 02 tarjetas de red.

- **Políticas para proxy.**

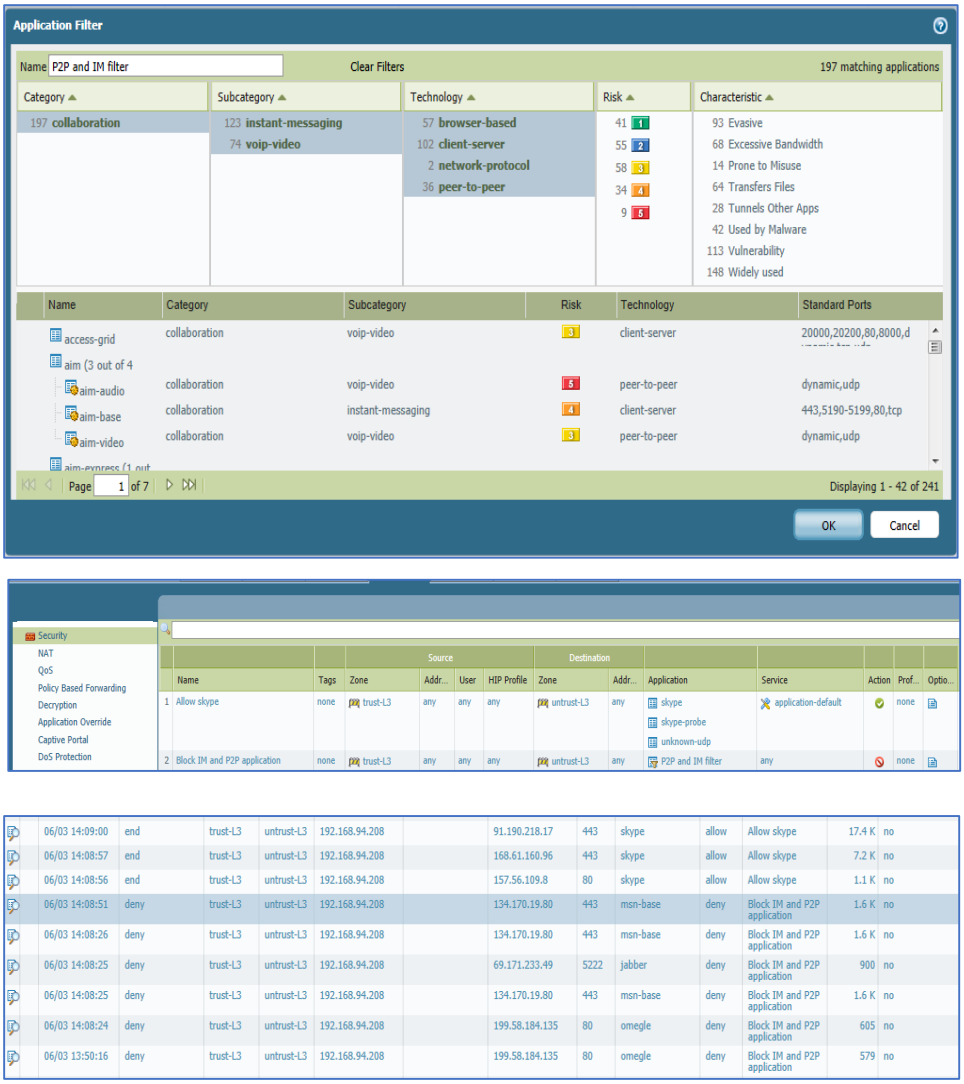
  Se implementó el tráfico basado en aplicaciones mediante la selección de opciones de filtrado

  Pasos

  Ir a objetos > filtro de aplicación

  Haga clic en Agregar para configurar un filtro de aplicación y P2P, a continuación: Categoría-colaboración, Subcategoría-mensajería instantánea + VoIP-video, Tecnología-basado en navegador + cliente-servidor + red-protocolo + peer-to-peer.

Figura 17: UNU – Configuración proxy



Directiva de seguridad generada contra Messenger, Chat de Google, Yahoo.

Trust-2-no Trust {de Trust-L3; de la fuente región de origen. a untrust-L3; destino; región de destino. usuario cualquier; Categoría; so/servicio [IRC-base/cualquie/cualquier/cualquier vidsoft/any/any/any SIP/any/any/cualquier h. 323/any/any/any **MSNbase**/cualquie/any/cualquiereBuddy/cualesquiera/cualesquiera/cualesquiera/cualesquiera/cualesquiera/cualquier Yahoo-

IM-base/cualesquiera/cualesquiera/cualquier Google-Talk-base/cualquier hovrs/Any/any Jabber/cualquie/any/cualquie QQ-base/cualquie/cualesquiera/cualquieAIMbase/cualquie/cualesquiera/cualquier ICQ/cualquier/cualquier/cualquie webaim/any/any/any Meebo-base/cualquie/cualquie/cualquie/cualquie/cualesquiera/cualesquiera/cualesquiera

chat/any/any/cualquie

Shape/any/any/any/cualquier/cualquier/cualquier

- **Registro de incidencias de copias de seguridad.**

Figura 19: UNU – Registro de incidencias de copias de seguridad

UNIVERSIDAD NACIONAL DE UCAYALI

OFICINA GENERAL DE TI SISTEMAS E INFORMATICA

FORMATO: REGISTRO DE INCIDENCIAS EN COPIAS DE SEGURIDAD

NRO	EQUIPOS	INCIDENCIA	PERSONAL REGISTRO	PERSONAL SOLUCION	FECHA	HORA	ACCIONES
1							
2							
3							

- **Registro de incidencias en telecomunicaciones.**

Figura 20: UNU – Registro de incidencias de equipos de telecomunicaciones

UNIVERSIDAD NACIONAL DE UCAYALI

OFICINA GENERAL DE TI SISTEMAS EINFORMATICA

FORMATO: REGISTRO DE INCIDENCIAS EN EQUIPOS DE TELECOMUNICACIONES

NRO	EQUIPOS	INCIDENCIA	PERSONAL REGISTRO	PROVEEDOR	PERSONAL SOLUCION	FECHA	HORA	ACCIONES
1								
2								
3								

4.2. UNIVERSIDAD NACIONAL INTERCULTURAL DE LA AMAZONIA - UNIA

4.2.1. INSTITUCIÓN

Universidad Nacional Intercultural de la Amazonía.

4.2.2. HISTORIA

Su creación fue el 10/12/1999 a través de la Ley Nº 27250, como consecuencia de la reivindicación de los pueblos de la Amazonía, gestionado por la Asociación Interétnica de la Selva Peruana – AIDESEP, para que los indígenas jóvenes contaran con la oportunidad de realizar una formación de nivel universitaria en distintas carreras profesionales, la sede que alberga la Ciudad Universitaria se ubica en el terreno del Instituto Lingüístico de Verano, ubicado en el Distrito de Yarinacocha, Provincia de Coronel Portillo, Región Ucayali.

4.2.3. DESCRIPCIÓN ACTUAL DE LA ARQUITECTURA

- **Personal de TI.**

Tabla N° 9:UNIA - Personal de TI

Cargo	Nombres y Apellidos	Especialidad
Jefe de oficina	Edeher Ponce Morales	Ingeniero de sistemas
Secretaria	Ketherine Lopez Vasquez	Secretaria
Analista	Isaac Abel Muñoz Gonzales	Ingeniero de sistemas
Soporte	Miguel Vasquez Moreno	Técnico informático
Soporte	Carlos Yngil Sanchez	Técnico informático

- **Producción y Desarrollo.**

  No cuenta con esta área.

- **Servidores.**

  3 TB disco duro, 128 GB de RAM, 2 procesadores Xeon 8 núcleos y de 10 núcleos.

  Equipos de seguridad: 2 hardware sophos XG(firewall perimetral).

  Servidor de dominio, servidor DNS, siaf y SIGA.

Tabla N° 10: UNIA - Servidor

Sistemas	Características
1. Aula Virtual UNIA 2. Sistema de Gestión Académica UNIA 3. Sistema de Registro de Resoluciones y Certificaciones UNIA 4. Sistema de Aula Virtual para el Centro de Idiomas UNIA 5. Sistema de Clases virtuales para Cepre-UNIA 6. Sistema de pruebas del aula Virtual UNIA 7. Sistema de pruebas Gestión Académica UNIA 8. Sistema de Inscripción del Examen de admisión 9. Sistema de Aula Virtual de Cepre-UNIA 10. Sistema Informativo de Cepre-UNIA 11. Sistema de Examen Virtual de admisión 12. Sistema Integrado de Seguimiento 13. Sistema de Repositorio de UNIA 14. Sistema de Revista de la UNIA 15. Sistema de Servicios Académicos antiguo 16. Sistema de Dirección de Bienestar Universitario 17. Sistema de Gobierno Electrónico de la UNIA 18. Sistema de Proyectos de Investigación y Desarrollo	- Sistema Operativo: WINDOWS SERVER 2012 R2. - Lenguaje de Programación: PHP. - Framework: LARAVEL - Memoria RAM Asignado en el Servidor: 16 gb. - Base de Datos: MARIA DB 10.2 - Velocidad de Transferencia de Datos 100/1000. - Compatibilidad: Es multiplataforma, responsive. - Dominio: unia.edu.pe y sus sub dominios.

- **Hardware del centro de datos.**

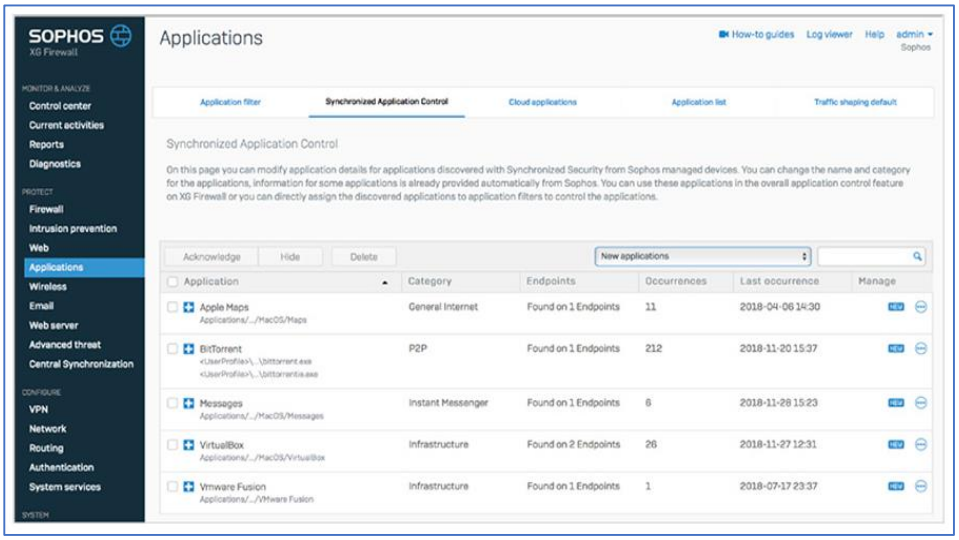
Tabla N° 11: UNIA – Hardware Centro de datos

Marca	Modelo	Procesador	RAM	HDD
Lenovo	Lenovo System X 3650 M5 procesador xeon 2.60GHz	procesador xeon 2.60GHz	128 GB de memoria ram	3TB de disco duro
Lenovo	Lenovo ThinkSystem SR630 procesador xeon 2.60GHz	procesador xeon 2.60GHz,	128 GB de memoria ram	3TB de disco duro

- **Servidor proxy**

  Cuenta con el sistema Sophos, donde posee la configuración necesaria para el proxy de la institución.

Figura 21: UNIA – Sophos



- **Sistema de Almacenamiento.**

  No cuentan con un sistema de almacenamiento configurado.

- **Proveedores y socios.**

  Como toda entidad es indispensable que la UNIA posee una relación y/o vínculo con sus proveedores de servicios, como es el paso para TI; pero no se cuenta con un control registrado, ni físico, ni digital de los proveedores.

- **Interconexión estratégica con otras instituciones.**

  No posee servicios de interconexión con otras entidades.

- **Flujos de trabajo.**

  La OTI, no cuenta con el diagrama de flujos de trabajo respecto a la seguridad perimetral.

- **Políticas, procedimiento de seguridad perimetral.**

  La UNIA no cuenta con políticas y/o procedimientos sobre seguridad perimetral.

- **Reuniones de difusión de políticas.**

  Al no contar con políticas y/o procedimientos, no se realiza esta actividad.

- **Reuniones sobre Gestión de la Seguridad.**

  No se realizan estas actividades por no contar con un Sistema de Gestión de la Seguridad de la Información.

- **Cooperación de los gerentes sobre Seguridad de la Información.**

  No se realiza esta actividad por no contar con un Sistema de Gestión de la Seguridad de la Información.

- **Registro y control de acceso sobre la seguridad perimetral.**

  No se lleva un registro para el control de acceso.

- **Gestión de claves de acceso para la seguridad perimetral.**

  No existe una política y/o procedimiento para la gestión de claves de acceso

- **Sistema biométrico para acceso.**

  No se cuenta con este tipo se sistema.

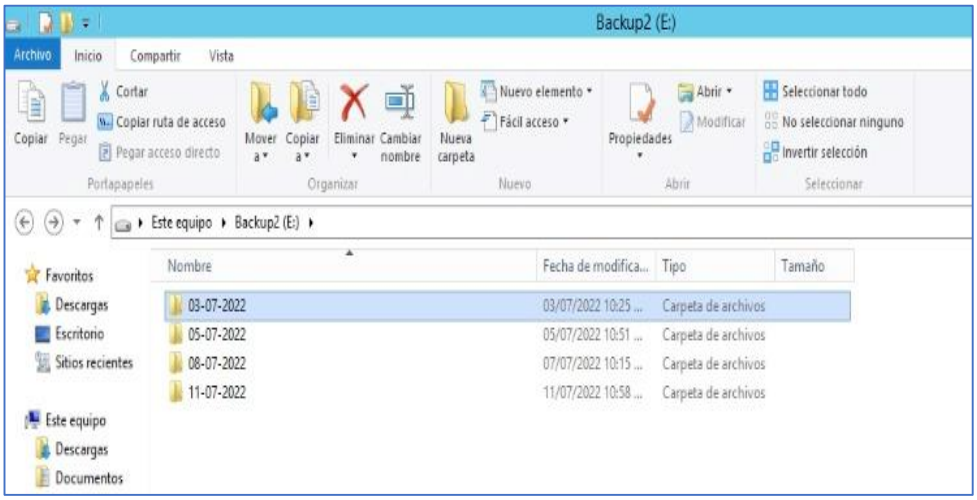
- **Registro de acceso al personal interno.**

  No se lleva el registro.

- **Respaldo de base de datos.**

  Se realizan respaldos de base de datos.

Figura 22: UNIA – Respaldos



- **Contingencias a nivel físico.**

  Únicamente redundancia de UPS, de Firewall Shopos.

- **Contingencias a nivel lógico.**

  Solo se realizan copias de seguridad, mas no se cuenta con una solución de contingencia.

- **Acceso a Internet.**

  Cuenta con servicio de internet dedicado de 100 Mb de velocidad, es decir al 100% de su velocidad de transferencia de subida y bajada, sin redundancia.

- **Acceso a Intranet.**

  No cuenta con intranet.

- **Extranet.**

  No cuenta con extranet.

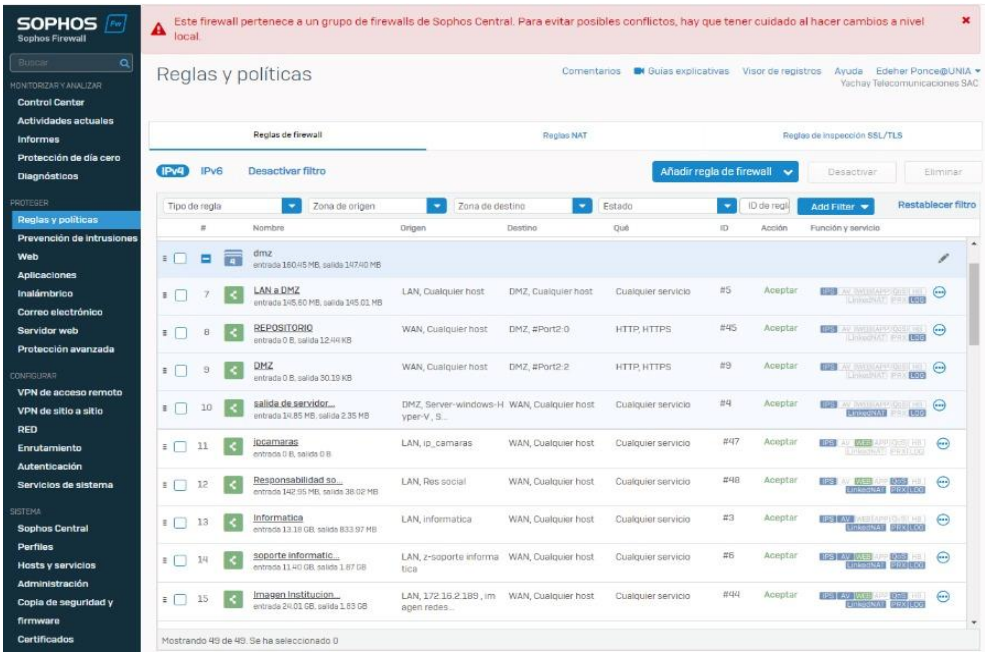
- **Verificación de IP salientes, entrantes.**

  No se realiza esta actividad.

- **Firewall Internet.**

  Sophos

Figura 23: UNIA – Firewall Internet



- **Firewall Extranet.**

  No cuenta.

- **Sistema de auditoría.**

  No cuenta con un componente de auditoría.

- **Monitorización de tráficos en la LAN.**

  Esta actividad no se realiza.

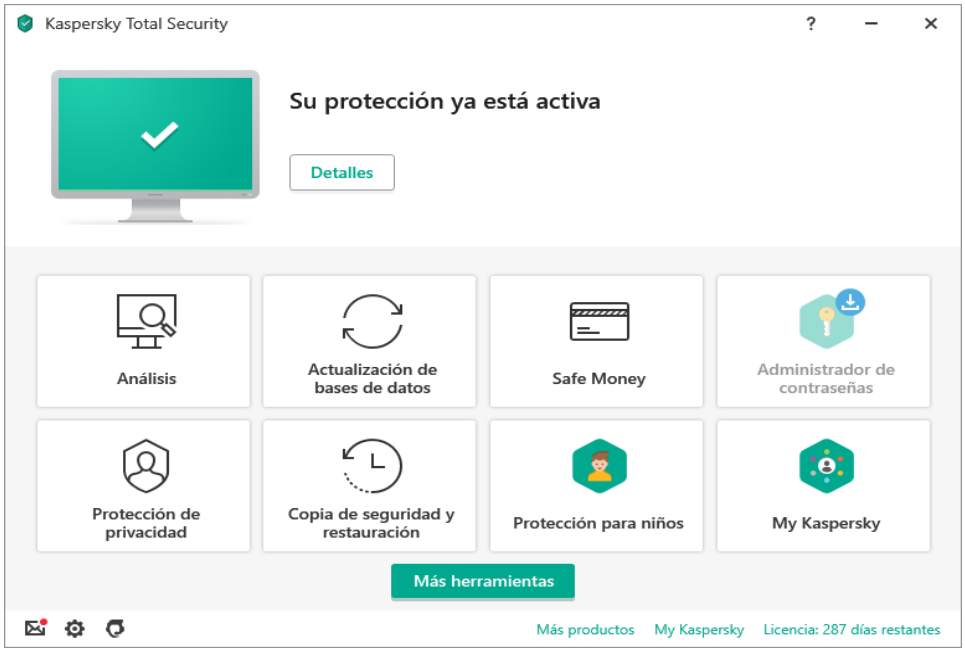
- **Monitorización de tráficos en la red Wireless.**

  Esta actividad no se realiza.

- **Pasarelas y antivirus.**

  Si se realiza a través del antivirus Kaspersky.

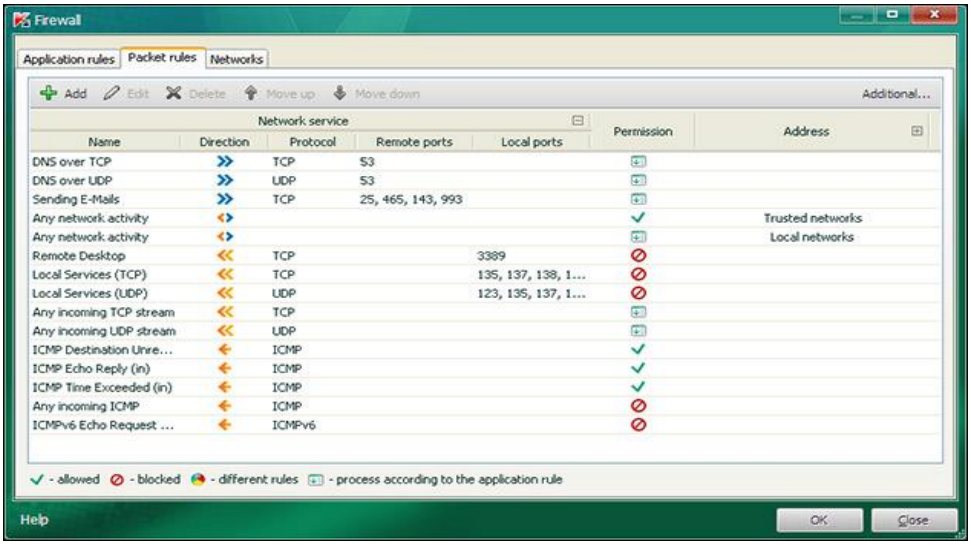
Figura 24: UNIA – Kaspersky



- **Testeo de DNS y DNS Blocklist.**

  Se realiza a nivel intermedio a través del firewall y antivirus.

Figura 25: UNIA – Firewall kaspersky



- **Servidores proxy.**

  No cuenta con servidor proxy.

- **Registro del personal externo.**

No se lleva el registro del personal externo que ingresas a las instalaciones relacionados con la seguridad perimetral.

- **Registro de indecencias de copias de seguridad.**

  No se lleva el registro de incidencias de copias de seguridad.

- **Registro de incidencias en telecomunicaciones.**

  No se lleva el registro de incidencias en telecomunicaciones.

4.2.4. PROPUESTA DE SOLUCIÓN E IMPLEMENTACIÓN DE SOLUCIÓN.

- **Área de producción y desarrollo.**

  El área deberá contar con las siguientes funciones básicas:

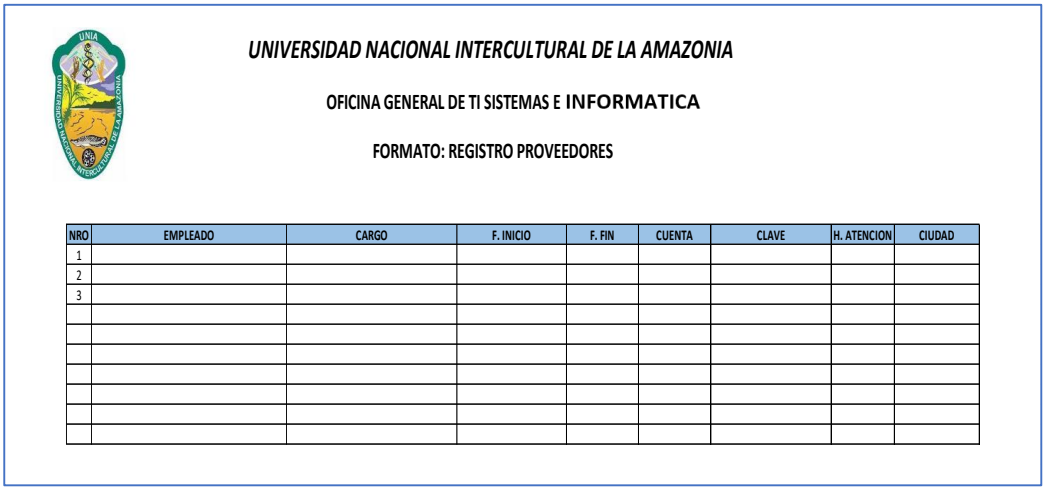
  - **Desarrollo de Sistemas Informáticos**

    Para procesamiento de la información, disminuir las laborares de las áreas actuales con el objeto de realizar las tareas en menos tiempo posible, contar con 03 personales administrativos (Analista y desarrolladores), se crearán e implementaran los sistemas informáticos de acuerdo a las necesidades, cumpliendo las etapas del ciclo de desarrollo, manejaran frameworks, realizaran la documentación de los sistemas, etc, se encontrarán bajo a la supervisión del jefe del Área de Informática.

- **Implementación registro de proveedores.**

  Se implementó el registro de control de los proveedores.

Figura 26: UNIA – Registro de proveedores



UNIVERSIDAD NACIONAL INTERCULTURAL DE LA AMAZONIA

OFICINA GENERAL DE TI SISTEMAS E INFORMATICA

FORMATO: REGISTRO PROVEEDORES

NRO	EMPLEADO	CARGO	F. INICIO	F. FIN	CUENTA	CLAVE	H. ATENCION	CIUDAD
1								
2								
3								

- **Interconexión con otras instituciones.**

  Reniec: Servicios como:

  - Consulta en línea, vía internet.
  - Verificación Biométrica.
  - Cotejo Masivo.

  Servicios de Bancos.

  - Para pagos de los servicios de UNIA a través de la plataforma online.
  - Pagos de servicios de UNIA a través de tarjetas de crédito o débito.

- **Procedimiento para control perimetral.**

  Se implementó la siguiente política.

PROCEDIMIENTO SEGURIDAD PERIMIMETRAL

Código del proceso	
Nombre del proceso	
Objetivo del proceso	
Nombre del proceso	
Responsable	

	Órgano / Unidad Orgánica	Firma y sello
Elaborado por:		
Revisado por:		
Aprobado por:		
Fecha:		

DESCRIPCIÓN DEL PROCEDIMIENTO:

1: Gestión de acceso a los Cuartos de Comunicaciones:

N°	Descripción de la actividad	Responsable	Puntos de Control / Observaciones	Documentos que se generan
1	Otorgar, al personal, roles de Administración de los Cuartos de Comunicaciones.	Jefe	**Punto de Control:** Definir funciones de acuerdo a perfiles y competencias.	Informe
2	Registrar el permiso diligenciado en el "Formato de acceso permanente al Centro de Datos y los Cuartos de Comunicaciones" (anexo 1).	Jefe	Punto de Control: Verifica que se asignen privilegios según las funciones.	Informe.
3	Comunicar a la OGA y la RRHH , la autorización de ingreso en horario no laboral en casos de emergencia a los Cuartos de Comunicaciones.	Jefe		Informe
4	Realizar las tareas de administración, monitoreo, mantenimiento en los Cuartos de Comunicaciones de acuerdo al rol. Registrar en "Bitácora de Acceso" (Anexo 2).	Personal de TI	**Punto de Control:** Director/a de la Oficina de Tecnologías de la Información debe verificar periódicamente el diligenciamiento de la Bitácora de Acceso y los fines de los accesos.	Bitácora
5	Solicitar autorización de acceso al a los Cuartos de Comunicaciones a personal no autorizado, (funcionario, tercero, y/o contratista), diligenciar el formato "Autorización Acceso a los Cuartos de Comunicaciones" **(Anexo 3)**.	Personal de TI		
6	Autorizar o denegar el ingreso de personal previa evaluación.	Jefe		Bitácora
7	Elaborar informe mensual de actividades realizadas en los Cuartos de Comunicación y gestión de aseguramiento de los servicios de red.	Personal de TI		

FORMATO DE PROCEDIMIENTOS

ANEXO 1. Formato de acceso permanente a los Cuartos de Comunicaciones

Fecha de autorización:	**Día:**	**Mes:**	**Año:**
Firma:	**Firma:**		
Nombre:	**Nombre:**		
Oficina General de Estadística e Informática	**Oficina de Tecnología de la Información**		

Nº	**Datos del personal autorizado**
	Nombre completo: DNI: **Cargo:** **Rol:** **Teléfono Móvil:** **Anexo:**

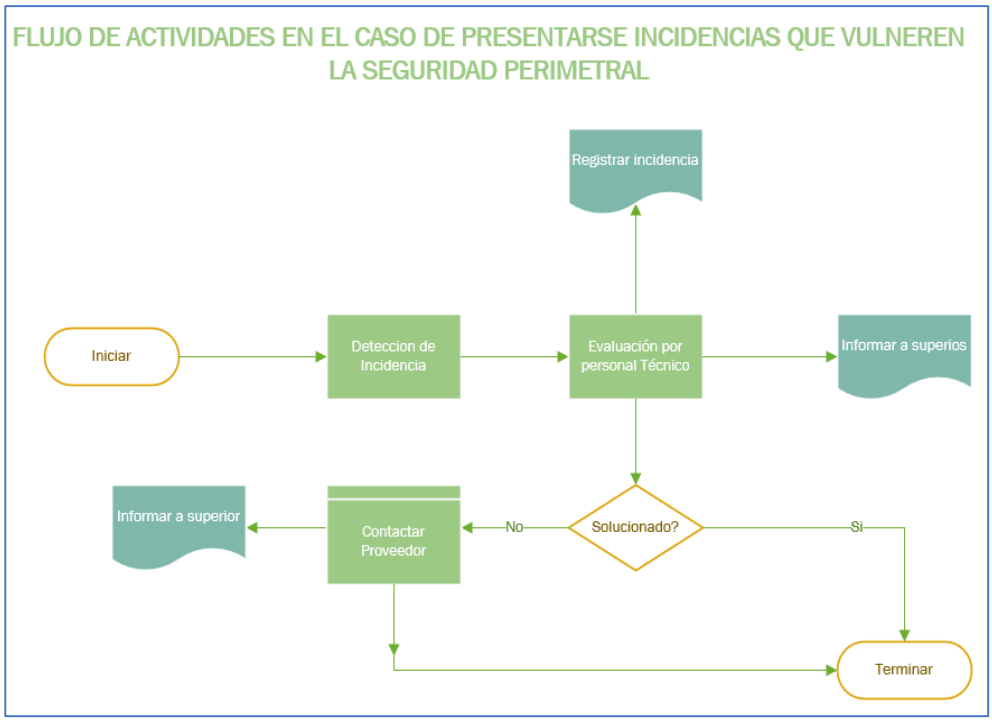
ANEXO 2. Bitácora de acceso al Centro de Datos y Cuartos de Comunicaciones

Fecha	DNI/RUC	Nombre y Apellidos	Empresa / Oficina	Labor a realizar	Hora de Ingreso	Hora de Salida	Autoriza	Firma

- **Flujos de trabajo, procedimiento.**

  Flujo de trabajo

Figura 27: UNIA – Flujo de actividades



- **Reuniones de difusión de políticas y/o procedimientos.**

  Es recomendable realizar reuniones de difusión de políticas y/o procedimiento en los siguientes casos:

  - Personal nuevo en el área.
  - Posterior a la una actualización del procedimiento y/o política.
  - Al crearse una nueva política y/o procedimiento.
  - Dos veces por año en los siguientes meses:
    - Abril.
    - Octubre.

- **Conformación de un comité de seguridad de la información (SGSI).**

  Este Comité estará comprometido en la elaboración de las estrategias y mejoras en lo que concierne la seguridad de la

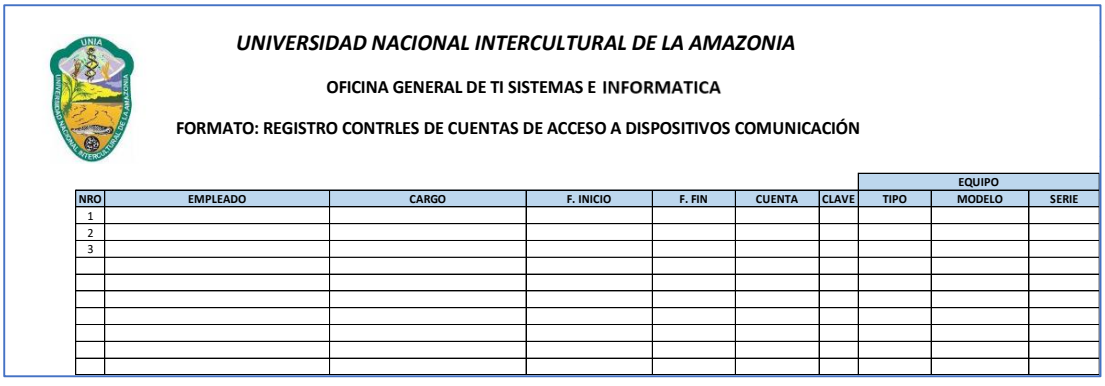
información. Estará integrado por personal de alta dirección jefaturas o direcciones.

Funciones:

- Precisar las políticas sobre seguridad de la información alineados con el Plan Estratégico Organizacional.
- Mantenimiento de los productos del SGSI.
- Identificación de riesgos respecto al SGSI.
- Adecuación del SGSI.
- Suministrar los recursos relacionados con el SGSI.
- Evaluación de las vulnerabilidades sobre lo implementado.
- Monitorear el SGSI.
- Concientización sobre el SGSI.

- **Registro de control de cuentas de acceso sobre equipos seguridad perimetral.**

Figura 28: UNIA – Registro de cuentas de acceso a dispositivos de comunicación



UNIVERSIDAD NACIONAL INTERCULTURAL DE LA AMAZONIA

OFICINA GENERAL DE TI SISTEMAS E INFORMATICA

FORMATO: REGISTRO CONTRLES DE CUENTAS DE ACCESO A DISPOSITIVOS COMUNICACIÓN

							EQUIPO		
NRO	EMPLEADO	CARGO	F. INICIO	F. FIN	CUENTA	CLAVE	TIPO	MODELO	SERIE
1									
2									
3									

- **Sistema biométrico para acceso a las instalaciones.**

Se propone implementar una adecuación para el ambiente del centro de datos que cuente con reforzamiento de las paredes, sellado, que posee aires acondicionados de precisión, falso piso, falso techo, tablero eléctrico, alarmas de acceso, contra

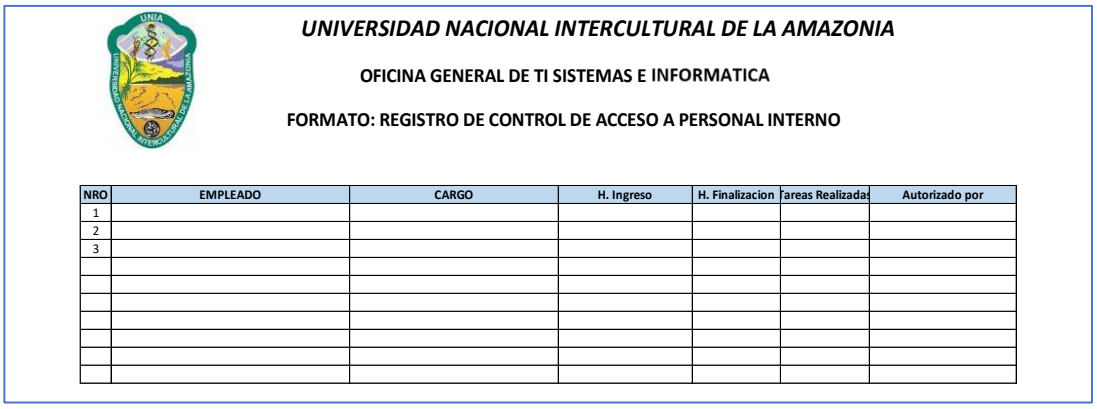
incendios, pasillos fríos-calientes y a nivel de la puerta de acceso implementar un sistema biométrico con las siguientes características mínimas:

Tabla N° 12: UNIA – Características del control de acceso.

Características	Valores
Biométrico	Huella
Tarjeta y Protocolo LF/HF	Dual RFID, MultiCLASS SE y Dual RFID
Max Usuarios	10 000
Tcp/Ip	Si
Usb	No
CPU	1,0Ghz
Memoria	8Gb
LED	Multicolor
Alimentación	12VDC
Tecnología	Huella dactilar

- **Registro de acceso al personal interno**

Figura 29: UNIA – Registro de control de acceso personal interno



UNIVERSIDAD NACIONAL INTERCULTURAL DE LA AMAZONIA

OFICINA GENERAL DE TI SISTEMAS E INFORMATICA

FORMATO: REGISTRO DE CONTROL DE ACCESO A PERSONAL INTERNO

NRO	EMPLEADO	CARGO	H. Ingreso	H. Finalizacion	Tareas Realizadas	Autorizado por
1						
2						
3						

- **Registro de copias de seguridad.**

Se implementó un registro para llevar el control de las copias de seguridad realizados.

Figura 30: UNIA – Registro backup

UNIVERSIDAD NACIONAL INTERCULTURAL DE LA AMAZONIA

OFICINA GENERAL DE TI SISTEMAS E INFORMATICA

FORMATO: REGISTRO DE INCIDENCIAS EN COPIAS DE SEGURIDAD

NRO	EQUIPOS	INCIDENCIA	PERSONAL REGISTRO	PERSONAL SOLUCION	FECHA	HORA	ACCIONES
1							
2							
3							

- **Contingencia a nivel Físico.**

  Se recomienda implementar servidores de contingencia, equipos de comunicación, sistemas contra incendios y climatización.

- **Contingencia a nivel Lógico.**

  Se recomienda lo siguiente:

  Adquirir software para replicación en tiempo real como MIMIX.

- **Respaldo de conexión de internet.**

  Para garantizar el acceso a internet es recomendable que se instale una redundancia de interconexión, reescribiendo un nuevo contrato con el operador.

  La conexión de backup deberá tener las siguientes características.

  - El sistema Backup debe ser de Fibra Óptica y/o 4G.
  - Permite la conexión a internet a todos los equipos y/o dispositivos.

- El ancho de banda debe ser el mismo que de la interconexión principal, así como los valores para subir y descargar.

- **Intranet – filtrado de tipos de archivos.**

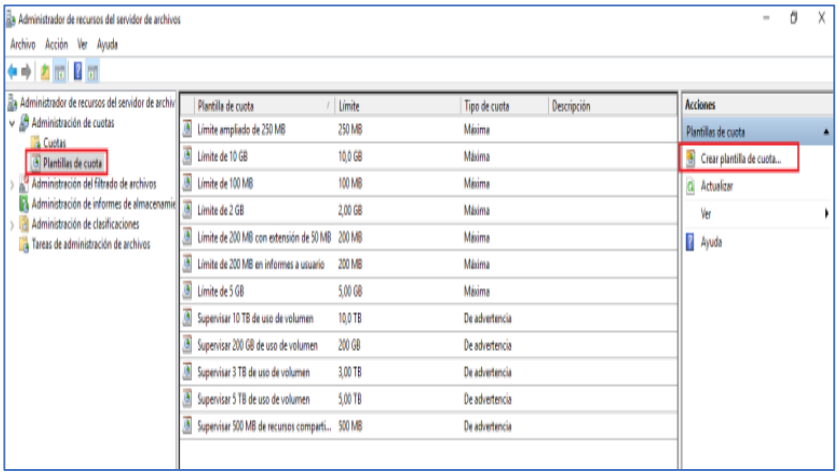
  Intranet. Para la intranet se requiere: gestión de contenidos (File Server), con filtrado de archivos y cuotas de almacenamiento para usuarios, así como del desarrollo de una GUI. Debido a la naturaleza del desarrollo de Software para la GUI de la intranet, podría corresponder a otra investigación, en esta investigación, y con la coordinación del jefe del Área, únicamente se implementó la base del almacenamiento con los filtros y cuotas, en su Servidor de producción el cual posee un SO Windows Server 2012 R2, siguiendo los pasos que a continuación se muestran:

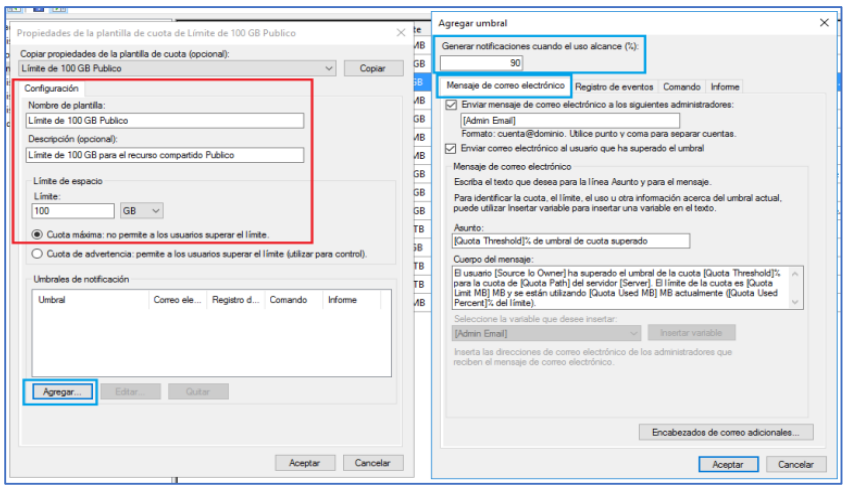
  - **Recursos Compartidos Público:** Todos los usuarios del AD podrán tener el acceso de lectura y escritura con una cuota de 100 GB.
  - **Recursos Compartidos Grupos:** Alojará las carpetas o UO de las áreas Administrativas, con una cuota de 50 GB.

- **Recursos compartidos Usuarios:** Información personal de cada usuario del AD, cuota de 25 GB

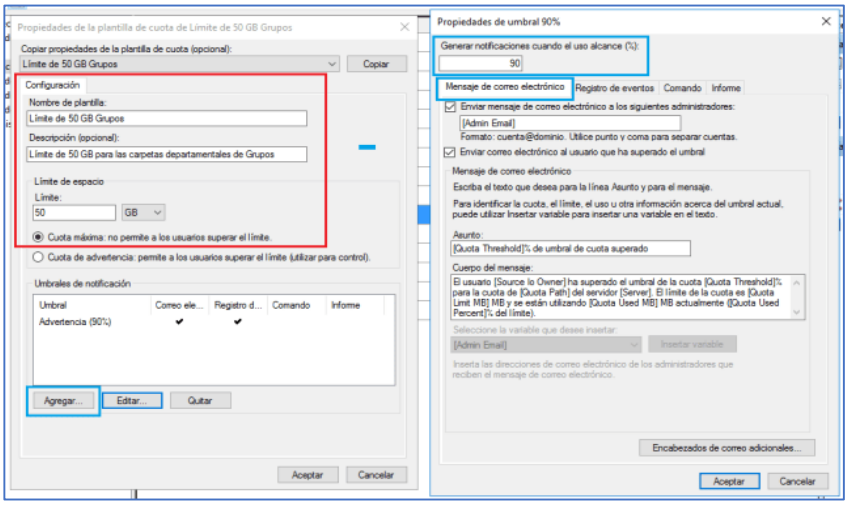


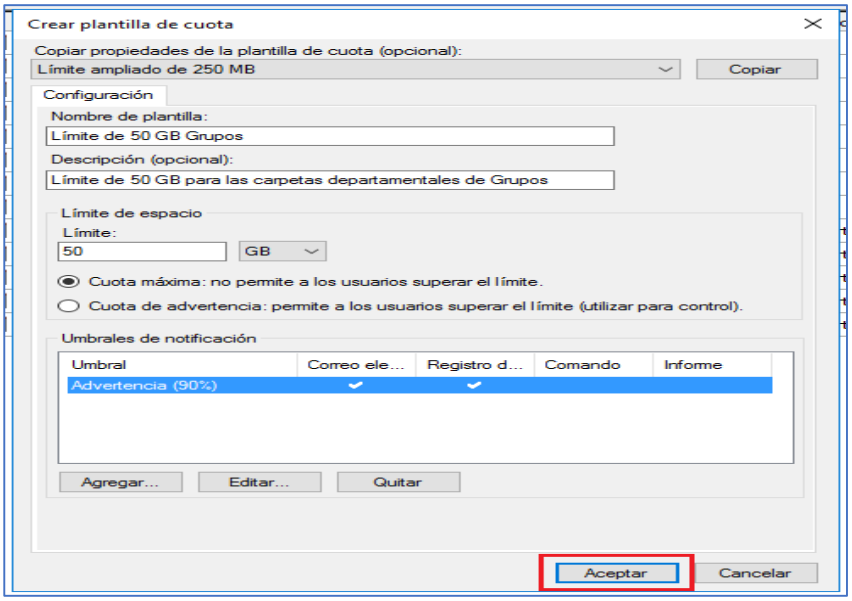
- En cuota, iniciamos por la cuota del recurso compartido Publico:



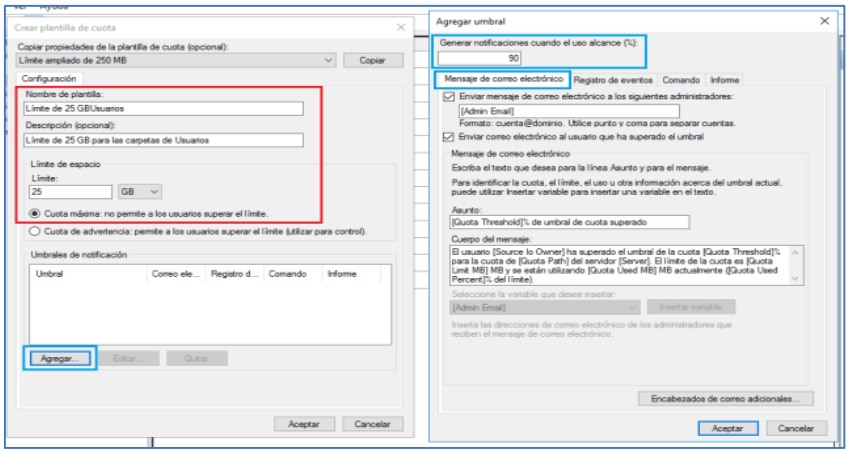


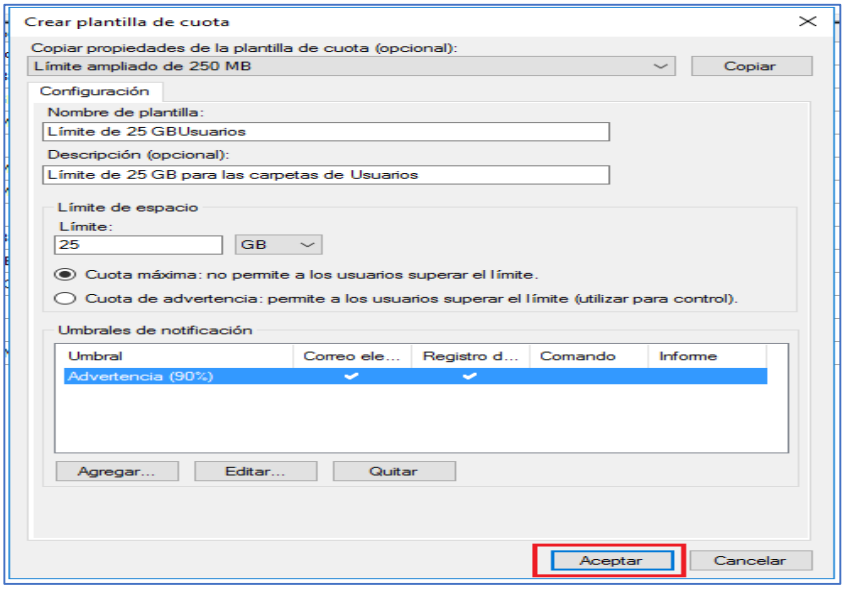
- Para las carpetas administrativas de Grupos, el límite en 50 GB y el visor de eventos cuando alcance el 90% de la capacidad:



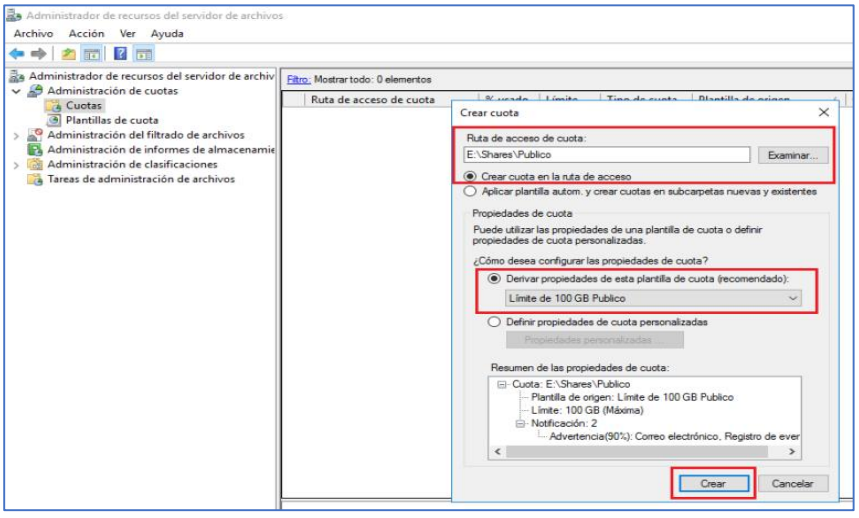


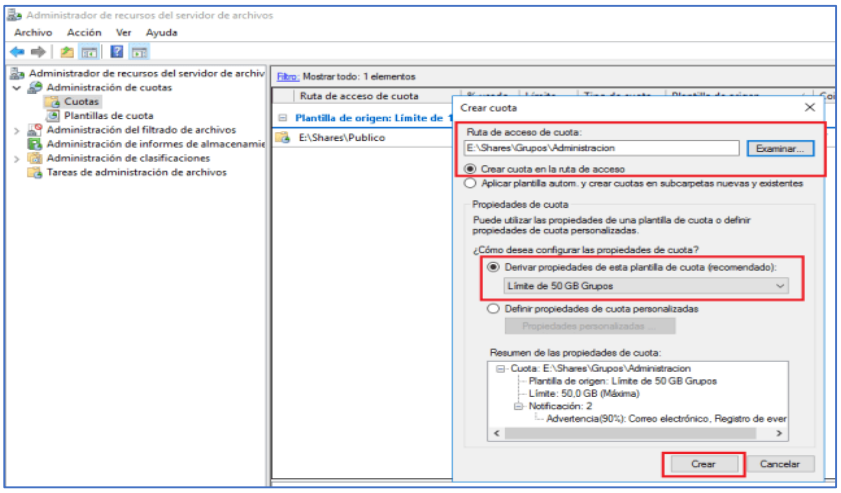
- Configuración de las carpetas personales de los usuarios 25 GB.





- La cuota para el recurso compartido Público.





- **Extranet – características.**

  Debido a la finalidad de la UNIA se recomienda implementar una extranet académica con los siguientes requerimientos mínimos:

  - Ingreso al sistema: Generar su acceso mediante el ingreso de su correo personal - Actualizar sus datos personales - Cambiar su contraseña - El personal administrativo ingresará mediante su cuenta de dominio.
  - Acceso a la información académica del estudiante: Notas - Unidades didácticas matriculadas - Inasistencias - Horario de clases - Record Académica - Avance curricular.
  - Acceso a deudas y pagos: Realizar pagos en línea, mediante una pasarela con visa - Visualizar sus pagos efectuados y pagos pendientes.
  - Gestión de la información del docente: Visualizar sus unidades didácticas - Visualizar su horario - Visualizar su asistencia - Visualizar documentos.

- Capacitación docente: Realizar la gestión de flyers - Gestión docentes - Gestión estudiantes - Gestión Documentos.
- Medio de comunicación académica: El personal administrativo podrá realizar el envío de mensajes y notificaciones a los estudiantes y profesores.

  Gestión de documentos, capacitaciones y eventos.

- **Firewall para Extranet.**

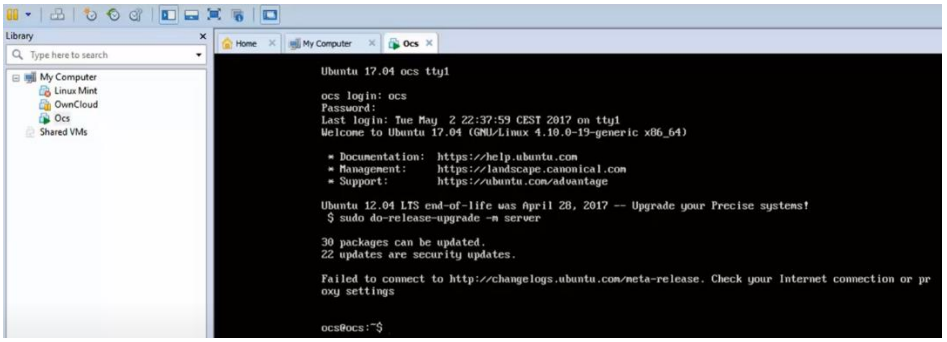
  Se recomienda un firewall que cumpla con las siguientes características mínimas:

  - Filtrado de las direcciones de IP de destino y de origen.
  - Gestión de protocoles TCP o UDP.
  - Filtrado de puertos.
  - Uso de flags en las cabeceras de TCP.
  - Filtrado de direcciones.

- **Sistema para auditoria.**

  Se implementó una pc con software libre de SO Ubuntu y el software de auditoria OCS Inventory en un entorno virtual de VMware Workstation. A continuación, se presentan capturas del proceso de instalación realizado.

  - Acceder a la MV de Ubuntu



- Verificación salida a internet.

```
ocs@ocs:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.136  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe8a:942  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:8a:09:42  txqueuelen 1000  (Ethernet)
        RX packets 357  bytes 459827 (459.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 308  bytes 28193 (28.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 358  bytes 26790 (26.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 358  bytes 26790 (26.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ocs@ocs:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=600 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=57 time=692 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=57 time=392 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=57 time=407 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4085ms
rtt min/avg/max/mdev = 392.390/523.317/692.657/127.682 ms
```

- Acceder al editor vi.

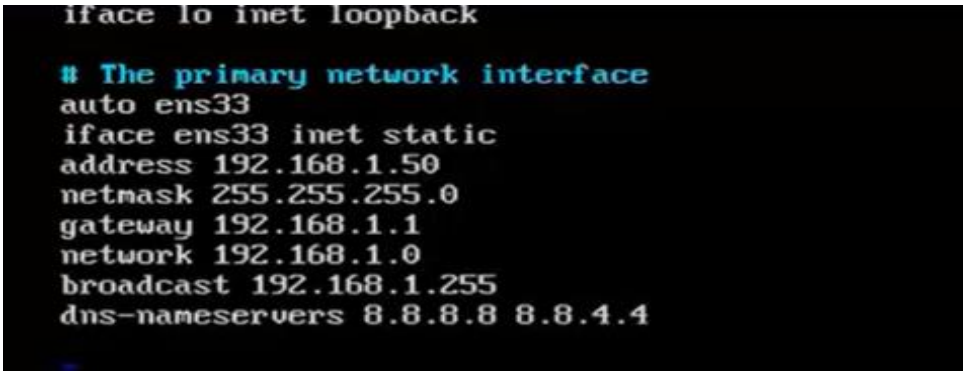
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

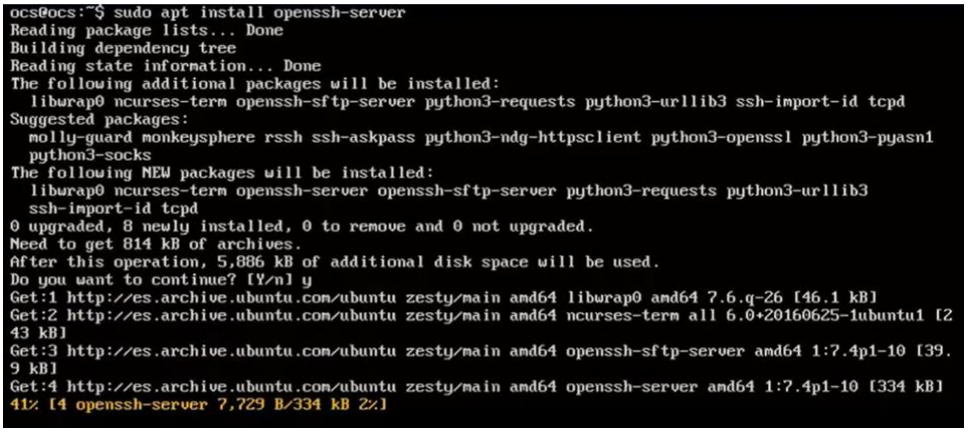
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens33
iface ens33 inet dhcp
~
~
~
~
```

- Configurar la red.



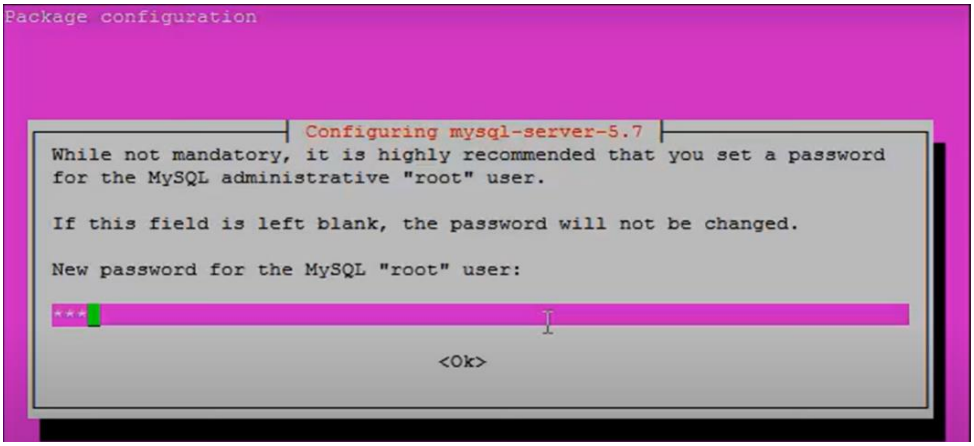
- Instalar el servidor.



- Instalar dependencias.



- Configurando usuarios root de mysql.



- Crear la BD.

```
ocs@ocs:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.7.18-0ubuntu0.17.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

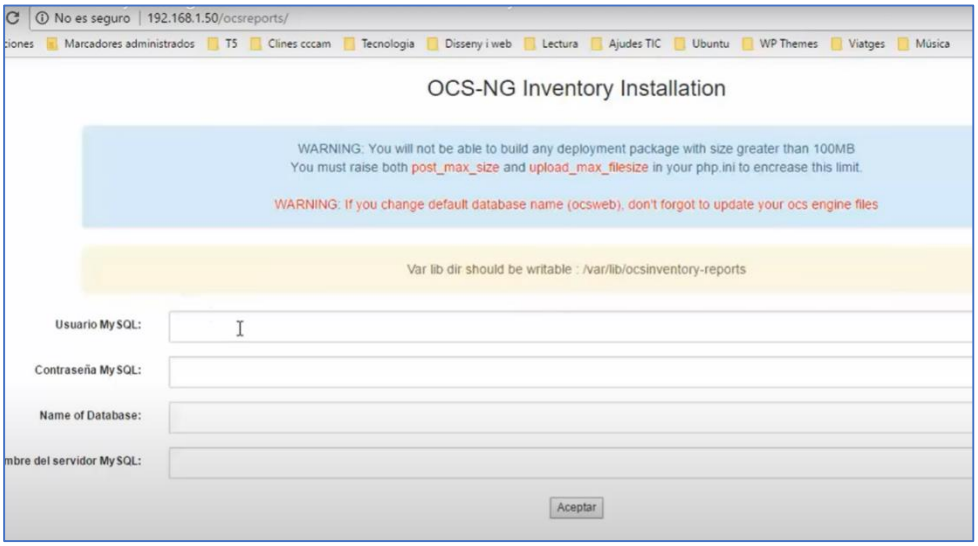
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE DATABASE ocweb
    -> DEFAULT CHARACTER SET utf8
    -> DEFAULT COLLATE utf8_general_ci;
```

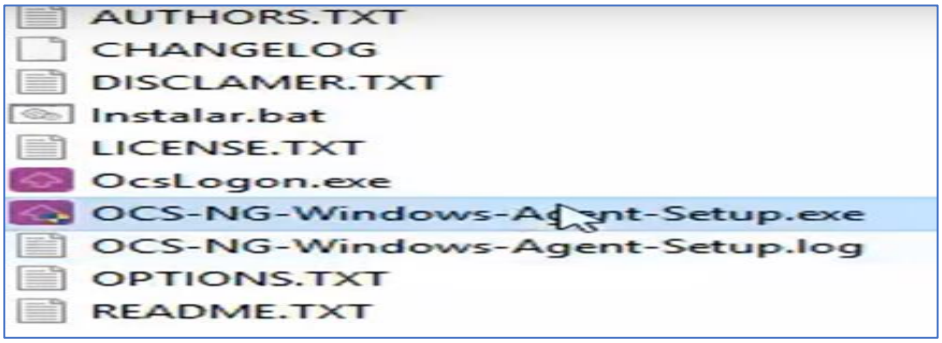
- Reiniciar el servidor apache.

```
root@ocs:~/ocs/OCSNG_UNIX_SERVER-2.3.1# cd /etc/apache2/conf-available/
root@ocs:/etc/apache2/conf-available# ls -l
total 44
-rw-r--r-- 1 root root   315 Dec  8 10:10 charset.conf
-rw-r--r-- 1 root root  3224 Dec  8 10:10 localized-error-pages.conf
-rw-r--r-- 1 root root  4157 May  2 23:35 ocsinventory-reports.conf
-rw-r--r-- 1 root root   189 Dec  8 10:10 other-vhosts-access-log.conf
-rw-r--r-- 1 root root  2174 Dec  8 10:10 security.conf
-rw-r--r-- 1 root root   455 Dec  8 10:10 serve-cgi-bin.conf
-rw-r--r-- 1 root root 13468 May  2 23:35 z-ocsinventory-server.conf
root@ocs:/etc/apache2/conf-available# ln -s /etc/apache2/conf-available/ocsinven
tory-reports.conf /etc/apache2/conf-enabled/
root@ocs:/etc/apache2/conf-available# ln -s /etc/apache2/conf-available/z-ocsinv
entory-server.conf /etc/apache2/conf-enabled/
root@ocs:/etc/apache2/conf-available# cd ..
root@ocs:/etc/apache2# cd conf-enabled/
root@ocs:/etc/apache2/conf-enabled# ls
charset.conf                 security.conf
localized-error-pages.conf   serve-cgi-bin.conf
ocsinventory-reports.conf    z-ocsinventory-server.conf
other-vhosts-access-log.conf
root@ocs:/etc/apache2/conf-enabled# service apache2 restart
```

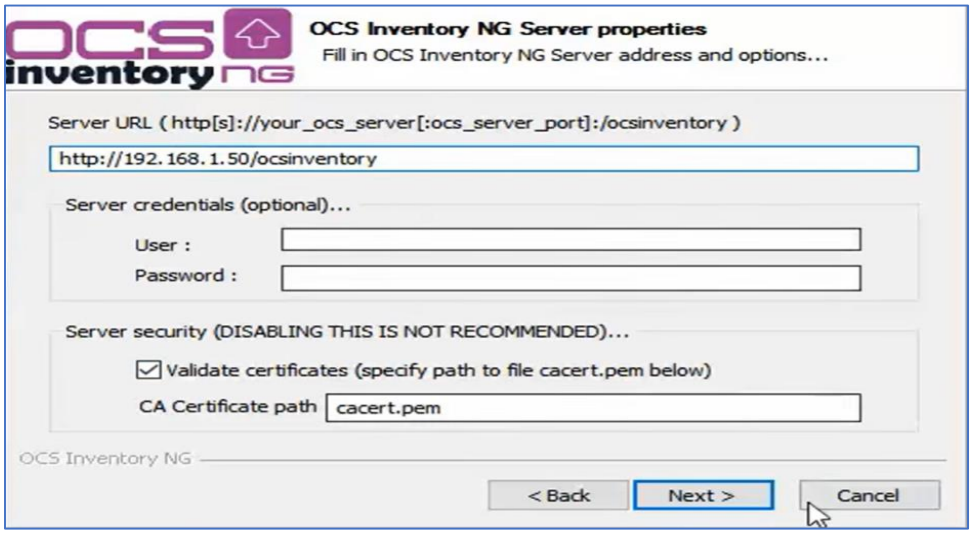
- Acceder a la web.

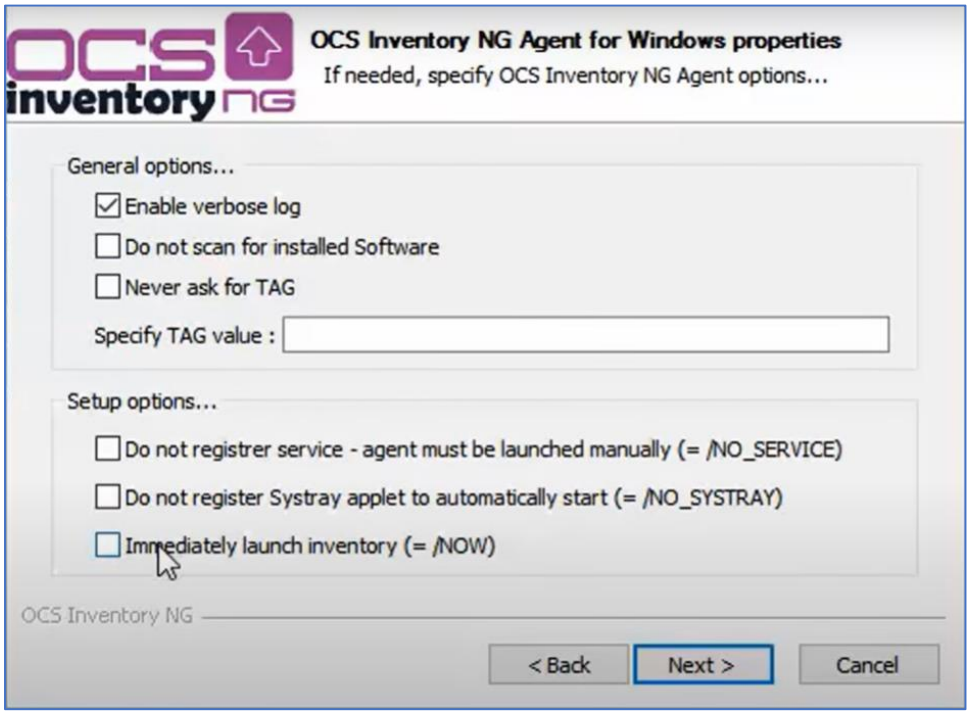


- Instalar agente para Windows.

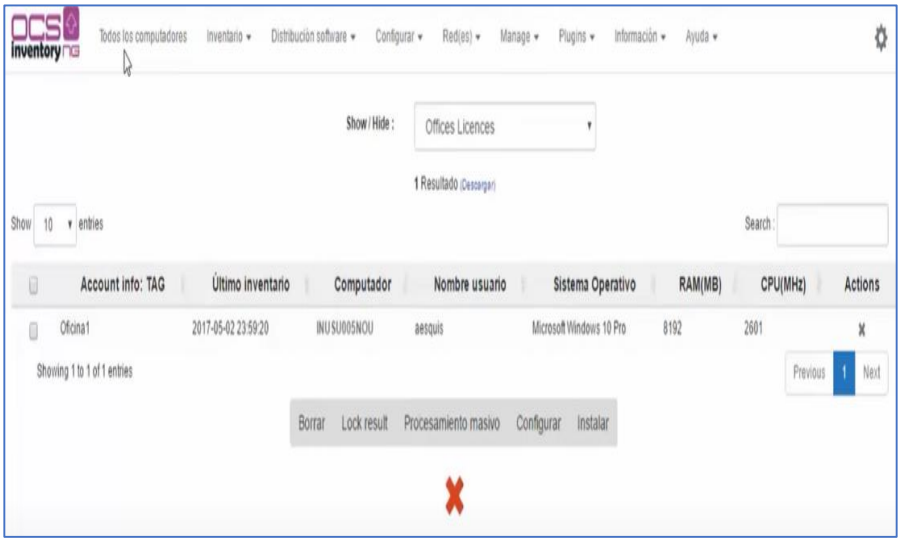


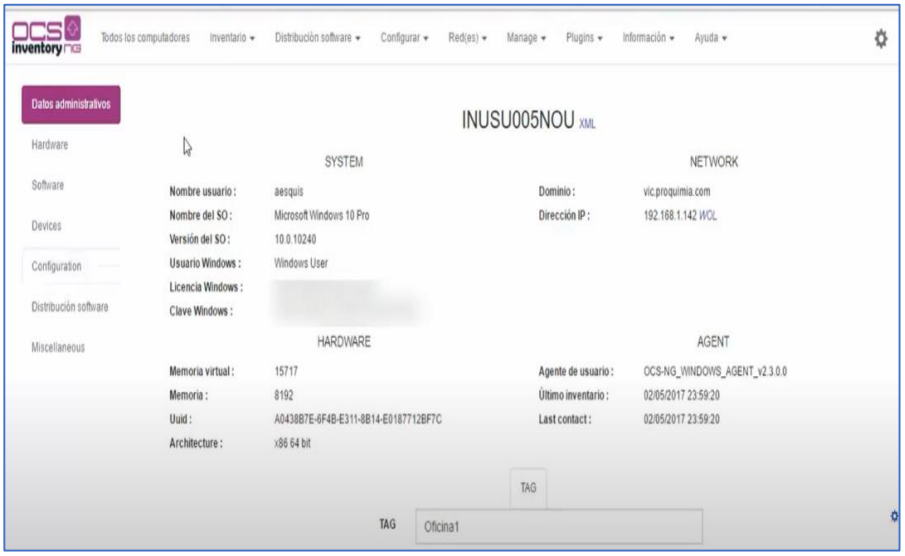
- Configurar servidor.

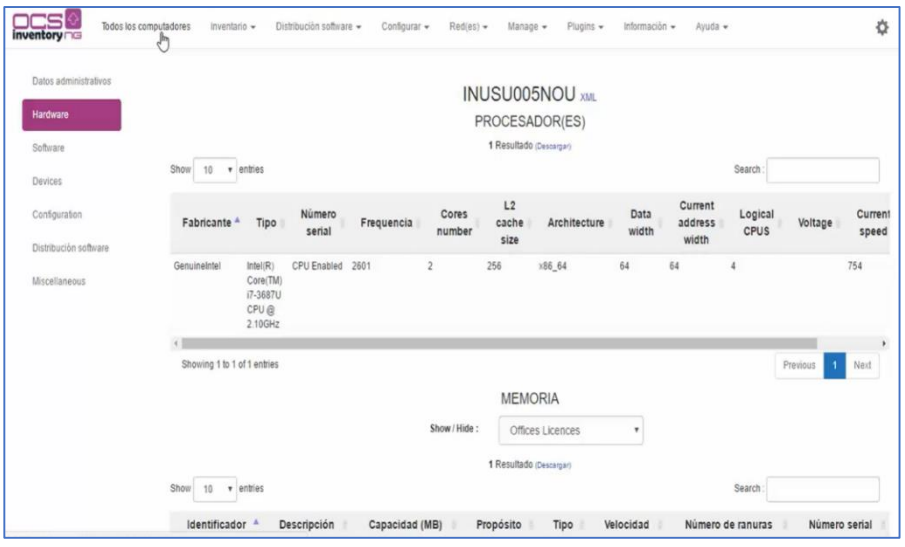




- Acceder al servidor y hacer una prueba.







- **Monitorización de red LAN y Wireless.**

  Se vio conveniente implementar un procedimiento para el monitoreo, el cual se detalla a continuación:

Modelo de procedimiento de monitoreo de redes

Fundamentos: Se describirá el uso de las herramientas actuales para efectuar una constante vigilancia de la red, con la finalidad de detectar componentes defectuosos, e informar al inmediato superior.

Objetivo: Asegurar que las redes funcionen en su óptimo rendimiento.

Características:

- **Administración:** Consiste en la planeación, diseño de la red, selección de infraestructura, instalación y administración de software y las políticas de seguridad.

  La administración del rendimiento se divide en 2 etapas: la de análisis y la monitoreo.

Procedimiento:

- **Identificación de dispositivos:** Tales como: Routers, Modems, Servidores, Switchs, etc.
- **Herramientas de monitores:** Se hará uso de las herramientas actuales como el programa PALO ALTO, con la configuración de alertas, seguimiento y evaluación permanente.
- **Resultados:**
  - Reducir los tiempos de atención de los usuarios.

- Eliminación de la documentación física.
- Mayor control sobre los servicios.
- Mejorar tiempos de respuesta.
- Minimizar solicitudes de atención.

- **Proceso de Gestión de Incidencias:**
  - Primer nivel: Telefónico, remoto o presencial.
  - Segundo nivel: Asistencia de un proveedor.
- **Soluciones y cierre.**

- **Registro de acceso al personal externo**

  Se implementó un registro para el control del personal externo que ingresa a realizar actividades relacionadas con la seguridad perimetral.

Figura 31: UNIA – Registro de control de acceso personal externo.



UNIVERSIDAD NACIONAL INTERCULTURAL DE LA AMAZONIA

OFICINA GENERAL DE TI SISTEMAS E INFORMATICA

FORMATO: REGISTRO DE CONTROL DE ACCESO A PERSONAL EXTERNO

NRO	NOMBRES Y APELLIDOS	EMPRESA DONDE LABORA	CARGO	EQUIPO A REVISAR	H. Ingreso	H. Finalizacion	Tareas Realizadas	Autorizado por
1								
2								
3								

- **Registro de incidencias de copias de seguridad.**

Figura 32: UNIA – Registro de incidencias de copias de seguridad.



UNIVERSIDAD NACIONAL INTERCULTURAL DE LA AMAZONIA

OFICINA GENERAL DE TI SISTEMAS E INFORMATICA

FORMATO: REGISTRO DE INCIDENCIAS EN COPIAS DE SEGURIDAD

NRO	EQUIPOS	INCIDENCIA	PERSONAL REGISTRO	PERSONAL SOLUCION	FECHA	HORA	ACCIONES
1							
2							
3							

- **Registro de incidencias en telecomunicaciones.**

Figura 33: UNIA – Registro de incidencias en equipos de telecomunicaciones



UNIVERSIDAD NACIONAL INTERCULTURAL DE LA AMAZONIA

OFICINA GENERAL DE TI SISTEMAS E INFORMATICA

FORMATO: REGISTRO DE INCIDENCIAS EN EQUIPOS DE TELECOMUNICACIONES

NRO	EQUIPOS	INCIDENCIA	PERSONAL REGISTRO	PROVEEDOR	PERSONAL SOLUCION	FECHA	HORA	ACCIONES
1								
2								
3								

CAPITULO V

RESULTADOS Y DISCUSIÓN

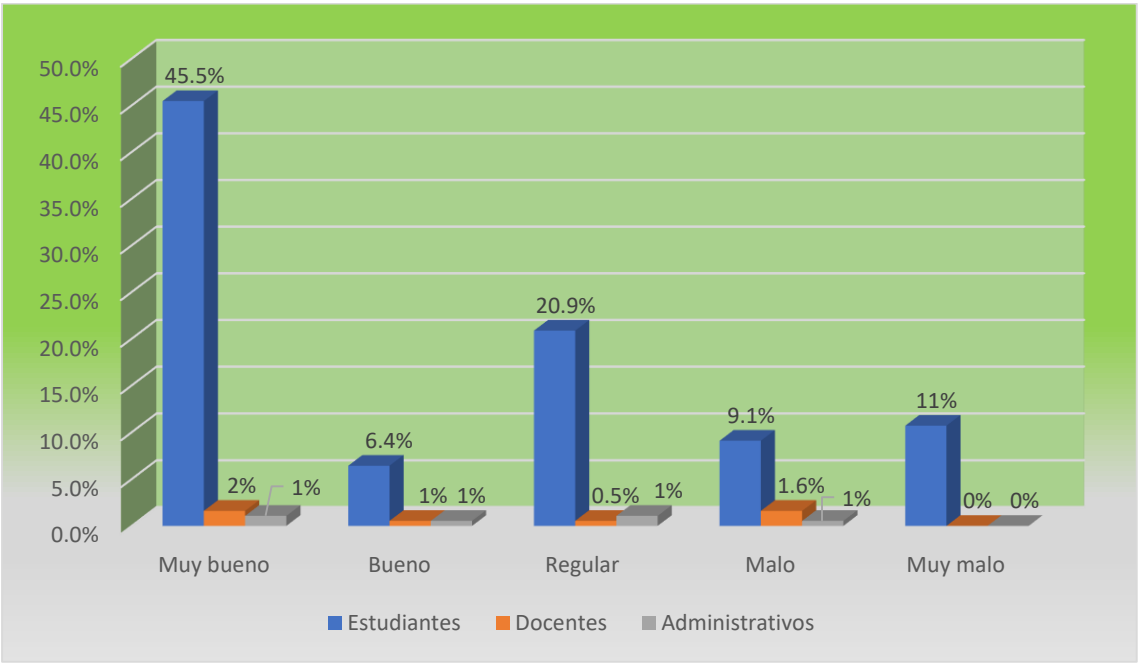
5.1 Procesamiento de datos de la Variable Seguridad Perimetral

Tabla N° 13: Distribución de frecuencia de la Variable Seguridad Perimetral

Variable 1	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	85	45.5%	3	1.6%	2	1.1%	90	48.1%
Bueno	12	6.4%	1	0.5%	1	0.5%	14	7.5%
Regular	39	20.9%	1	0.5%	2	1.1%	42	22.5%
Malo	17	9.1%	3	1.6%	1	0.5%	21	11.2%
Muy malo	20	10.7%	0	0%	0	0%	20	10.7%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 34: UNIA – Barras porcentuales de la Variable Seguridad Perimetral de TI



Fuente: tabla 13

Descripción: de acuerdo a la tabla 13 y figura 34, los estudiantes manifiestan que la Seguridad Perimetral de TI es muy buena y buena en un 51.9%, mientras que los Docentes manifiestan que es muy bueno y bueno en un 2.1%, asimismo los Administrativos indican que la Seguridad Perimetral de TI es muy buena, buena y regular en un 2.7%.

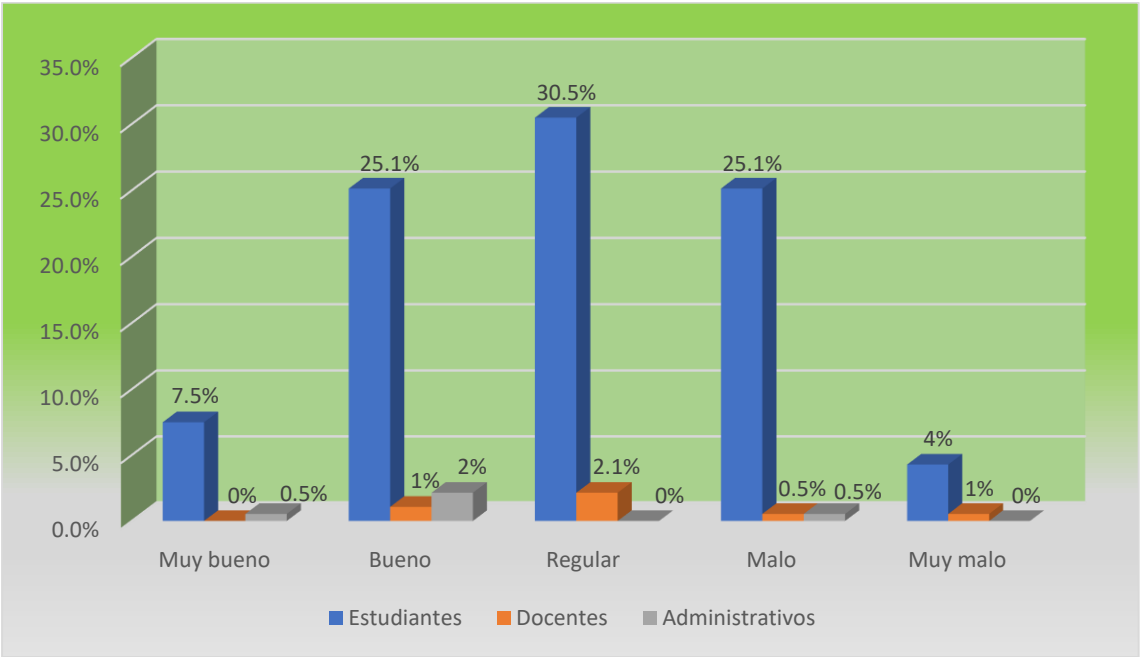
5.1.1. Procesamiento de datos de la Dimensión Políticas

Tabla N° 144: Distribución de frecuencia de la dimensión dimensión Políticas

Políticas	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	14	7.5%	0	0%	1	0.5%	15	8%
Bueno	47	25.1%	2	1.1%	4	2.1%	53	28.3%
Regular	57	30.5%	4	2.1%	0	0.0%	61	32.6%
Malo	47	25.1%	1	0.5%	1	0.5%	49	26.2%
Muy malo	8	4.3%	1	0.5%	0	0%	9	4.8%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 35: UNIA – Barras porcentuales de la dimensión Políticas



Fuente: tabla 14

Descripción: de acuerdo a la tabla 14 y figura 35, los estudiantes manifiestan que la Políticas de TI es muy buena, buena y regular en un 63.1%, mientras que los Docentes manifiestan que es bueno y regular en un 3.2%, asimismo los Administrativos indican que la Políticas de TI es muy buena y buena en un 2.6%

.

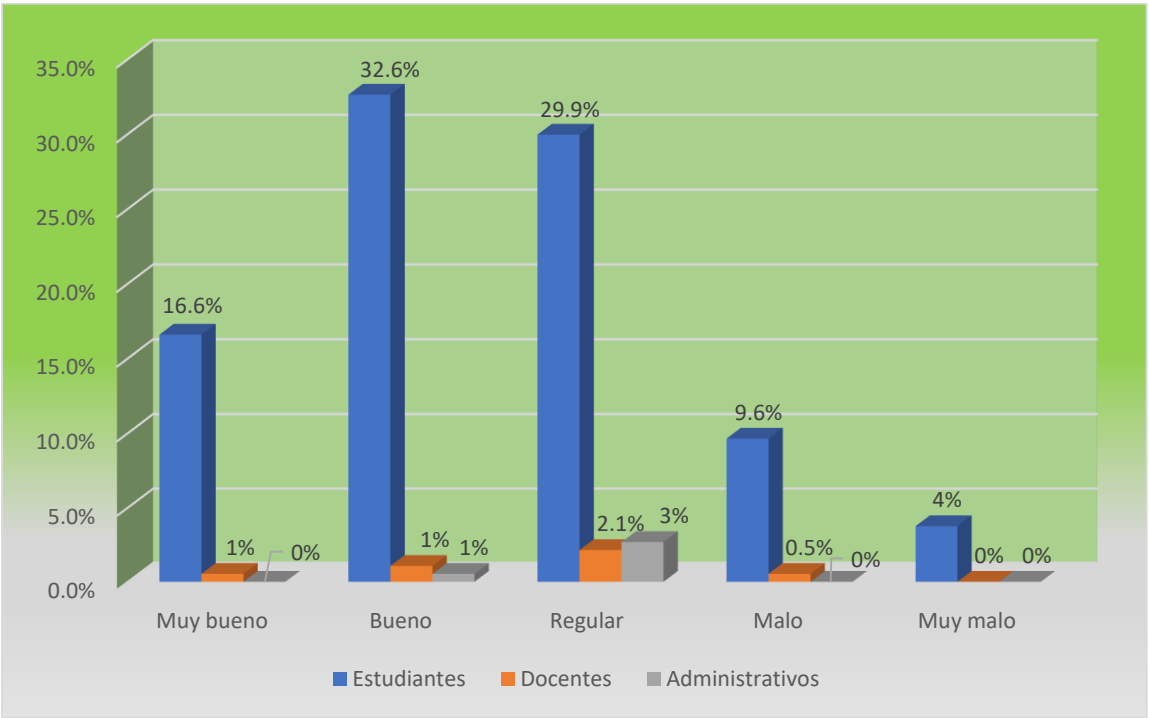
5.1.2. Procesamiento de datos de la Dimensión Aspectos organizativos

Tabla N° 155: Distribución de frecuencia de la dimensión Aspectos Organizativos

Aspectos organizativos	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	31	16.6%	1	0.5%	0	0.0%	32	17.1%
Bueno	61	32.6%	2	1.1%	1	0.5%	64	34.2%
Regular	56	29.9%	4	2.1%	5	2.7%	65	34.8%
Malo	18	9.6%	1	0.5%	0	0.0%	19	10.2%
Muy malo	7	3.7%	0	0.0%	0	0.0%	7	3.7%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 36: UNIA – Barras porcentuales de la dimensión Aspectos Organizativos



Fuente: tabla 15

Descripción: de acuerdo a la tabla 15 y figura 36, los estudiantes manifiestan que los aspectos organizativos de TI son muy buena, buena y regular en un 79.1%, mientras que los Docentes manifiestan que es bueno y regular en un 3.2%, asimismo los Administrativos indican que los aspectos organizativos de TI son buenos y regular en un 3.2%.

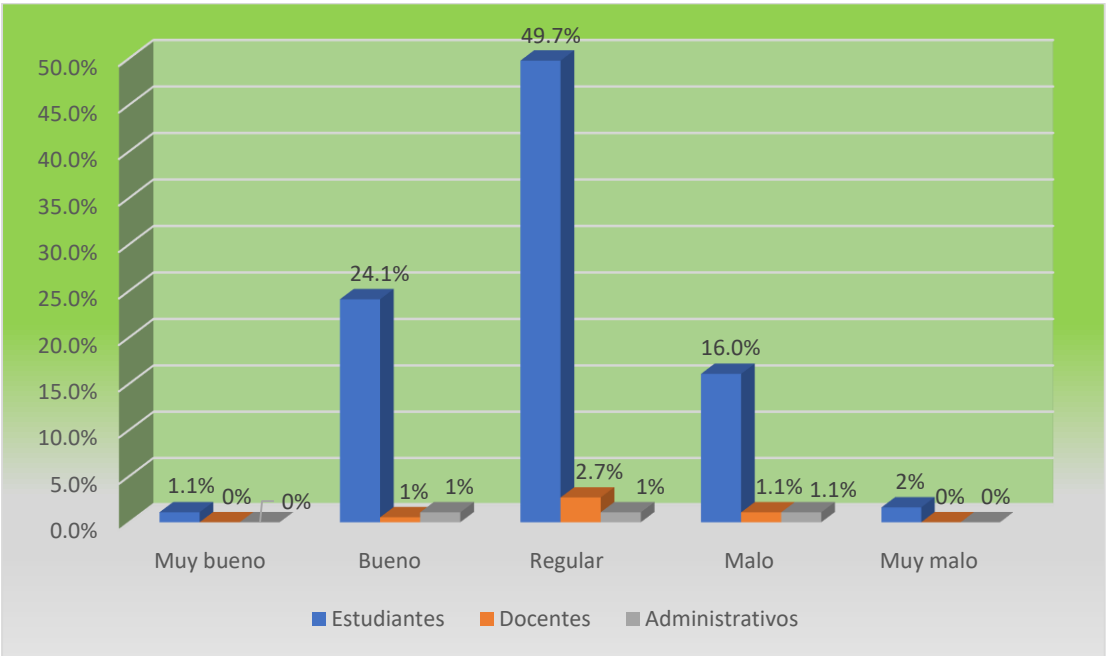
5.1.3 Procesamiento de datos de la Dimensión Control de Accesos.

Tabla N° 166: Distribución de frecuencia de la dimensión Control de Accesos

Control de accesos	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	2	1.1%	0	0%	0	0%	2	1.1%
Bueno	45	24.1%	1	0.5%	2	1.1%	48	25.7%
Regular	93	49.7%	5	2.7%	2	1.1%	100	53.5%
Malo	30	16%	2	1.1%	2	1.1%	34	18.2%
Muy malo	3	1.6%	0	0%	0	0%	3	1.6%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 37: UNIA – Barras porcentuales de la dimensión Aspectos Organizativos



Fuente: tabla 16

Descripción: de acuerdo a la tabla 16 y figura 37, los estudiantes manifiestan que el Control de Accesos de TI es muy buena, buena y regular en un 74.9%, mientras que los Docentes manifiestan que es bueno y regular en un 3.2%, asimismo los Administrativos indican que el Control de Accesos de TI es bueno y regular en un 2.2%.

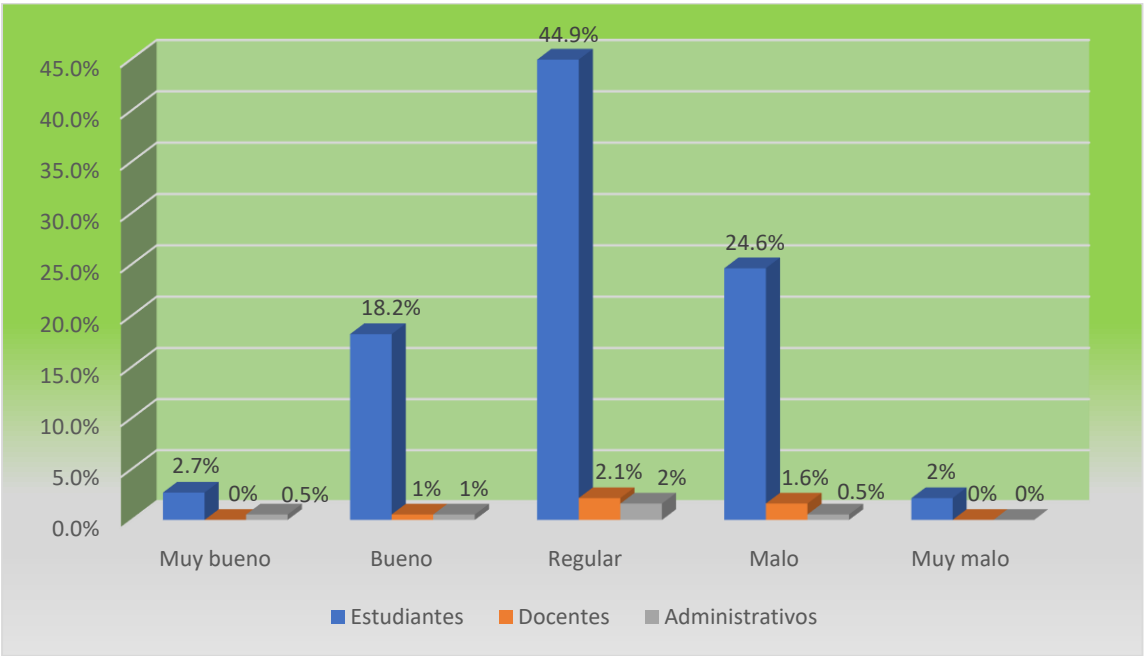
5.1.4. Procesamiento de datos de la Dimensión Seguridad en la Operación

Tabla N° 17: Distribución de frecuencia de la dimensión Seguridad en la Operación

Seguridad en la operación	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	5	2.7%	0	0%	1	0.5%	6	3.2%
Bueno	34	18.2%	1	0.5%	1	0.5%	36	19.3%
Regular	84	44.9%	4	2.1%	3	1.6%	91	48.7%
Malo	46	24.6%	3	1.6%	1	0.5%	50	26.7%
Muy malo	4	2.1%	0	0%	0	0%	4	2.1%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 38: UNIA – Barras porcentuales de la dimensión Seguridad en la Operación



Fuente: tabla 17

Descripción: de acuerdo a la tabla 17 y figura 38, los estudiantes manifiestan que la Seguridad en la Operación de TI es muy buena, buena y regular en un 65.8%, mientras que los Docentes manifiestan que es bueno y regular en un 2.6%, asimismo los Administrativos indican que la Seguridad en la Operación de TI es muy buena, buena y regular en un 2.6%.

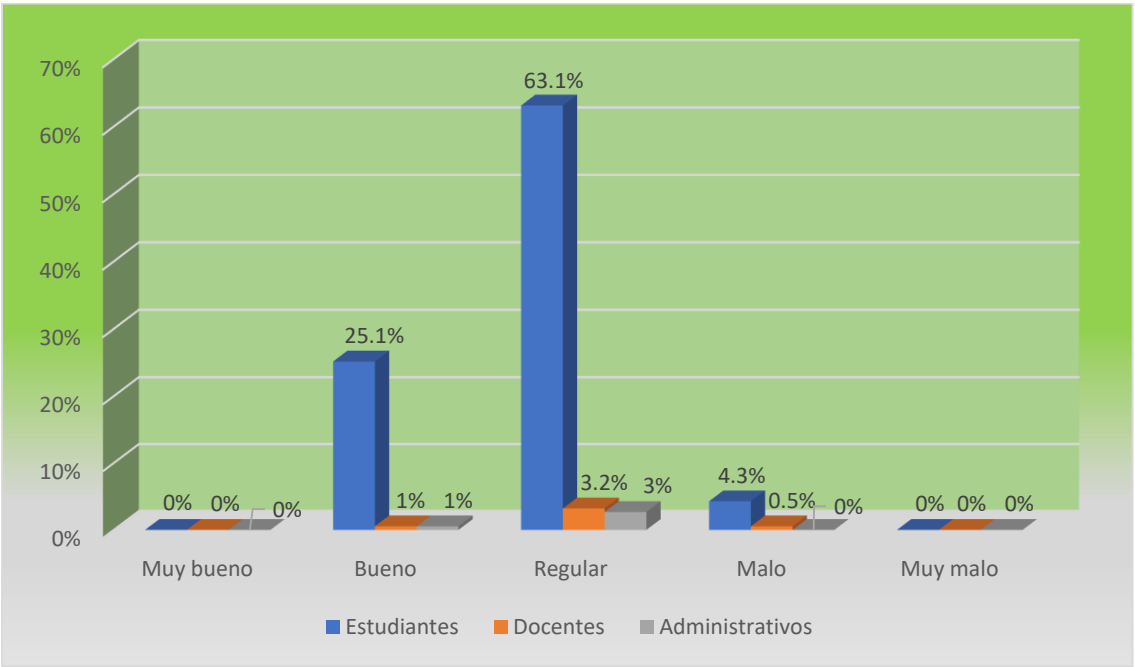
5.1.5. Procesamiento de datos de la Dimensión Seguridad en las Telecomunicaciones

Tabla N° 18: Distribución de frecuencia de la dimensión Seguridad en las Telecomunicaciones

Seguridad en las telecomunicaciones	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	0	0%	0	0%	0	0%	0	0%
Bueno	47	25.1%	1	0.5%	1	0.5%	49	26.2%
Regular	118	63.1%	6	3.2%	5	2.7%	129	69.0%
Malo	8	4.3%	1	0.5%	0	0%	9	4.8%
Muy malo	0	0%	0	0%	0	0%	0	0%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 39: UNIA – Barras porcentuales de la dimensión Seguridad en las Telecomunicaciones



Fuente: tabla 18

Descripción: de acuerdo a la tabla 18 y figura 39, los estudiantes manifiestan que la Seguridad en las Telecomunicaciones de TI es bueno y regular en un 88.2%, mientras que los Docentes manifiestan que es bueno y regular en un 3.7%, asimismo los Administrativos indican que la Seguridad en las Telecomunicaciones de TI es muy buena, buena y regular en un 3.2%

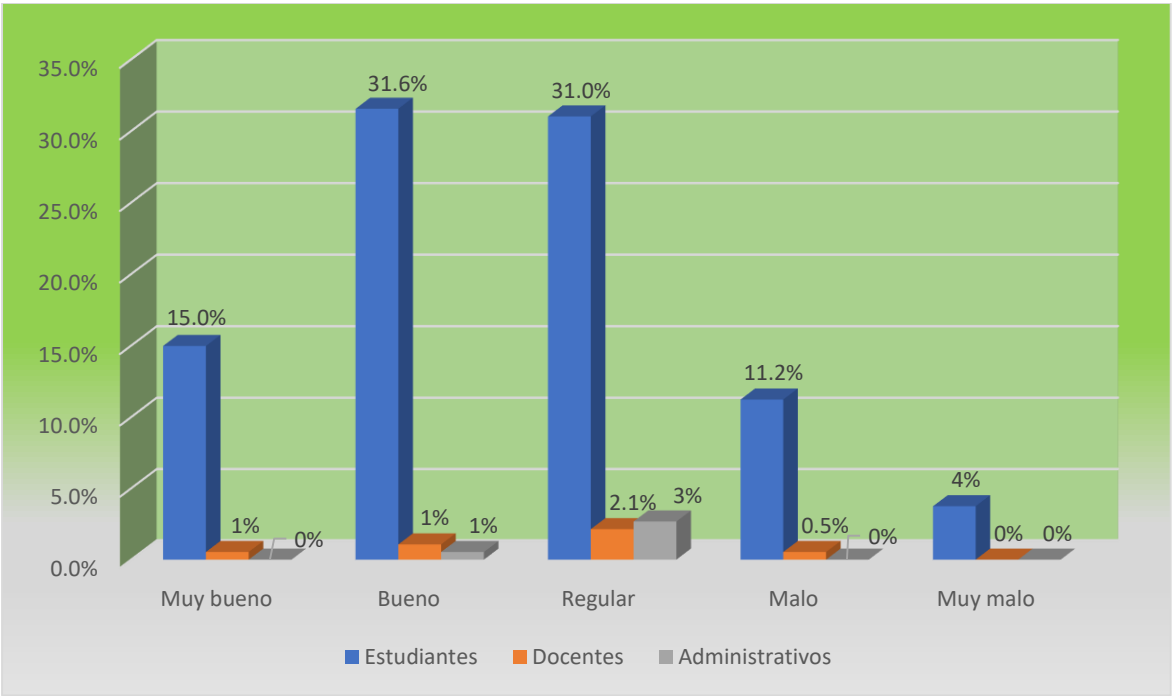
5.1.6. Procesamiento de datos de la Dimensión Adquisición y Desarrollo

Tabla N° 19: Distribución de frecuencia de la dimensión Adquisición y Desarrollo

Adquisición	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	28	15%	1	0.5%	0	0%	29	15.5%
Bueno	59	31.6%	2	1.1%	1	0.5%	62	33.2%
Regular	58	31%	4	2.1%	5	2.7%	67	35.8%
Malo	21	11.2%	1	0.5%	0	0%	22	11.8%
Muy malo	7	3.7%	0	0%	0	0%	7	3.7%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 40: UNIA – Barras porcentuales de la dimensión Adquisición y Desarrollo



Fuente: tabla 19

Descripción: de acuerdo a la tabla 19 y figura 40, los estudiantes manifiestan que la Adquisición y Desarrollo de TI es muy buena, buena y regular en un 77.6%, mientras que los Docentes manifiestan que es muy buena, buena y regular en un 3.7%, asimismo los Administrativos indican que la Adquisición y Desarrollo de TI es buena y regular en un 3.2%

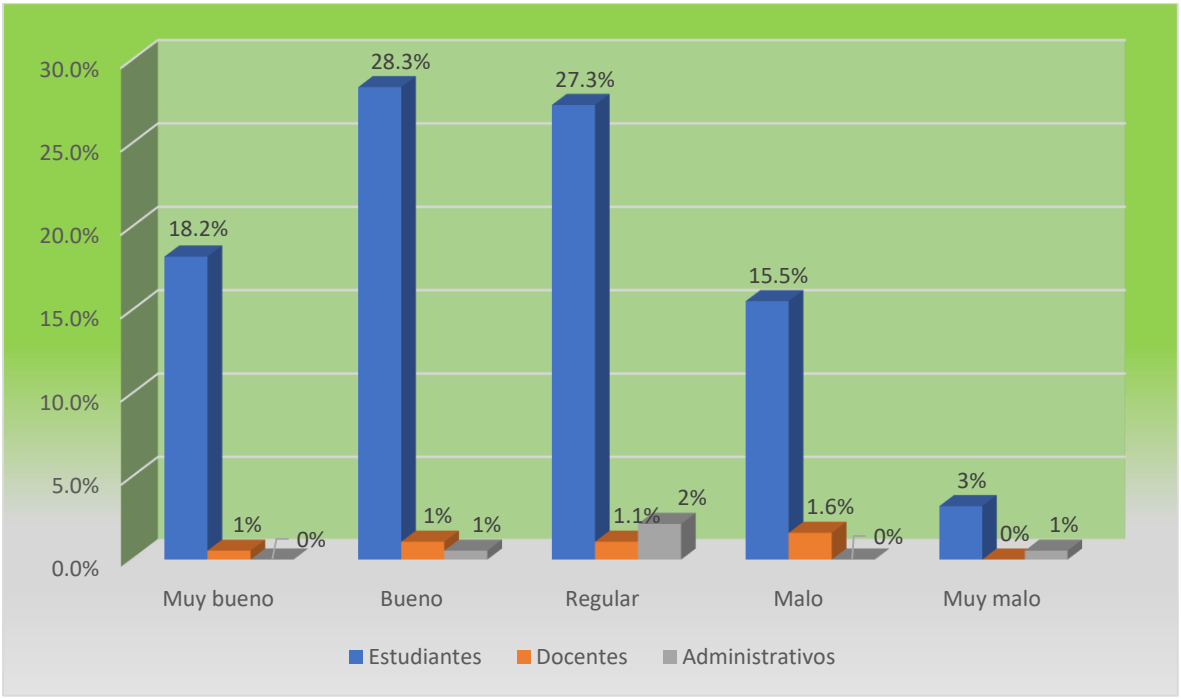
5.1.7. Procesamiento de datos de la Dimensión Gestión de incidentes

Tabla N° 20: Distribución de frecuencia de la dimensión Gestión de Incidentes

Gestión de Incidentes	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	34	18.2%	1	0.5%	0	0%	35	18.7%
Bueno	53	28.3%	2	1.1%	1	0.5%	56	29.9%
Regular	51	27.3%	2	1.1%	4	2.1%	57	30.5%
Malo	29	15.5%	3	1.6%	0	0%	32	17.1%
Muy malo	6	3.2%	0	0%	1	0.5%	7	3.7%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 41: UNIA – Barras porcentuales de la dimensión Adquisición y Desarrollo



Fuente: tabla 20

Descripción: de acuerdo a la tabla 20 y figura 41 los estudiantes manifiestan que la Gestión de Incidentes de TI es muy buena, buena y regular en un 73.8%, mientras que los Docentes manifiestan que es muy buena, buena y regular en un 2.7%, asimismo los Administrativos indican que la Gestión de Incidentes de TI es buena y regular en un 2.6%.

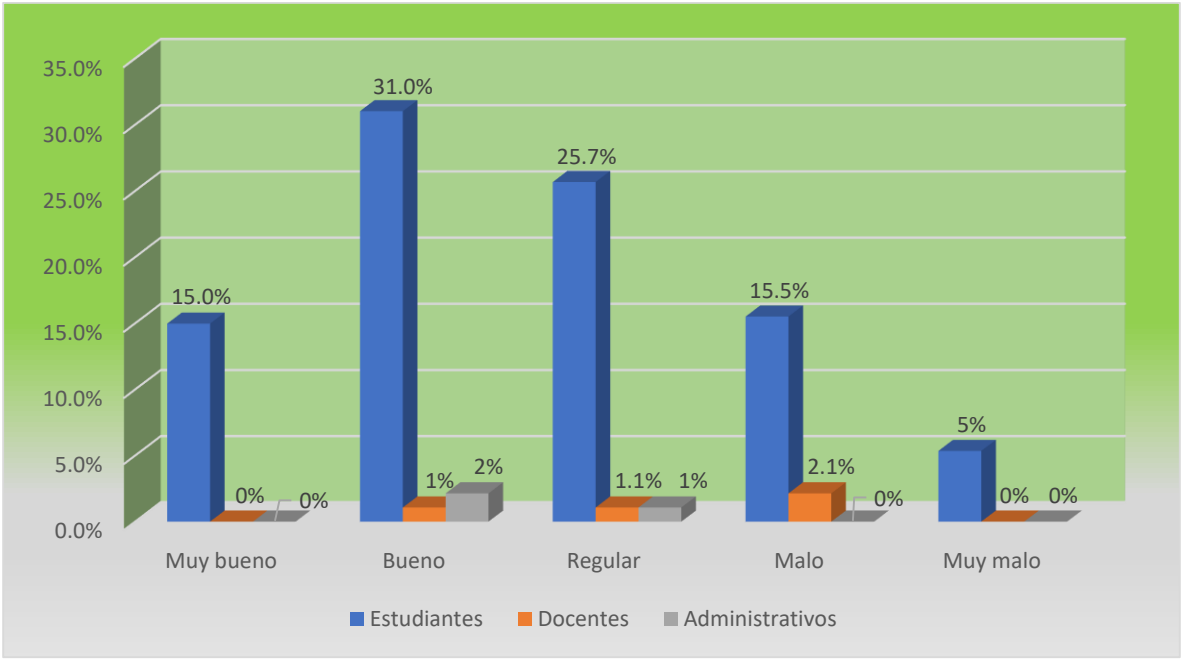
5.2. Procesamiento de datos de la Variable Gestión de Servicios de TI.

Tabla N° 21: Distribución de frecuencia de la Variable Gestión de Servicios de TI

Variable_2	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	28	15%	0	0%	0	0%	28	15%
Bueno	58	31%	2	1.1%	4	2.1%	64	34.2%
Regular	48	25.7%	2	1.1%	2	1.1%	52	27.8%
Malo	29	15.5%	4	2.1%	0	0%	33	17.6%
Muy malo	10	5.3%	0	0%	0	0%	10	5.3%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 42: UNIA – Barras porcentuales de la Variable Gestión de Servicios de TI



Fuente: tabla 21

Descripción: de acuerdo a la tabla 21 y figura 42 los estudiantes manifiestan que la Gestión de Servicios de TI es muy buena, buena y regular en un 71.7%, mientras que los Docentes manifiestan que es regular y malo en un 3.2%, asimismo los Administrativos indican que la Gestión de Servicios de TI es buena y regular en un 3.2%.

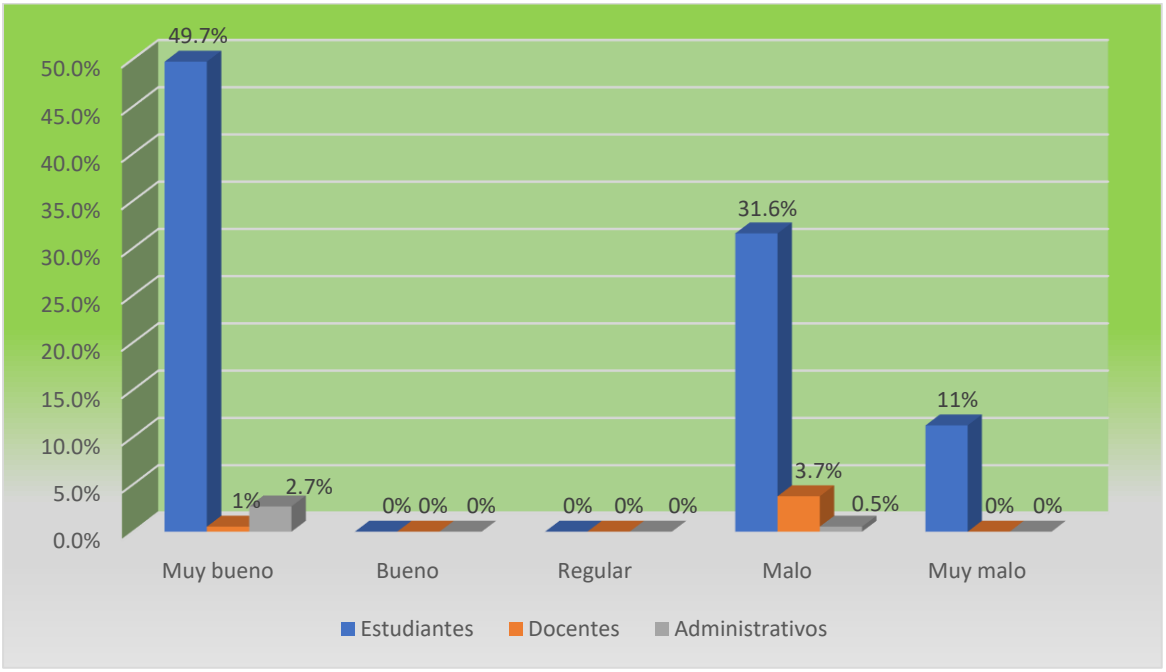
5.2.1. Procesamiento de datos de la Dimensión Personal y Organización

Tabla N° 22: Distribución de frecuencia de la dimensión Personal y Organización

Personal	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	93	49.7%	1	0.5%	5	2.7%	99	52.9%
Bueno	0	0%	0	0%	0	0%	0	0%
Regular	0	0%	0	0%	0	0%	0	0%
Malo	59	31.6%	7	3.7%	1	0.5%	67	35.8%
Muy malo	21	11.2%	0	0%	0	0%	21	11.2%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 43: UNIA – Barras porcentuales de la dimensión Personal y Organización



Fuente: tabla 22

Descripción: de acuerdo a la tabla 22 y figura 43 los estudiantes manifiestan que el Personal y Organización de TI es muy buena en un 49.7%, mientras que los Docentes manifiestan que es malo en un 3.7%, asimismo los Administrativos indican que el Personal y Organización de TI es muy bueno en un 2.7%.

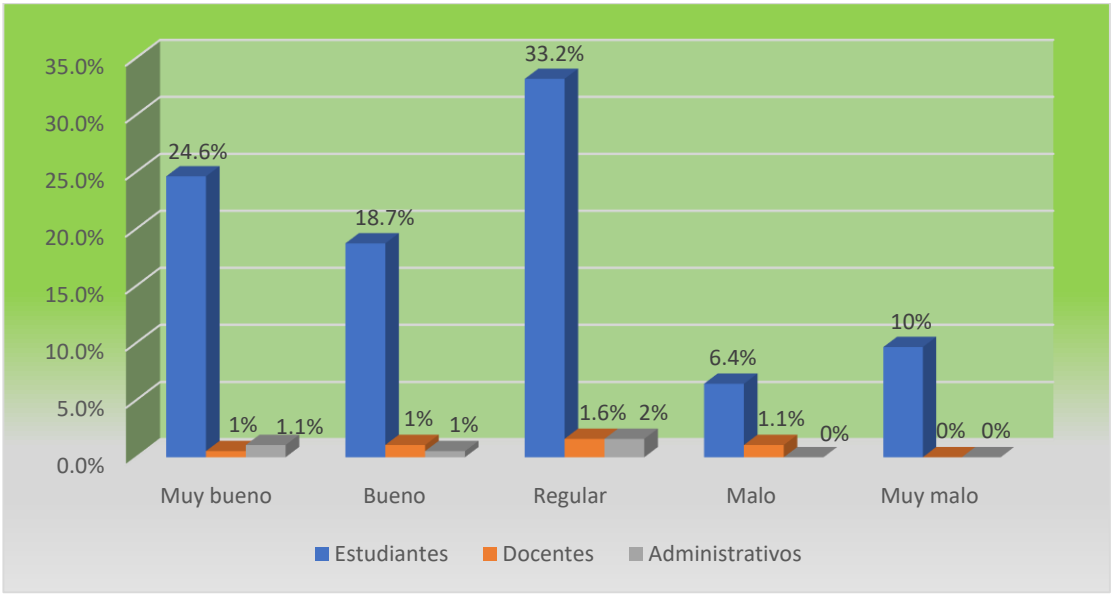
5.2.2. Procesamiento de datos de la Dimensión Información y Tecnología

Tabla N° 23: Distribución de frecuencia de la dimensión Información y Tecnología

Información y tecnología	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	46	24.6%	1	0.5%	2	1.1%	49	26.2%
Bueno	35	18.7%	2	1.1%	1	0.5%	38	20.3%
Regular	62	33.2%	3	1.6%	3	1.6%	68	36.4%
Malo	12	6.4%	2	1.1%	0	0.%	14	7.5%
Muy malo	18	9.6%	0	0%	0	0%	18	9.6%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 44: UNIA – Barras porcentuales de la dimensión Información y Tecnología



Fuente: tabla 23

Descripción: de acuerdo a la tabla 23 y figura 44 los estudiantes manifiestan que la Información y Tecnología de TI es muy buena, buena y regular en un 76.5%, mientras que los Docentes manifiestan que es muy buena, buena y regular en un 3.2%, asimismo los Administrativos indican que la Información y Tecnología de TI es muy buena, buena y regular en un 3.2%.

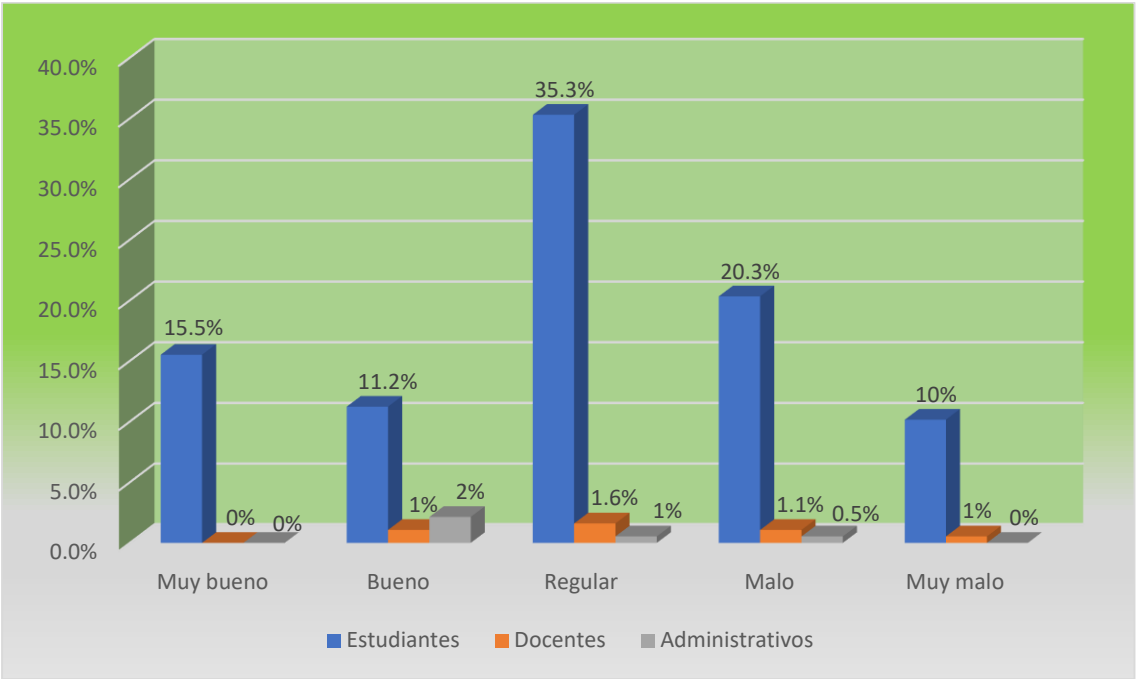
5.2.3. Procesamiento de datos de la Dimensión Proveedores y Socios

Tabla N° 24: Distribución de frecuencia de la dimensión Proveedores y Socios

Proveedores	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	29	15.5%	0	0%	0	0%	29	15.5%
Bueno	21	11.2%	2	1.1%	4	2.1%	27	14.4%
Regular	66	35.3%	3	1.6%	1	0.5%	70	37.4%
Malo	38	20.3%	2	1.1%	1	0.5%	41	21.9%
Muy malo	19	10.2%	1	0.5%	0	0%	20	10.7%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 45 UNIA – Barras porcentuales de la dimensión Proveedores y Socios



Fuente: tabla 24

Descripción: de acuerdo a la tabla 24 y figura 45 los estudiantes manifiestan que los Proveedores y socios de TI es muy buena, buena y regular en un 62%, mientras que los Docentes manifiestan que es buena y regular en un 2.7%, asimismo los Administrativos indican que los Proveedores y socios de TI es buena y regular en un 2.6%.

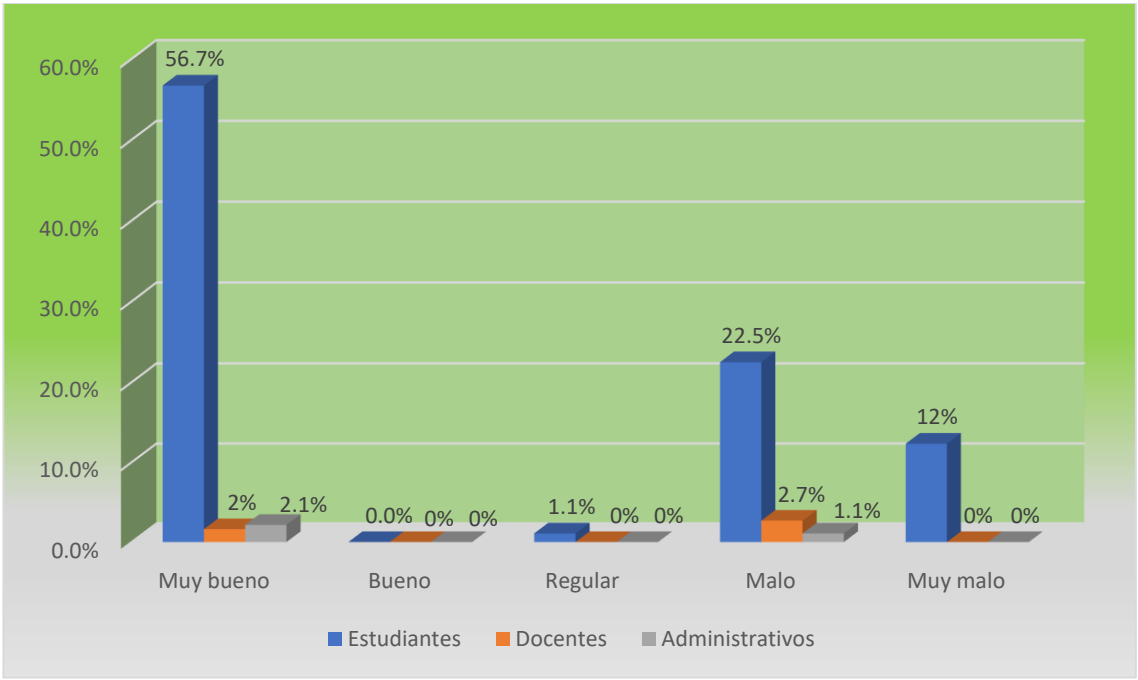
5.2.4. Procesamiento de datos de la Dimensión Flujo de Valor

Tabla N° 25: Distribución de frecuencia de la dimensión Flujo de Valor

Flujo de Valor	Estudiantes		Docentes		Administrativos		Total	
	fi	hi%	fi	hi%	fi	hi%	fi	hi%
Muy bueno	106	56.7%	3	1.6%	4	2.1%	113	60.4%
Bueno	0	0%	0	0%	0	0%	0	0%
Regular	2	1.1%	0	0%	0	0%	2	1.1%
Malo	42	22.5%	5	2.7%	2	1.1%	49	26.2%
Muy malo	23	12.3%	0	0%	0	0%	23	12.3%
Total	173	92.5%	8	4.3%	6	3.2%	187	100%

Fuente: Anexo 2

Figura 46: UNIA – Barras porcentuales de la dimensión Flujo de Valor



Fuente: tabla 13

Descripción: de acuerdo a la tabla 25 y figura 46 los estudiantes manifiestan que el Flujo de Valor de TI es muy buena y regular en un 57.8%, mientras que los Docentes manifiestan que es malo en un 2.7%, asimismo los Administrativos indican que el Flujo de Valor de TI es muy bueno en un 2.1%.

5.3. Prueba de hipótesis

La prueba de hipótesis “es un proceso que nos conduce a tomar la decisión de aceptar o rechazar la hipótesis nula H_0, en contraposición de la hipótesis alternativa H_1 y en base a los resultados de una muestra aleatoria seleccionada de la población en estudio”. (Córdova Zamora, 2003, pág. 434). Además, los pasos a seguir para demostrar la hipótesis, se realizó en base, a lo que afirma (Pérez Legoas, 2010), quien establece que:

- Plantear la hipótesis nula y la alternativa.
- Seleccionar el nivel de significancia.
- Calcular el valor estadístico de la prueba
- Aplicar la regla de decisión.
- Tomar una decisión.

5.3.1. Prueba de hipótesis general.

I. Plantear la hipótesis nula y la alternativa

Ho: La Seguridad Perimetral Informática no se relaciona con la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana: 2021.

H1: La Seguridad Perimetral Informática se relaciona con la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana: 2021.

II. Seleccionar el nivel de significancia

El nivel de significancia: $\alpha = 5\% = 0{,}05$

Este nivel de significancia será para todas las demás pruebas de hipótesis específicas, por tanto, ya no se repetirán en las demás hipótesis específicas.

III. Calcular el valor estadístico de la prueba

Es un estudio trasversal, en la que se aplicó la prueba de Correlación de Rho de Spearman. Para confirmar se aplicó la **Lectura de P – Valor a través de la prueba de Normalidad** se debe de corroborar que la variable aleatoria en ambos grupos se distribuye normalmente. Para ello se utilizó la prueba de Kolmogórov-Smirnov, porque según (Romero Saldaña, 2016), considera que se aplica cuando la muestra es mayor a 50 datos. El criterio para determinar si la (VA) se distribuye normalmente es:

a) **P–valor** $> \alpha$**. Aceptar la Ho =** Los datos provienen de una distribución normal.

b) **P–valor** $\leq \alpha$**. Aceptar la** H_1 **=** Los datos no provienen de una distribución normal.

Estas condiciones se aplicarán en las demás pruebas de hipótesis específica, por tanto, ya no se considerarán en las demás pruebas de las hipótesis específicas.

Tabla N° 26: Prueba de normalidad de la prueba de hipótesis general

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
Hipótesis General	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Seguridad Perimetral Informática	,049	187	,200	,992	187	,430
Gestión de Servicios de TI	,091	187	,001	,960	187	,000

a. Corrección de significación de Lilliefors

Fuente: anexo 2
Elaboración: propia

Tabla N° 27: Toma de decisión de la hipótesis general

P-valor de la variable: Seguridad Perimetral Informática = 0.200	>	0.050
P-valor de la variable: Gestión de Servicios de TI = 0.000	<	0.050

Conclusion: La variable Seguridad Perimetral Informática se comportan normalmente y la variable Gestión de Servicios de TI no se comporta normalmente por lo que se recomienda la aplicacion de la prueba de Correlacion de Rho de Spearman.

Fuente: tabla 26

IV. Aplicación la regla de decisión

Tabla N° 28 Prueba de correlación de Rho Spearman de la hipótesis general

Correlaciones

			Seguridad Perimetral Informática	Gestión de Servicios de TI
Rho de Spearman	Seguridad Perimetral Informática	Coeficiente de correlación	1,000	,437**
		Sig. (bilateral)	.	,000
		N	187	187
	Gestión de Servicios de TI	Coeficiente de correlación	,437**	1,000
		Sig. (bilateral)	,000	.
		N	187	187

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Anexo 2

V. Toma de decisión:

Afirmamos que existe una relación directamente proporcional y significativa entre las variables: Seguridad Perimetral Informática y Gestión de Servicios de TI, Porque el valor sig. (bilateral) es 0.000.

Además, en Base en la tabla N° 28. Afirmamos que el p valor (Sig.) 0.000, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Seguridad Perimetral Informática se relaciona con la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana: 2021.

Por lo tanto, en base a lo estipulado (Hernandez Sampieri, Fernandez Collado, & Bapista Lucio, 2014), r = 0.44. Indica que existe un grado de correlación positiva media.

5.3.2. Prueba de hipótesis especifica 1

I. Plantear la hipótesis nula y la alternativa

Ho: 1. La Seguridad Perimetral Informática no se relaciona con el Personal y Organización en las Universidades Públicas de la Amazonía Peruana: 2021

H1: 1. La Seguridad Perimetral Informática se relaciona con el Personal y Organización en las Universidades Públicas de la Amazonía Peruana:2021

II. Calcular el valor estadístico de la prueba

Tabla N° 29: Prueba de normalidad de la prueba de hipótesis especifica 1

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
Hipótesis Especifica 1	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Seguridad Perimetral Informática	,049	187	,200	,992	187	,430
Personal y Organización	,366	187	,000	,696	187	,000

a. Corrección de significación de Lilliefors

Fuente: anexo 2
Elaboración: propia

Tabla N° 30: Toma de decisión de la hipótesis especifica 1

P-valor de la variable: Seguridad Perimetral Informática = 0.200	>	0.050
P-valor de la variable: Personal y Organización = 0.000	<	0.050

Conclusion: La variable Seguridad Perimetral Informática se comporta normalmente pero la dimension Personal y Organización no se comporta normalmente por lo que se recomienda la aplicacion de la prueba de Correlacion de Rho de Spearman.

Fuente: tabla 29

III. Aplicación la regla de decisión

Tabla N° 31 Prueba de correlación de Rho Spearman de la hipótesis especifica 1

Correlaciones

			Seguridad Perimetral Informática	Personal y Organización
Rho de Spearman	Seguridad Perimetral Informática	Coeficiente de correlación	1,000	,360**
		Sig. (bilateral)	.	,000
		N	187	187
	Personal y Organización	Coeficiente de correlación	,360**	1,000
		Sig. (bilateral)	,000	.
		N	187	187

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Anexo 2

IV. Toma de decisión:

Afirmamos que existe una relación directamente proporcional y significativa entre las variables: Seguridad Perimetral Informática y Personal y Organización, Porque el valor sig. (bilateral) es 0.000.

Además, en Base en la tabla N° 31. Afirmamos que el p valor (Sig.) 0.000, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Seguridad Perimetral Informática se relaciona con el Personal y Organización en las Universidades Públicas de la Amazonía Peruana:2021.

Por lo tanto, en base a lo estipulan (Hernandez Sampieri, Fernandez Collado, & Bapista Lucio, 2014), r = 0.36. Indica que existe un grado de correlación positiva media.

5.3.3. Prueba de hipótesis especifica 2

I. Plantear la hipótesis nula y la alternativa

Ho: 1. La Seguridad Perimetral Informática no se relaciona con la Información y tecnología en las Universidades Públicas de la Amazonía Peruana: 2021.

H1: 1. La Seguridad Perimetral Informática se relaciona con la Información y tecnología en las Universidades Públicas de la Amazonía Peruana: 2021.

II. Calcular el valor estadístico de la prueba

Tabla N° 32: Prueba de normalidad de la prueba de hipótesis especifica 2

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
Hipótesis Especifica 2	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Seguridad Perimetral Informática	,049	187	,200	,992	187	,430
Información y tecnología	,151	187	,000	,959	187	,000

a. Corrección de significación de Lilliefors

Fuente: anexo 2
Elaboración: propia

Tabla N° 33: Toma de decisión de la hipótesis especifica 2

P-valor de la variable: Seguridad Perimetral Informática = 0.200	>	0.050
P-valor de la variable: Información y tecnología = 0.000	<	0.050

Conclusion: La variable Seguridad Perimetral Informática se comporta normalmente pero la dimension información y tecnología no se comporta normalmente por lo que se recomienda la aplicacion de la prueba de Correlacion de Rho de Spearman.

Fuente: tabla 32

III. Aplicación la regla de decisión

Tabla N° 34 Prueba de correlación de Rho Spearman de la hipótesis especifica 2

Correlaciones

			Seguridad Perimetral Informática	Información y tecnología
Rho de Spearman	Seguridad Perimetral Informática	Coeficiente de correlación	1,000	,207**
		Sig. (bilateral)	.	,004
		N	187	187
	Información y tecnología	Coeficiente de correlación	,207**	1,000
		Sig. (bilateral)	,004	.
		N	187	187

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Anexo 2

IV. Toma de decisión:

Afirmamos que existe una relación directamente proporcional y significativa entre las variables: Seguridad Perimetral Informática e Información y tecnología, Porque el valor sig. (bilateral) es 0.004.

Además, en Base en la tabla N° 34. Afirmamos que el p valor (Sig.) 0.004, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Seguridad Perimetral Informática se relaciona con la Información y tecnología en las Universidades Públicas de la Amazonía Peruana: 2021.

Por lo tanto, en base a lo estipulan (Hernandez Sampieri, Fernandez Collado, & Bapista Lucio, 2014), r = 0.21. Indica que existe un grado de correlación positiva débil.

5.3.4. Prueba de hipótesis especifica 3

I. Plantear la hipótesis nula y la alternativa

Ho: 1. La Seguridad Perimetral Informática no se relaciona con los Proveedores y Socios en las Universidades Públicas de la Amazonía Peruana: 2021.

H1: 1. La Seguridad Perimetral Informática se relaciona con los Proveedores y Socios en las Universidades Públicas de la Amazonía Peruana: 2021.

II. Calcular el valor estadístico de la prueba

Tabla N° 35: Prueba de normalidad de la prueba de hipótesis especifica 3

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
Hipótesis Especifica 3	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Seguridad Perimetral Informática	,049	187	,200	,992	187	,430
Proveedores y Socios	,090	187	,001	,975	187	,002

a. Corrección de significación de Lilliefors

Fuente: anexo 2
Elaboración: propia

Tabla N° 36: Toma de decisión de la hipótesis especifica 3

P-valor de la variable: Seguridad Perimetral Informática = 0.200	>	0.050
P-valor de la variable: Proveedores y Socios = 0.002	<	0.050

Conclusion: La variable Seguridad Perimetral Informática se comporta normalmente pero la dimension Proveedores y Socios no se comporta normalmente por lo que se recomienda la aplicacion de la prueba de Correlacion de Rho de Spearman.

Fuente: tabla 35

III. Aplicación la regla de decisión

Tabla N° 37 Prueba de correlación de Rho Spearman de la hipótesis especifica 3

Correlaciones

			Seguridad Perimetral Informática	Proveedores y Socios
Rho de Spearman	Seguridad Perimetral Informática	Coeficiente de correlación	1,000	,133**
		Sig. (bilateral)	.	,009
		N	187	187
	Proveedores y Socios	Coeficiente de correlación	,133**	1,000
		Sig. (bilateral)	,069	.
		N	187	187

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Anexo 2

IV. Toma de decisión:

Afirmamos que existe una relación directamente proporcional y significativa entre las variables: Seguridad Perimetral Informática y Proveedores y Socios, Porque el valor sig. (bilateral) es 0.009

Además, en Base en la tabla N° 37. Afirmamos que el p valor (Sig.) 0.009, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Seguridad Perimetral Informática se relaciona con los Proveedores y Socios en las Universidades Públicas de la Amazonía Peruana: 2021.

Por lo tanto, en base a lo estipulan (Hernandez Sampieri, Fernandez Collado, & Bapista Lucio, 2014), r = 0.133. Indica que existe un grado de correlación positiva débil.

5.3.5. Prueba de hipótesis especifica 4

I. Plantear la hipótesis nula y la alternativa

Ho: 1. La Seguridad Perimetral Informática no se relaciona con el Flujo de valor y Procesos en las Universidades Públicas de la Amazonía Peruana: 2021.

H1: 1. La Seguridad Perimetral Informática se relaciona con el Flujo de valor y Procesos en las Universidades Públicas de la Amazonía Peruana: 2021.

II. Calcular el valor estadístico de la prueba

Tabla N° 38: Prueba de normalidad de la prueba de hipótesis especifica 4

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
Hipótesis Especifica 3	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Seguridad Perimetral Informática	,409	187	,200	,992	187	,430
Flujo de valor y Procesos	,390	187	,000	,686	187	,000

a. Corrección de significación de Lilliefors

Fuente: anexo 2
Elaboración: propia

Tabla N° 39: Toma de decisión de la hipótesis especifica 4

P-valor de la variable: Seguridad Perimetral Informática = 0.430	>	0.050
P-valor de la variable: Flujo de valor y Procesos = 0.000	<	0.050

Conclusion: La variable Seguridad Perimetral Informática se comporta normalmente pero la dimension Flujo de valor y Procesos no se comporta normalmente por lo que se recomienda la aplicacion de la prueba de Correlacion de Rho de Spearman.

Fuente: tabla 38

III. Aplicación la regla de decisión

Tabla N° 40 Prueba de correlación de Rho Spearman de la hipótesis especifica 4

Correlaciones

			Seguridad Perimetral Informática	Flujo de valor y Procesos
Rho de Spearman	Seguridad Perimetral Informática	Coeficiente de correlación	1,000	,319**
		Sig. (bilateral)	.	,000
		N	187	187
	Flujo de valor y Procesos	Coeficiente de correlación	,319**	1,000
		Sig. (bilateral)	,000	.
		N	187	187

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Anexo 2

IV. Toma de decisión:

Afirmamos que existe una relación directamente proporcional y significativa entre las variables: Seguridad Perimetral Informática y Flujo de valor y Procesos, Porque el valor sig. (bilateral) es 0.000.

Además, en Base en la tabla N° 40. Afirmamos que el p valor (Sig.) 0.000, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Seguridad Perimetral Informática se relaciona con el Flujo de valor y Procesos en las Universidades Públicas de la Amazonía Peruana: 2021.

Por lo tanto, en base a lo estipulan (Hernandez Sampieri, Fernandez Collado, & Bapista Lucio, 2014), r = 0.32. Indica que existe un grado de correlación positiva media.

CONCLUSIONES

Afirmamos que existe una relación directamente proporcional y significativa entre las variables: Seguridad Perimetral Informática y Gestión de Servicios de TI, Porque el valor sig. (bilateral) es 0.000, que es menor que el nivel de significancia de 0,05. Por lo tanto, se concluye que la Seguridad Perimetral Informática se relaciona con la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana: 2021. Asimismo, el grado de correlación de Rho Spearman es r = 0.44 que indica que existe un grado de correlación positiva media.

Afirmamos que existe una relación directamente proporcional y significativa entre las variables: Seguridad Perimetral Informática y Personal y Organización, Porque el valor sig. (bilateral) es 0.000, que es menor que el nivel de significancia de 0,05. Por lo tanto, se concluye que la Seguridad Perimetral Informática se relaciona con el Personal y Organización en las Universidades Públicas de la Amazonía Peruana: 2021. Asimismo, el grado de correlación de Rho Spearman es r = 0.36. Indica que existe un grado de correlación positiva media.

Afirmamos que existe una relación directamente proporcional y significativa entre las variables: Seguridad Perimetral Informática e Información y tecnología, Porque el valor sig. (bilateral) es 0.004, que es menor que el nivel de significancia de 0,05. Por lo tanto, se concluye que la Seguridad Perimetral Informática se relaciona con la Información y tecnología en las Universidades Públicas de la Amazonía Peruana: 2021. Asimismo, el grado de correlación de Rho Spearman es r = 0.21. Indica que existe un grado de correlación positiva débil.

Afirmamos que existe una relación directamente proporcional y significativa entre las variables: Seguridad Perimetral Informática y Proveedores y Socios, Porque el valor sig. (bilateral) es 0.009, que es menor que el nivel de significancia de

0,05. Por lo tanto, se concluye que la Seguridad Perimetral Informática se relaciona con los Proveedores y Socios en las Universidades Públicas de la Amazonía Peruana: 2021. Asimismo, el grado de correlación de Rho Spearman es r = 0.13. Indica que existe un grado de correlación positiva débil.

Afirmamos que existe una relación directamente proporcional y significativa entre las variables: Seguridad Perimetral Informática y Flujo de valor y Procesos, Porque el valor sig. (bilateral) es 0.000, que es menor que el nivel de significancia de 0,05. Por lo tanto, se concluye que la Seguridad Perimetral Informática se relaciona con el Flujo de valor y Procesos en las Universidades Públicas de la Amazonía Peruana: 2021. Asimismo, el grado de correlación de Rho Spearman es r = 0.32. Indica que existe un grado de correlación positiva media.

RECOMENDACIONES

La investigación reveló que la Seguridad Perimetral Informática se relaciona con la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana: 2021. Por lo tanto, se recomienda gestionar mayor asignación presupuestal para el área de TI de las Universidades Públicas de la Amazonía Peruana.

El estudio ha demostrado que la Seguridad Perimetral Informática se relaciona con la Información y Tecnología en las Universidades Públicas de la Amazonía Peruana: 2021. Por lo tanto, se recomienda la implementar a mediano o largo plazo las propuestas de solución planteadas en la investigación.

Los resultados obtenidos demostraron que la Seguridad Perimetral Informática se relaciona con el Personal y Organización en las Universidad Públicas de la Amazonía Peruana: 2021. Por lo tanto, se recomienda realizar y gestionar capacitaciones constantes para el personal de TI, así como para colaboradores, con el uso y manejo de los equipos informáticos, sistemas o software utilizados dentro de las Universidades Públicas de la Amazonía Peruana.

Al analizar los resultados en la investigación se demuestra que la Seguridad Perimetral Informática se relaciona con el Flujo de Valor y Procesos en las Universidades Públicas de la Amazonía Peruana. Por lo tanto, se recomienda gestionar la implementación de Sistema de Gestión de Seguridad de la Información (SGSI) dentro de las Universidades Públicas de la Amazonía Peruana.

REFERENCIAS BIBLIOGRÁFICAS

Accensit_admin. (2 de 07 de 2017). *https://www.accensit.com/*. Obtenido de https://www.accensit.com/blog/seguridad-perimetral-informatica-informacion-necesaria/

Alvarado, B. (2019). *Tec Management.* Obtenido de https://tecmanagement.org/itil-4-las-4-dimensiones-de-la-gestion-de-servicio/

Anguitaa, J. C., Repullo Labradora, J., & Donado Camposb, J. (2002). La encuesta como técnica de investigación. *elsevier*, 12.

Bailon, a. (6 de 12 de 2019). *https://www.bits.com.mx*. Obtenido de https://www.bits.com.mx/gestion-de-servicios-de-ti-que-es/

Barrantes, R. (2008). *Investigación. Un camino al conocimiento.* San José, Costa Rica: Universidad Estatal a Distancia.

BOLAÑOS BOTINA, J. (2018). *DISEÑO DE LA ARQUITECTURA DE SEGURIDAD PERIMETRAL DE LA RED INFORMATICA EN LA INDUSTRIA DE LICORES DEL VALLE.* SANTIAGO DE CALI.

Carrasco Díaz, S. (2010). *Metodologia dela Investigación Científica.* Lima: San Marcos.

Córdova Zamora, M. (2003). *ESTADÍSTICA Descriptiva e Inferencial.* Lima: MOSHERA S.R.L.

DELSOL. (2019). *DELSOL.* Obtenido de https://www.sdelsol.com/glosario/servicio/

Enetic. (2021). *enetic soluciones.* Obtenido de https://enetic.es/soluciones-perimetral-y-redes/

Eserp. (2020). *Eserp.* Obtenido de https://es.eserp.com/articulos/que-son-los-kpis/?_adin=02021864894

Eude. (14 de 05 de 2019). *Eude*. Obtenido de https://www.eude.es/blog/eficiencia-eficacia-diferencias/

GARCIA, D. F. (2016). *ESTUDIO DE LAS TECNOLOGIAS DE SEGURIDAD PERIMETRAL INFORMÁTICAS Y PROPUESTA DE UN PLAN DE IMPLEMENTACIÓN PARA LA AGENCIA NACIONAL DE TRÁNSITO.* Quito.

Gestion. (05 de 08 de 2021). *Gestion*. Obtenido de https://gestion.pe/economia/management-empleo/se-debera-indemnizar-a-trabajadores-por-dano-moral-si-su-despido-afecta-su-calidad-de-vida-noticia/?ref=nota&ft=autoload

GOMEZ. (2004). *Evolución científica y metodológica de la economía. .*

Hernandez Sampieri, R., Fernandez Collado, C., & Bapista Lucio, P. (2014). *Metodologia de la investigación.* Mejico: Mexicana.

Hernandez, F. B. (2001). *Metodología de la Investigación.* Mexico: Mc Graw Hill.

Huergo, J. (2019). *El proceso de Gestion.* Obtenido de http://servicios.abc.gov.ar/lainstitucion/univpedagogica/especializaciones/seminario/materialesparadescargar/seminario4/huergo3.pdf

Humberto. (03 de 2019). Obtenido de https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/1833/Humberto%20Pajares_Trabajo%20de%20Suficiencia%20Profesional_Titulo%20Profesional_2019.pdf?sequence=3&isAllowed=y

IBM. (2015). *SPSS Statistics Base.* Obtenido de http://www-03.ibm.com/software/products/es/spss-stats-base

INSPQ. (2021). *INSPQ.* Obtenido de https://www.inspq.qc.ca/es/centro-collaborador-oms-de-quebec-para-la-promocion-de-la-seguridad-y-prevencion-de-traumatismos/definicion-del-concepto-de-seguridad

MARCEL, A. B. (2017). *DISEÑO DE UN SISTEMA DE SEGURIDAD PERIMETRAL EN LAS INSTALACIONES DEL CONSORCIO EXPANSION PTAR SALITRE, SEDE BOGOTÁ D.C.* Bogota.

Marina. (19 de 04 de 2021). *Atico34*. Obtenido de https://protecciondatos-lopd.com/empresas/seguridad-perimetral-informatica/

Motadata. (15 de 02 de 2020). *Motadata*. Obtenido de www.motadata.com: https://www.motadata.com/es/what-is-it-service-management/#top

Nicomedes, E. (2017). *TIPOS DE INVESTIGACIÓN.* CORE.

Pérez Legoas, L. A. (2010). *Estadística Básica.* Lima: San Marcos.

Rodríguez, D. (17 de 9 de 2020). *Lifeder*. Obtenido de https://www.lifeder.com/investigacion-basica/

Romero Saldaña, M. (3 de 9 de 2016). *Metodología de la investigación Pruebas de bondad de ajuste a una distribución normal.* Obtenido de Metodología de la investigación Pruebas de bondad de ajuste a una distribución normal web site: https://dialnet.unirioja.es/descarga/articulo/5633043.pdf

Rubi. (26 de 02 de 2019). *protecciondatos*. Obtenido de https://www.protecciondatos.org/seguridad-perimetral/

RUIZ VIEIRA, K. E. (2018). *Implementación de una solución de seguridad perimetral Open Source en La Red Implementación de una solución de seguridad perimetral Open Source en La Red.* Chiclayo.

Sáez, J. M. (2017). *Investigación educativa. fundamentos teóricos, procesos y elementos prácticos (enfoque práctico con ejemplos. esencial para tfg, tfm y tesis).* Madrid: Editorial UNED. Obtenido de https://books.google.com.pe/books?id=c3CZDgAAQBAJ&pg=PT70&dq=tecnicas+e+instrumentos+de+investigacion+tesis+2017&hl=es&sa=X&ved=0ahUKEwjo-fTFnazeAhVFy1MKHen5AmcQ6AEILzAB#v=onepage&q&f=false

Salas, & Héctor. (2011). INVESTIGACIÓN CUANTITATIVA. *Scielo*, 21.

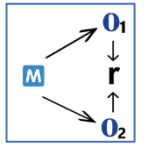
ServiceDesk. (26 de 05 de 2020). *www.manageengine.com*. Obtenido de https://www.manageengine.com/latam/service-desk/itsm/guia-para-principiantes.html#benefits?toc

Unir. (30 de 07 de 2020). *La Universidad en Internet*. Obtenido de https://www.unir.net/ingenieria/revista/seguridad-perimetral-informatica/

UNL. (2021). *UNL.* Obtenido de http://www.unl.edu.ar/ingreso/cursos/cac/21ot/

ANEXOS

Anexos N° 1: Matriz de consistencia.

<table>
<tr><th>FORMULACIÓN DEL PROBLEMA</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th>VARIABLES/DIMENSIONES E INDICADORES</th><th>METODOLOGÍA DE LA INVESTIGACIÓN</th></tr>
<tr>
<td>¿De qué manera la Seguridad Perimetral Informática se relaciona con la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana: 2021?</td>
<td>Determinar en nivel de relación entre la Seguridad Perimetral Informática y la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana: 2021.</td>
<td>La Seguridad Perimetral Informática se relaciona con la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana: 2021.</td>
<td rowspan="2">Variable independiente: Seguridad Perimetral de TI
<table>
<tr><th>Dimensión</th><th>Indicador</th></tr>
<tr><td>Políticas</td><td>Documentos</td></tr>
<tr><td></td><td>Difusión</td></tr>
<tr><td>Control de accesos</td><td>Identificación y control de usuarios</td></tr>
<tr><td></td><td>Gestión de claves de acceso</td></tr>
<tr><td></td><td>Sistemas biométricos</td></tr>
<tr><td></td><td>Registros de acceso al personal y terceros</td></tr>
<tr><td>Seguridad en la Operación</td><td>Respaldo de información.</td></tr>
<tr><td></td><td>Aplicación o software de terceros.</td></tr>
<tr><td></td><td>Contingencia</td></tr>
<tr><td>Seguridad en las Telecomunicaciones</td><td>Firewalls o cortafuegos</td></tr>
<tr><td></td><td>Sistemas (IDS/IPS)</td></tr>
<tr><td></td><td>Honeypots</td></tr>
<tr><td></td><td>Pasarelas antivirus y antispam</td></tr>
<tr><td>Adquisición, desarrollo y mantenimiento de SI</td><td>Participación</td></tr>
<tr><td></td><td>Registro</td></tr>
<tr><td>Gestión de incidentes en la Seg. Inf.</td><td>Registro</td></tr>
</table>
Variable dependiente: Gestión de Servicios de TI.
<table>
<tr><th>Dimensión</th><th>Indicador</th></tr>
<tr><td>Personal y Organización</td><td>Cultura Organizacional</td></tr>
<tr><td></td><td>Objetivos</td></tr>
<tr><td></td><td>Estrategias</td></tr>
<tr><td></td><td>Documentos de Gestión</td></tr>
<tr><td>Información y tecnología</td><td>Hardware</td></tr>
<tr><td></td><td>Software</td></tr>
<tr><td></td><td>Servicios</td></tr>
<tr><td>Proveedores y Socios</td><td>Registro</td></tr>
<tr><td>Flujo de valor y Procesos</td><td>Registro</td></tr>
</table>
</td>
<td rowspan="2">Tipo de investigación: Básica
Nivel de investigación: Descriptivo
Población: La población está constituido por 8221 personas que conformar a estudiantes, docentes y administrativos.
Muestra: Se aplicarán los fundamentos estadísticos, con un muestreo NO PROBALISTICO POR CONVENIENCIA ya que la población está conformada por una cantidad por 187 personas.
Diseño de la investigación: Correlacional – No experimental


Dónde:
<table>
<tr><th>Icono</th><th>Significado</th></tr>
<tr><td>M</td><td>Muestra</td></tr>
<tr><td>O1</td><td>Seguridad Perimetral</td></tr>
<tr><td>O2</td><td>Gestión de Servicios de TI</td></tr>
<tr><td>r</td><td>Relación entre variables</td></tr>
</table>
Tratamiento de datos. El tratamiento se efectuará a través de la herramienta IBM SPSS Stadistics versión 19.
<table>
<tr><th>Fuentes</th><th>Técnicas</th><th>Instrumentos</th></tr>
<tr><td>Primaria</td><td>Encuesta</td><td>-Cuestionarios</td></tr>
<tr><td>Secundaria</td><td>Análisis documental</td><td>-Resumen de autores.</td></tr>
</table>
</td>
</tr>
<tr>
<td>1. ¿Cómo la Seguridad Perimetral Informática se relaciona con el Personal y Organización de las Universidades Públicas de la Amazonía Peruana:2021?
2. ¿En qué medida la Seguridad Perimetral Informática se relaciona con la Información y Tecnología en las Universidades Públicas de la Amazonía Peruana:2021?
3. ¿De qué manera la Seguridad Perimetral Informática se relaciona con los Proveedores y Socios en las Universidades Públicas de la Amazonía Peruana:2021?
4. ¿En qué medida la Seguridad Perimetral Informática se relaciona con el Flujo de valor y Procesos en las Universidades Públicas de la Amazonía Peruana:2021?</td>
<td>1. Identificar el nivel de relación entre la Seguridad Perimetral Informática con el Personal y la Organización en las Universidades Públicas de la Amazonía Peruana:2021
2. Establecer el nivel de relación entre la Seguridad Perimetral Informática y la Información y tecnología en las Universidades Públicas de la Amazonía Peruana:2021
3. Conocer el nivel de relación entre la Seguridad Perimetral Informática y los Proveedores y Socios en las Universidades Públicas de la Amazonía Peruana:2021
4. Determinar el nivel relación entre la Seguridad Perimetral Informática y el Flujo de valor y Procesos en las Universidades Públicas de la Amazonía Peruana:2021</td>
<td>1. La Seguridad Perimetral Informática se relaciona con el Personal y Organización en las Universidades Públicas de la Amazonía Peruana: 2021
2. La Seguridad Perimetral Informática se relaciona con la Información y tecnología en las Universidades Públicas de la Amazonía Peruana: 2021
3. La Seguridad Perimetral Informática se relaciona con los Proveedores y Socios en las Universidades Públicas de la Amazonía Peruana: 2021
4. La Seguridad Perimetral Informática se relaciona con el Flujo de valor y Procesos en las Universidades Públicas de la Amazonía Peruana: 2021.</td>
</tr>
</table>

Anexos N° 2: Base de datos

	Políticas			Aspectos Organizativos			Control de accesos					Seguridad en la Operación				Seguridad en las Telecomunicaciones													Adquisición, desarrollo			Gestión de incidentes			variable 1
Codigo	Item 1	Item 2		Item 3	Item 4		Item 5	Item 6	Item 7	Item 8		Item 9	Item 10	Item 11		Item 12	Item 13	Item 14	Item 15	Item 16	Item 17	Item 18	Item 19	Item 20	Item 21	Item 22	Item 23		Item 24	Item 25		Item 26	Item 27		
1	3	1	2	4	5	5	1	3	1	2	2	2	4	2	3	3	2	4	2	3	2	2	3	3	2	2	2	3	4	5	5	2	3	3	3
2	4	5	5	2	2	2	2	3	1	4	3	2	1	2	2	3	3	2	2	2	5	3	4	3	2	4	2	3	2	2	2	2	4	3	3
3	3	1	2	3	5	4	3	5	2	3	3	5	4	2	4	5	4	3	2	3	3	5	5	5	4	4	4	4	3	5	4	3	5	4	4
4	4	3	4	3	4	4	1	3	3	3	3	3	1	2	2	4	5	5	2	5	2	3	5	2	2	5	4	4	3	4	4	3	2	3	3
5	5	3	4	2	4	3	3	3	4	1	3	4	1	5	3	5	4	4	5	5	3	4	5	4	3	5	2	4	2	4	3	5	5	5	4
6	2	4	3	3	4	4	4	1	5	3	3	4	2	4	3	4	2	2	5	5	4	4	3	2	3	4	3	3	3	4	4	5	4	5	4
7	2	2	2	4	4	4	2	5	4	4	4	4	2	2	3	4	2	5	2	4	5	2	3	4	3	5	5	3	2	4	3	5	2	4	3
8	3	3	3	2	3	3	3	3	1	3	3	1	4	4	3	4	5	2	5	2	4	5	3	2	4	5	2	4	2	3	3	2	5	4	3
9	3	2	3	4	4	4	1	1	3	3	2	1	5	3	3	3	4	5	5	3	3	3	5	2	3	5	3	4	2	2	2	5	2	4	3
10	3	4	4	2	4	3	5	2	4	5	4	5	2	5	4	3	5	3	4	2	4	5	2	5	5	5	2	4	2	4	3	5	3	4	4
11	5	5	5	5	4	5	5	2	5	2	4	5	4	3	4	5	2	4	5	5	4	2	3	5	5	3	2	4	5	2	4	4	3	4	4
12	4	1	3	4	4	4	1	2	5	1	2	1	2	1	1	5	5	5	4	3	3	5	4	5	5	5	3	4	4	4	4	5	2	4	3
13	4	1	3	5	4	5	4	5	5	3	4	5	3	5	4	5	3	4	4	3	4	2	2	3	2	3	3	3	5	2	4	2	3	3	4
14	3	1	2	5	4	5	3	2	3	1	2	2	2	5	3	3	2	5	5	5	4	4	5	4	5	2	3	4	5	2	4	5	3	4	3
15	5	4	5	3	4	4	2	5	2	3	3	1	5	5	4	2	5	5	2	5	3	5	2	4	4	3	5	4	3	2	3	5	5	5	4
16	3	2	3	4	4	4	2	1	1	5	2	4	1	3	3	3	5	3	2	5	4	5	2	4	5	2	2	4	2	2	2	5	4	5	3
17	2	5	4	4	4	4	2	5	2	4	3	2	5	1	3	3	5	4	2	5	2	3	5	4	2	4	3	3	2	2	2	5	4	5	3
18	4	4	4	4	2	3	1	1	1	5	2	5	1	5	4	2	4	5	5	3	5	4	5	2	3	5	4	4	4	2	3	5	3	4	3
19	2	1	2	4	4	4	2	2	5	3	3	3	4	2	3	3	4	5	3	5	5	3	2	5	5	4	3	4	4	3	4	2	4	3	3
20	3	1	2	2	5	4	2	5	5	4	4	1	5	3	3	4	5	2	5	5	4	2	5	4	2	5	2	4	2	5	4	5	2	4	3
21	5	5	5	5	3	4	5	1	1	4	3	5	5	3	4	5	5	3	5	3	4	4	5	4	5	5	4	4	5	2	4	3	3	3	4
22	1	2	2	3	3	3	5	2	1	2	3	3	3	2	3	1	5	5	4	3	5	2	3	5	5	5	3	4	3	3	3	4	4	4	3
23	2	4	3	2	2	2	5	4	4	5	5	1	3	1	2	4	4	3	4	2	4	3	2	3	5	3	3	3	2	2	2	3	4	4	3
24	4	1	3	2	5	4	4	2	4	5	4	2	1	3	2	4	3	3	3	5	5	4	3	4	5	2	4	4	2	5	4	3	2	3	3
25	2	1	2	5	4	5	4	4	4	3	4	3	3	4	3	3	2	5	5	2	2	3	2	5	5	4	2	4	5	4	5	5	5	5	4
26	4	1	3	4	2	3	5	3	2	2	3	3	2	3	3	3	2	3	4	2	4	5	5	5	5	5	2	4	4	2	3	5	5	5	3
27	3	1	2	2	4	3	2	4	3	4	3	1	5	2	3	4	2	4	4	3	5	4	5	2	3	2	4	3	2	4	3	5	5	5	3
28	3	5	4	3	5	4	2	2	3	4	3	4	4	5	4	4	5	5	4	2	2	3	2	2	2	5	3	3	3	5	4	3	5	4	4
29	2	2	2	4	4	4	1	2	2	5	3	3	2	2	2	2	5	5	4	2	5	5	5	2	4	5	4	4	4	4	4	5	4	5	3
30	1	2	2	2	2	2	5	2	3	4	4	3	2	4	3	5	4	2	2	5	2	2	2	2	2	2	2	3	2	2	2	5	2	4	3
31	1	4	3	5	2	4	3	1	1	3	2	1	5	1	2	3	2	3	5	2	3	5	2	5	5	2	2	4	5	2	4	5	5	5	3
32	4	1	3	2	4	3	3	3	5	3	4	3	2	5	3	3	4	5	4	4	5	5	5	3	3	4	5	4	2	4	3	5	4	5	3
33	2	2	2	2	4	3	4	4	4	1	3	3	5	1	3	1	2	5	2	4	4	2	5	2	2	2	5	3	2	4	3	3	3	3	3
34	1	4	3	3	2	3	2	4	3	3	3	1	5	4	3	1	3	5	5	2	4	5	2	2	4	5	3	3	2	3	3	5	5	5	3
35	5	3	4	3	3	3	4	3	4	4	4	2	4	1	2	1	2	2	2	4	4	5	3	5	5	3	5	3	3	3	3	2	2	2	3
36	3	5	4	5	5	5	3	2	5	4	4	5	1	3	3	3	5	3	5	5	2	2	5	3	3	3	3	4	5	5	5	4	5	5	4
37	2	1	2	5	3	4	1	2	2	1	2	2	4	3	3	1	3	5	5	4	5	5	5	4	3	3	3	4	5	3	4	2	2	2	3
38	5	2	4	5	4	5	5	5	5	4	5	2	1	4	2	1	4	5	2	4	3	5	5	4	4	4	4	4	5	4	5	5	3	4	4
39	1	3	2	5	4	5	4	3	2	5	4	3	5	2	3	1	2	4	2	4	3	5	2	2	5	5	2	3	5	4	5	5	5	5	4
40	5	2	4	2	5	4	1	5	2	1	2	3	4	3	3	1	2	2	2	3	2	3	2	4	2	3	2	2	2	5	4	2	3	3	3
41	1	4	3	2	4	3	4	4	2	2	3	5	4	5	5	2	4	4	2	5	3	3	5	5	3	3	3	3	2	4	3	4	4	4	3
42	2	5	4	5	5	5	4	4	4	2	4	1	3	2	2	2	5	3	5	5	4	5	4	5	2	5	2	4	5	5	5	2	4	3	4
43	2	4	3	5	5	5	4	2	3	1	3	1	1	4	2	1	5	5	4	3	2	2	5	5	3	5	4	4	5	5	5	3	3	3	3
44	2	1	2	2	5	4	1	4	5	3	3	4	2	2	3	1	4	3	5	2	2	5	2	2	2	2	2	3	2	5	4	1	2	2	3
45	1	4	3	5	1	3	3	5	5	1	4	3	5	1	3	3	2	4	4	2	4	5	4	2	3	4	2	4	5	1	3	2	5	4	3
46	3	1	2	5	4	5	3	3	5	5	4	1	4	2	2	2	4	2	2	5	3	3	2	5	3	2	2	3	5	4	5	3	5	4	4

47	3	4	4	5	3	4	4	5	4	4	4	3	1	4	3	2	3	3	2	4	4	2	2	3	3	2	3	3	5	3	4	3	4	4	4
48	1	2	2	4	5	5	2	4	2	2	3	2	1	3	2	2	5	2	2	3	4	5	5	2	5	5	4	4	4	5	5	4	5	5	3
49	3	4	4	5	2	4	4	3	4	2	3	5	1	3	3	5	2	5	3	4	5	3	3	2	4	5	5	4	5	2	4	4	5	5	4
50	2	3	3	5	3	4	1	5	2	3	3	1	2	3	2	1	2	2	3	2	3	2	4	4	2	2	3	3	5	3	4	5	4	5	3
51	1	5	3	5	2	4	4	5	4	4	4	1	3	2	2	5	2	5	5	5	5	5	2	5	5	2	3	4	5	2	4	2	3	3	3
52	1	4	3	4	3	4	4	5	5	2	4	1	3	5	3	1	2	3	4	5	3	5	4	2	1	3	1	3	4	3	4	4	3	4	3
53	5	2	4	4	1	3	5	5	2	2	4	3	1	1	2	5	3	4	2	5	4	2	2	4	1	5	3	3	4	1	3	3	1	2	3
54	3	5	4	5	4	5	3	5	5	1	4	5	1	1	2	3	2	5	2	5	3	2	1	4	3	3	1	3	5	4	5	1	5	3	4
55	5	3	4	4	3	4	5	3	2	5	4	5	4	5	5	1	3	5	5	3	4	2	1	4	3	4	1	3	4	3	4	3	1	2	4
56	1	2	2	5	5	5	1	3	3	5	3	5	3	3	4	1	2	5	2	3	5	2	3	5	1	4	4	3	5	5	5	2	4	3	3
57	4	3	4	4	1	3	4	3	3	2	3	1	2	3	2	1	2	2	4	2	2	1	2	4	3	2	4	2	4	1	3	4	2	3	3
58	2	2	2	3	1	2	4	2	4	2	3	3	1	3	2	5	3	3	5	3	1	2	2	5	5	3	1	3	3	1	2	3	5	4	3
59	5	2	4	2	2	2	4	1	3	5	3	3	2	3	3	4	3	3	2	4	2	3	3	2	1	5	1	3	2	2	2	1	4	3	3
60	1	3	2	1	1	1	4	4	5	3	4	3	3	2	3	4	4	5	2	2	4	2	1	4	5	4	4	3	1	1	1	3	4	4	2
61	4	4	4	2	4	3	2	3	2	3	3	3	5	5	4	5	3	1	4	2	3	2	3	4	2	5	5	3	2	4	3	2	4	3	3
62	4	1	3	4	2	3	4	2	1	4	3	2	2	5	3	4	5	3	2	4	4	3	3	5	3	1	1	3	4	2	3	4	3	4	3
63	1	5	3	1	5	3	1	2	4	3	3	4	2	3	3	5	2	1	2	4	5	1	4	1	5	2	2	3	1	5	3	2	4	3	3
64	5	5	5	5	3	4	3	3	4	5	4	5	1	1	2	5	3	4	5	4	4	3	4	3	4	4	1	4	5	3	4	5	3	4	4
65	2	2	2	4	3	4	4	5	3	1	3	5	1	3	3	5	2	5	4	3	3	5	4	2	5	2	4	4	4	3	4	2	1	2	3
66	4	5	5	5	4	5	5	4	1	4	4	2	3	4	3	2	3	2	5	5	4	3	1	1	4	5	5	3	5	4	5	1	2	2	4
67	2	5	4	5	5	5	3	3	4	1	3	2	3	5	3	2	1	1	1	4	2	4	5	2	1	5	2	3	5	5	5	5	4	5	4
68	5	1	3	4	2	3	5	2	5	2	4	2	1	1	1	3	3	4	2	5	5	3	4	3	5	5	4	4	4	2	3	3	1	2	3
69	1	1	1	4	2	3	1	4	3	5	3	5	3	2	3	5	2	3	5	2	1	5	1	2	5	5	2	3	4	2	3	2	5	4	3
70	3	4	4	4	3	4	2	2	1	3	2	1	1	3	2	3	5	3	3	4	2	4	2	2	1	3	3	3	4	3	4	4	3	4	3
71	1	4	3	4	1	3	2	2	2	4	3	4	4	5	4	3	3	1	2	2	3	4	4	4	4	5	2	3	4	1	3	1	1	1	3
72	5	1	3	5	5	5	1	1	4	1	2	5	2	5	4	4	3	4	1	4	4	2	2	4	5	1	1	3	5	5	5	5	5	5	4
73	1	3	2	5	4	5	1	4	1	1	2	4	4	4	4	2	4	3	3	3	3	3	5	4	2	3	2	3	5	4	5	3	3	3	3
74	5	5	5	5	2	4	3	4	3	1	3	1	2	2	2	2	1	5	4	5	3	1	4	5	2	3	2	3	5	2	4	4	4	4	3
75	3	1	2	3	1	2	2	1	5	1	2	2	4	2	3	3	1	1	2	3	1	5	1	4	3	3	3	3	3	1	2	1	3	2	2
76	2	4	3	2	4	3	3	2	5	4	4	5	3	4	4	5	5	5	4	4	4	2	1	2	1	4	4	3	2	4	3	2	5	4	3
77	2	2	2	5	2	4	3	1	5	2	3	1	2	3	2	3	4	3	1	1	5	1	2	1	3	2	3	3	5	2	4	2	3	3	3
78	3	5	4	2	3	3	2	3	2	4	3	1	4	5	3	3	1	3	2	5	4	4	4	3	2	1	1	3	2	3	3	1	4	3	3
79	4	3	4	2	4	3	3	2	1	5	3	2	4	1	2	5	4	5	5	3	1	4	3	5	4	5	4	4	2	4	3	4	4	4	3
80	2	3	3	4	4	4	4	4	4	1	3	5	1	3	3	2	1	4	4	1	2	3	5	1	5	5	3	3	4	4	4	4	4	4	3
81	1	1	1	3	3	3	1	4	5	1	3	4	5	2	4	3	5	3	4	1	5	1	1	1	3	3	4	3	3	3	3	1	3	2	3
82	5	2	4	2	4	3	2	5	2	5	4	3	2	3	3	1	1	2	2	5	2	4	5	1	3	4	1	3	2	4	3	5	1	3	3
83	2	4	3	5	5	5	3	2	1	2	2	1	2	1	1	4	4	5	1	4	3	2	1	1	5	4	5	3	5	5	5	5	4	5	3
84	2	5	4	5	3	4	1	1	3	5	3	1	1	3	2	2	3	3	2	1	3	4	2	2	5	4	2	3	5	3	4	2	2	2	3
85	1	2	2	1	4	3	2	3	2	2	2	3	3	2	3	4	4	5	5	4	4	4	5	2	3	4	5	4	1	4	3	5	4	5	3
86	3	3	3	5	5	5	1	1	1	2	1	5	2	1	3	2	2	1	3	2	5	4	2	1	1	4	2	3	5	5	5	4	3	4	3
87	2	1	2	1	1	1	3	5	4	1	3	2	2	2	2	2	1	4	5	3	5	5	5	2	5	2	1	3	1	1	1	2	3	3	2
88	2	2	2	1	4	3	1	2	1	1	1	4	5	5	5	2	1	4	4	1	5	1	1	5	2	4	3	3	1	4	3	3	4	4	3
89	2	4	3	5	5	5	1	5	1	4	3	2	3	3	3	3	4	2	3	3	5	1	5	4	3	5	2	4	5	5	5	4	3	4	4
90	4	4	4	1	5	3	2	2	4	1	2	5	3	5	4	3	4	4	5	5	1	2	5	2	3	3	3	3	1	5	3	2	2	2	3
91	2	5	4	1	5	3	3	3	3	2	3	4	2	3	3	4	3	5	1	5	5	5	4	5	4	4	5	4	1	5	3	4	3	4	3
92	2	1	2	5	1	3	1	3	4	2	3	1	4	4	3	3	3	1	4	1	3	5	4	4	3	1	1	3	5	1	3	4	2	3	3
93	1	3	2	5	1	3	1	1	2	4	2	2	4	5	4	4	2	3	1	3	2	5	4	2	5	2	3	3	5	1	3	2	1	2	3
94	5	5	5	3	4	4	2	2	4	4	3	5	5	2	4	2	3	5	4	2	1	4	2	3	4	1	1	3	3	4	4	5	1	3	4
95	2	5	4	4	4	4	1	5	3	2	3	4	4	4	4	1	3	3	3	2	3	2	4	5	1	2	4	3	4	4	4	5	4	5	4
96	3	2	3	3	2	3	2	5	4	3	4	4	2	2	3	1	1	4	3	1	2	5	2	1	2	4	1	2	3	2	3	5	5	5	3
97	3	5	4	4	5	5	2	3	3	1	2	5	2	1	3	3	4	5	1	3	5	1	4	3	3	5	3	3	4	5	5	5	5	5	4
98	3	3	3	3	3	3	3	4	5	2	4	1	1	2	1	2	5	3	2	5	5	3	3	5	1	1	3	3	3	3	3	1	2	2	3
99	1	1	1	2	5	4	1	5	4	1	3	2	5	1	3	3	4	2	5	1	3	5	2	1	4	4	5	3	2	5	4	5	3	4	3
100	4	4	4	1	4	3	2	1	3	1	2	2	5	4	4	4	2	4	5	3	2	5	5	1	2	1	3	3	1	4	3	5	5	5	3

101	5	3	4	4	5	5	1	4	5	4	4	5	5	2	4	3	4	3	1	3	3	4	1	1	2	1	1	3	4	5	5	2	5	4	4
102	1	2	2	2	5	4	1	5	4	2	3	4	4	1	3	3	5	2	1	2	1	4	4	4	4	2	1	3	2	5	4	4	5	5	3
103	2	4	3	3	5	4	4	5	1	2	3	2	4	4	3	3	4	5	1	3	2	3	2	1	2	4	3	3	3	5	4	3	3	3	3
104	5	3	4	2	2	2	1	3	1	5	3	2	3	2	2	3	1	2	3	5	4	5	4	4	1	2	2	3	2	2	2	3	3	3	3
105	1	5	3	3	4	4	2	5	4	5	4	4	5	3	4	4	3	2	2	5	4	1	1	1	4	2	3	3	3	4	4	2	4	3	3
106	1	3	2	2	5	4	4	2	1	4	3	5	2	5	4	5	4	1	2	2	3	5	2	2	4	5	5	3	2	5	4	3	3	3	3
107	4	1	3	2	4	3	4	2	5	2	3	5	3	4	4	1	5	5	4	5	3	2	2	3	3	5	3	3	2	4	3	2	2	2	3
108	1	3	2	4	1	3	1	2	3	1	2	5	5	5	5	1	2	1	2	3	5	2	3	3	1	5	5	3	4	1	3	1	2	2	3
109	1	5	3	1	3	2	5	5	1	1	3	1	3	2	2	3	1	3	4	4	3	4	2	2	5	1	3	3	1	3	2	4	5	5	3
110	1	5	3	2	3	3	2	1	1	1	1	2	2	1	2	1	4	5	5	2	5	4	5	5	4	3	4	4	2	3	3	3	1	2	2
111	2	1	2	2	2	2	5	3	5	1	4	1	3	1	2	4	1	1	5	5	1	2	3	5	1	2	3	3	2	2	2	5	2	4	2
112	4	4	4	4	5	5	3	3	2	2	3	2	5	1	3	1	3	3	5	5	3	4	3	1	4	4	4	3	4	5	5	4	4	4	4
113	1	5	3	5	1	3	3	4	1	1	2	1	5	1	2	3	3	4	2	1	5	2	2	4	3	4	1	3	5	1	3	5	4	5	3
114	1	1	1	2	2	2	5	4	2	3	4	3	1	3	2	5	2	2	4	2	2	5	5	4	2	5	3	3	2	2	2	2	1	2	3
115	5	3	4	3	1	2	5	4	3	5	4	5	1	5	4	2	2	2	5	1	2	2	1	4	1	5	2	3	3	1	2	2	1	2	3
116	1	1	1	3	5	4	5	3	2	3	3	3	1	1	2	2	5	5	3	5	4	4	3	5	2	1	3	4	3	5	4	3	2	3	3
117	4	5	5	4	4	4	1	1	5	5	3	2	3	4	3	3	3	3	4	2	5	4	2	1	1	2	4	3	4	4	4	2	4	3	3
118	3	2	3	2	2	2	3	4	2	3	3	2	5	1	3	1	2	2	3	2	5	5	4	4	1	1	2	3	2	2	2	1	2	2	2
119	4	3	4	4	1	3	3	5	1	2	3	4	5	2	4	2	1	4	3	5	3	5	5	4	4	2	2	4	4	1	3	3	1	2	3
120	4	4	4	3	4	4	1	1	1	5	2	3	5	5	4	4	4	1	1	1	1	1	1	5	2	2	2	2	3	4	4	3	3	3	3
121	3	1	2	4	2	3	3	5	1	2	3	2	5	3	3	4	2	5	2	2	5	5	1	4	5	2	1	3	4	2	3	2	3	3	3
122	2	5	4	5	3	4	1	2	4	4	3	5	2	1	3	3	3	5	4	5	4	1	4	3	3	5	2	4	5	3	4	4	3	4	3
123	3	5	4	5	5	5	1	3	4	4	3	2	2	1	2	2	1	5	3	3	2	3	1	2	1	4	4	3	5	5	5	5	1	3	3
124	1	2	2	4	3	4	2	3	1	1	2	1	4	5	3	5	4	2	5	4	4	5	5	1	4	4	5	4	4	3	4	5	3	4	3
125	4	4	4	2	5	4	4	2	5	2	3	1	1	4	2	2	1	2	2	5	4	4	4	3	2	3	3	3	2	5	4	4	3	4	3
126	1	1	1	3	4	4	4	4	5	2	4	4	2	4	3	5	2	4	1	4	5	1	2	1	1	5	3	3	3	4	4	3	5	4	3
127	4	4	4	5	3	4	2	5	2	3	3	3	4	2	3	2	3	3	3	2	3	4	5	4	1	2	4	3	5	3	4	5	5	5	4
128	1	1	1	5	1	3	2	3	3	4	3	5	3	1	3	1	2	1	4	4	5	4	5	5	1	2	5	3	5	1	3	4	4	4	3
129	4	4	4	4	1	3	1	5	1	5	3	2	5	4	4	4	3	3	5	3	3	4	5	5	1	5	2	4	4	1	3	3	3	3	3
130	4	1	3	3	4	4	2	4	2	4	3	3	3	3	3	4	4	2	2	2	4	3	4	3	2	4	4	3	3	4	4	5	5	5	3
131	1	2	2	1	4	3	3	3	4	2	3	4	4	4	4	4	5	1	3	4	4	2	3	2	3	3	2	3	1	4	3	2	4	3	3
132	4	1	3	4	5	5	1	2	4	5	3	5	1	4	3	5	4	3	2	5	3	1	3	2	4	5	4	3	4	5	5	4	4	4	4
133	3	3	3	4	4	4	2	3	3	5	3	3	5	2	3	5	5	2	1	5	5	2	2	5	3	3	4	4	4	4	4	4	2	3	3
134	2	5	4	5	4	5	4	3	3	3	3	3	3	3	3	2	2	4	3	3	5	3	1	5	2	4	2	3	5	4	5	1	5	3	4
135	4	2	3	5	5	5	5	1	2	3	3	1	5	3	3	1	1	4	3	5	1	1	3	1	3	2	2	3	5	5	5	1	5	3	3
136	2	4	3	3	1	2	2	5	1	3	3	2	5	1	3	4	2	4	2	3	5	3	2	5	1	2	2	3	3	1	2	5	5	5	3
137	5	5	5	3	3	3	4	3	5	3	4	1	1	5	2	5	1	4	3	2	4	1	3	4	3	4	5	3	3	3	3	4	4	4	3
138	2	3	3	1	1	1	5	1	3	1	3	5	3	2	3	4	2	1	2	4	5	1	4	2	3	2	1	3	1	1	1	1	4	3	2
139	3	3	3	5	3	4	4	4	1	3	3	2	3	2	2	3	5	4	1	2	2	5	4	4	4	1	4	3	5	3	4	4	3	4	3
140	4	5	5	3	4	4	4	5	2	4	4	3	3	3	3	2	2	2	2	2	4	3	4	5	5	5	5	3	3	4	4	1	1	1	3
141	2	2	2	2	2	2	5	1	5	1	3	2	4	3	3	1	3	4	1	3	1	4	5	4	5	3	2	3	2	2	2	2	3	3	3
142	2	1	2	1	1	1	5	5	5	2	4	2	5	2	3	4	5	4	5	5	4	1	4	2	4	1	5	3	1	1	1	3	3	3	2
143	5	1	3	3	5	4	2	1	2	3	2	4	3	1	3	5	3	3	5	2	4	1	4	4	1	2	3	3	3	5	4	4	2	3	3
144	2	1	2	3	1	2	2	2	2	5	3	3	2	5	3	2	5	2	2	3	2	1	1	4	1	5	4	3	3	1	2	3	1	2	2
145	2	3	3	5	5	5	4	5	4	1	4	1	3	1	2	3	3	2	1	3	3	3	4	2	3	1	3	3	5	5	5	3	5	4	3
146	2	4	3	4	1	3	3	1	1	4	2	2	2	3	2	2	4	5	3	1	4	1	1	5	3	4	1	3	4	1	3	4	2	3	3
147	1	3	2	1	1	1	2	1	5	1	2	3	3	1	2	1	5	5	3	5	3	1	3	3	2	5	3	1	1	1	1	2	1	2	2
148	1	5	3	5	2	4	1	5	2	1	2	1	4	1	2	3	1	1	4	1	1	2	1	5	3	3	1	3	5	2	4	3	2	3	3
149	4	4	4	1	3	2	1	5	3	2	3	3	3	1	2	2	4	4	4	2	2	2	4	1	1	2	1	2	1	3	2	4	1	3	3
150	1	1	1	2	5	4	3	1	5	5	4	4	3	4	4	2	4	2	5	5	4	1	4	2	1	1	1	3	2	5	4	2	4	3	3
151	2	1	2	1	4	3	5	5	5	2	4	4	4	3	4	4	2	5	2	1	5	4	5	3	2	1	1	3	1	4	3	5	2	4	3
152	2	2	2	3	3	3	3	4	3	1	3	2	2	3	2	3	4	4	3	2	4	1	2	4	2	4	3	3	3	3	3	2	4	3	3
153	3	5	4	5	2	4	2	1	2	2	2	3	5	1	3	3	4	4	5	4	4	4	4	3	5	1	5	4	5	2	4	2	3	3	3
154	4	1	3	4	1	3	4	4	2	1	3	4	1	2	2	1	2	1	4	5	3	4	1	2	4	4	1	3	4	1	3	2	3	3	3
155	2	1	2	3	1	2	3	2	1	4	3	2	1	5	3	5	2	2	2	1	3	3	5	2	2	3	4	3	3	1	2	1	1	1	2
156	4	5	5	5	4	5	5	4	2	2	3	3	3	1	2	4	3	1	5	3	3	5	5	4	3	5	1	4	5	4	5	4	2	3	4
157	2	2	2	3	2	3	3	2	1	2	2	2	2	2	2	3	5	2	4	1	2	5	4	2	1	3	1	3	3	2	3	1	2	2	2
158	3	2	3	4	2	3	1	3	5	4	3	4	3	3	3	1	2	1	4	3	1	1	4	3	2	2	4	3	2	4	2	3	1	5	3
159	1	5	3	2	2	2	4	1	1	2	2	3	5	2	3	5	1	1	2	5	1	4	3	4	1	3	2	3	2	2	2	1	3	2	2
160	2	5	4	4	3	4	3	3	3	2	3	4	3	1	3	1	1	4	1	5	3	3	4	4	4	1	3	3	4	3	4	3	4	4	3
161	1	5	3	1	1	1	3	5	5	4	4	4	5	5	5	4	5	2	2	1	4	5	2	3	3	5	5	3	1	1	1	2	2	2	3
162	4	1	3	2	5	4	3	5	4	4	4	2	3	5	3	2	3	2	4	2	3	5	2	2	4	2	3	3	2	5	4	3	4	4	3
163	1	2	2	4	2	3	4	4	3	2	3	5	2	1	3	4	4	3	5	4	5	1	2	1	2	4	2	3	4	2	3	3	5	4	3
164	2	5	4	2	3	3	3	2	2	5	3	2	5	4	4	1	4	5	5	3	3	1	1	3	2	1	3	3	2	3	3	3	1	2	3
165	1	3	2	5	1	3	4	3	4	4	4	4	3	2	3	5	5	1	1	3	5	2	3	5	1	5	2	3	5	1	3	1	3	2	3
166	1	4	3	5	3	4	5	3	1	4	3	2	5	2	3	2	4	4	4	5	1	2	3	2	3	2	2	3	5	3	4	2	2	2	3
167	2	1	2	3	4	4	2	3	1	5	3	4	4	3	4	1	4	5	3	3	5	3	4	1	5	4	2	3	3	4	4	1	4	3	3
168	5	2	4	2	4	3	3	2	3	3	3	3	3	4	3	4	2	5	3	1	2	3	2	3	3	1	3	3	2	4	3	3	5	4	3
169	1	5	3	1	1	1	3	3	3	3	3	2	1	2	2	3	3	3	2	5	1	2	1	2	2	2	1	1	1	5	3	4	2		
170	4	5	5	5	3	4	3	2	1	5	3	2	4	3	3	3	3	1	4	5	1	5	1	3	5	5	1	3	5	3	4	5	3	4	4
171	3	2	3	4	2	3	5	5	5	2	4	3	3	4	3	4	4	4	2	2	2	4	4	2	5	2	4	3	4	2	3	5	4	5	3
172	4	5	5	5	5	5	2	4	2	3	3	3	1	5	3	2	3	2	2	4	2	1	4	2	4	5	4	3	5	5	5	4	5	5	4
173	1	4	3	4	3	4	3	2	5	1	3	5	3	5	4	4	3	2	2	1	1	3	1	4	1	3	1	2	4	3	4	5	4	5	3
174	4	3	4	5	4	5	2	3	4	3	3	1	1	5	2	4	4	5	5	5	1	5	1	1	4	3	5	4	5	4	5	1	3	2	3
175	1	1	1	1	2	2	4	2	3	5	4	2	2	3	2	2	1	5	2	1	1	1	3	5	1	1	1	2	1	2	2	2	5	4	2
176	2	5	4	3	2	3	4	3	4	2	3	4	2	3	3	1	5	1	2	3	3	2	1	2	3	5	3	3	3	2	3	4	1	3	3
177	2	3	3	4	1	3	5	1	1	3	3	3	2	1	2	1	1	5	4	3	1	3	5	3	2	2	3	3	4	1	3	4	5	5	3
178	1	2	2	5	2	4	4	4	1	2	3	4	3	2	3	4	3	2	5	4	4	4	1	3	1	4	3	3	5	2	4	1	2	2	3
179	3	2	3	1	4	3	2	4	2	1	2	2	5	1	3	2	4	5	1	2	2	1	1	3	5	4	2	3	1	4	3	5	1	3	3
180	1	4	3	3	4	4	2	3	1	5	3	1	5	5	4	3	3	3	2	5	2	1	2	2	2	3	3	3	3	4	4	2	2	2	3
181	1	5	3	4	2	3	4	1	2	2	2	3	4	2	3	5	4	2	5	1	1	4	1	4	1	2	1	3	4	2	3	4	4	4	3
182	1	3	2	2	5	4	2	3	5	5	4	4	5	2	4	5	1	3	1	1	4	5	4	3	5	4	5	3	2	5	4	1	1	5	3
183	3	4	4	3	2	3	3	4	1	3	3	2	2	1	2	4	2	1	4	5	4	1	4	3	5	1	3	3	3	2	3	3	2	3	3
184	3	5	4	3	2	3	2	4	1	2	2	5	3	2	3	2	5	1	2	5	5	4	2	4	5	1	4	3	2	3	4	4	4	3	
185	5	2	4	1	4	3	1	3	1	5	3	4	2	2	3	2	1	2	3	2	4	4	4	2	1	5	2	3	1	4	3	4	1	3	3
186	4	5	5	1	5	3	3	5	2	5	4	5	5	4	5	3	1	5	5	4	5	2	3	1	5	2	1	3	1	5	3	4	2	3	4
187	4	3	4	2	3	3	1	2	2	4	2	3	5	2	3	2	1	5	2	5	5	2	1	5	4	5	5	3	2	3	3	1	1	1	3

Personal	Información y tecnología			Proveedores y Socios				Flujo de valor	Variable 2
Item 28	Item 29	Item 30		Item 31	Item 32	Item 33		Item 34	
5	2	2	2	2	5	5	4	1	3
5	2	4	3	3	5	2	3	1	3
5	5	5	5	5	4	5	5	5	5
5	5	4	5	4	2	2	3	1	3
5	2	5	4	5	5	2	4	1	3
5	5	2	4	2	5	4	4	5	4
5	4	5	5	4	2	5	4	5	5
5	5	3	4	2	5	2	3	5	4
5	2	4	3	2	5	2	3	1	3
5	4	4	4	4	5	5	5	5	5
5	5	5	5	2	5	2	3	5	5
5	2	4	3	2	4	2	3	1	3
5	4	5	5	2	5	4	4	5	5
5	5	3	4	5	2	3	3	5	4
5	4	4	4	5	5	2	4	5	5
5	2	5	4	5	2	2	3	5	4
5	5	3	4	5	5	2	4	5	5
5	5	3	4	5	2	2	3	5	4
5	5	5	5	5	3	5	4	5	5
5	4	4	4	2	4	4	3	5	4
5	5	3	4	4	4	2	3	5	4
5	3	3	3	2	5	2	3	5	4
5	5	5	5	2	2	4	3	5	4
1	2	5	4	5	4	2	4	1	2
5	5	5	5	5	4	4	4	5	5
5	5	5	5	2	5	5	4	5	5
5	2	2	2	2	5	5	4	5	4
1	4	4	4	4	2	4	3	1	2
1	3	5	4	2	2	4	3	1	2
5	5	4	5	5	4	2	4	5	5
1	4	2	3	2	2	3	2	1	2
5	4	2	3	5	5	4	5	5	4
1	5	5	5	2	3	4	3	1	3
5	3	5	4	5	2	2	3	5	4
5	2	3	3	3	5	3	4	1	3
5	4	5	5	2	4	4	3	5	4
1	3	3	3	3	5	3	4	5	3
5	5	5	5	2	3	2	2	1	3
5	4	3	4	5	5	4	5	5	5
1	5	2	4	2	4	3	3	1	2
5	5	4	5	2	5	2	3	5	4
5	5	4	5	2	2	2	2	5	4
5	4	2	3	2	2	3	2	5	4
1	2	4	3	5	4	2	4	1	2
5	5	1	3	2	4	1	2	5	4
5	4	5	5	2	2	4	3	5	4

5	4	1	3	2	1	2	2	5	4
5	4	4	4	4	4	4	4	5	5
5	2	3	3	4	1	4	3	5	4
5	2	3	3	5	1	5	4	5	4
1	5	1	3	5	2	3	3	1	2
5	2	4	3	4	1	4	3	5	4
1	1	1	1	1	3	3	2	1	1
5	5	1	3	2	5	3	3	5	4
5	2	4	3	5	4	2	4	5	4
5	1	4	3	3	2	3	3	5	4
1	5	1	3	3	3	1	2	5	3
1	1	2	2	4	3	2	3	1	2
5	5	1	3	5	4	5	5	5	4
5	4	3	4	1	2	2	2	5	4
5	3	2	3	3	3	3	3	5	4
5	2	4	3	5	2	3	3	5	4
5	5	4	5	1	2	1	1	5	4
5	4	4	4	1	5	3	3	5	4
5	5	4	5	4	2	4	3	5	4
1	3	1	2	3	1	2	2	5	3
5	1	4	3	3	4	1	3	5	4
1	5	3	4	3	5	1	3	1	2
5	5	1	3	4	5	4	4	5	4
1	5	1	3	2	3	1	2	2	2
1	3	2	3	4	2	4	3	5	3
5	3	5	4	1	3	3	2	5	4
5	2	4	3	1	1	5	2	2	3
5	2	5	4	5	4	1	3	5	4
2	5	2	4	3	1	4	3	2	3
5	4	5	5	4	3	2	3	5	4
2	4	1	3	1	5	4	3	1	2
2	2	3	3	1	1	3	2	5	3
2	5	4	5	2	4	1	2	3	3
5	4	3	4	3	3	1	2	5	4
2	5	4	5	1	5	2	3	1	3
5	4	4	4	4	4	5	4	5	5
2	5	4	5	5	3	2	3	5	4
5	3	4	4	4	5	3	4	2	4
5	1	5	3	3	3	3	3	5	4
2	1	4	3	5	5	2	4	2	3
2	3	2	3	5	1	4	3	2	2
2	3	4	4	5	2	4	4	2	3
2	4	3	4	2	3	1	2	2	2
5	4	2	3	4	5	5	5	5	4
2	4	1	3	4	4	2	3	5	3
2	3	1	2	5	1	4	3	2	2
5	4	4	4	2	5	2	3	2	4
5	5	5	5	2	4	4	3	5	5
5	4	2	3	5	1	4	3	2	3
2	3	4	4	2	5	4	4	5	4
5	5	3	4	4	5	3	4	5	5
2	3	1	2	5	1	5	4	2	2
2	3	3	3	3	5	3	4	2	3
5	2	3	3	1	5	4	3	5	4

5	2	3	3	4	2	3	3	5	4
5	5	5	5	4	3	4	4	2	4
5	4	2	3	2	5	5	4	5	4
5	4	2	3	2	3	4	3	5	4
2	3	2	3	2	3	4	3	5	3
2	2	4	3	2	4	1	2	5	3
5	5	4	5	2	3	5	3	5	4
2	1	4	3	1	1	5	2	5	3
2	1	4	3	1	4	1	2	2	2
2	3	5	4	2	1	5	3	5	3
5	3	3	3	3	4	1	3	2	3
2	4	4	4	5	1	3	3	2	3
5	2	2	2	2	5	1	3	5	4
2	2	2	2	4	4	2	3	1	2
2	1	1	1	1	1	2	1	2	2
2	4	5	5	5	1	3	3	2	3
2	4	5	5	1	2	1	1	5	3
5	5	3	4	1	4	4	3	2	4
5	5	4	5	1	4	3	3	5	4
5	5	2	4	1	4	1	2	2	3
2	4	2	3	1	2	5	3	2	2
5	1	2	2	4	1	5	3	5	4
2	1	4	3	3	5	5	4	5	3
2	5	1	3	3	1	3	2	5	3
2	5	2	4	5	3	2	3	5	3
2	5	1	3	2	5	3	3	2	3
5	1	2	2	2	3	5	3	5	4
2	4	2	3	5	5	1	4	2	3
5	5	2	4	4	1	1	2	5	4
5	4	3	4	5	3	3	4	5	4
2	5	2	4	1	4	1	2	5	3
5	2	3	3	1	2	5	3	3	3
2	5	3	4	2	2	3	2	5	3
5	4	3	4	4	5	5	5	5	5
5	5	5	5	2	5	3	3	1	4
2	2	4	3	3	3	1	2	5	3
2	5	4	5	2	2	4	3	5	4
2	4	4	4	1	4	1	2	2	3
5	5	1	3	5	1	3	3	5	4
5	2	4	3	1	5	3	3	5	4
2	2	1	2	2	4	4	3	5	3
5	4	4	4	1	4	3	3	5	4
5	2	2	2	4	5	2	4	5	4
2	1	5	3	3	5	1	3	2	3
2	4	2	3	3	5	2	3	2	3
2	5	1	3	1	5	1	2	2	2
2	3	2	3	2	4	1	2	2	2
2	5	2	4	3	1	4	3	5	3
2	1	5	3	1	3	3	2	5	3
2	4	1	3	1	3	4	3	2	2
5	3	4	4	2	1	5	3	2	3
2	1	4	3	5	4	1	3	5	3
2	5	3	4	1	4	2	2	2	3
5	1	5	3	3	4	4	4	5	4
2	4	3	4	2	2	1	2	2	2
2	4	2	3	3	2	3	3	5	3
2	2	2	2	2	3	2	2	2	2
2	5	2	4	3	2	4	3	2	3
2	1	5	3	1	3	5	3	2	3
5	1	5	3	3	2	1	2	2	3
2	3	5	4	1	2	1	1	2	2
2	2	1	2	2	4	4	3	5	3
2	5	4	5	2	1	3	2	2	3
5	3	5	4	4	1	4	3	5	4
2	1	1	1	4	4	5	4	2	2
5	3	2	3	5	4	5	5	5	4
2	5	2	4	3	1	3	2	2	2
2	5	4	5	3	1	2	2	5	3
2	1	5	3	2	2	4	3	5	3
5	4	5	5	2	2	2	2	5	4
5	3	2	3	4	1	2	2	5	4
2	1	3	2	5	4	1	3	2	2
5	4	1	3	1	2	4	2	5	4
2	3	2	3	1	1	5	2	2	2
2	1	3	2	3	4	1	3	2	2
2	3	3	3	2	2	4	3	5	3
2	5	2	4	2	5	4	4	5	4
2	5	5	5	5	3	3	4	2	3
2	3	1	2	5	1	4	3	2	2
2	4	1	3	1	2	1	1	2	2
5	4	3	4	1	1	3	2	5	4
2	5	2	4	5	5	3	4	5	4
5	4	5	5	2	2	3	2	2	3
5	4	2	3	3	5	3	4	5	4
5	4	1	3	5	4	4	4	5	4
5	5	5	5	5	2	1	3	5	4
5	4	1	3	2	5	4	4	2	3

Anexos N° 3: Cuestionario de preguntas para la recolección de datos

CUESTIONARIO DE PREGUNTAS SOBRE LA INVESTIGACIÓN "SEGURIDAD PERIMETRAL INFORMÁTICA Y LA GESTION DE SERVICIOS DE TI EN LAS UNIVERSIDADES PÚBLICAS DE LA AMAZONÍA PERUANA :2021

N° de cuestionario: _____

Fecha: _____

INDICACIONES

- Marque con X en el cuadro que considere el valor adecuado como respuesta a las preguntas específicas.

Escala de Likert

Tabla N° 41: Reseña de recolección de datos

Valor	Descripción
1	Nunca
2	Muy pocas veces
3	Algunas veces
4	Casi siempre
5	Siempre

PREGUNTAS GENERALES

Sexo: *a) M* *b) F*

Edad: *a) De 18 a 20 años* *b) De 21 a 40 años*

c) Mas de 40 años.

Condición: *a) Contratado* *b) Nombrado* *c) Locador*

PREGUNTAS ESPECÍFICAS

Tabla N° 42: Recolección de datos

N°	PREGUNTAS	1	2	3	4	5
VARIABLE 1: Base de datos del sistema de gestión de operaciones y procesos de giros radiales						
	DIMENSIÓN: Políticas					
P 01	La OGTISE cuenta con políticas de seguridad perimetral aprobadas.					
P 02	La OGTISE realiza reuniones de difusión de las políticas y/o procedimientos.					
	DIMENSIÓN: Aspectos Organizativos de la Seguridad de la Información					
P 03	La Universidad brinda las posibilidades necesarias para iniciar y controlar la implementación de políticas de seguridad.					
P 04	Las responsabilidades del personal OGTISE, con respecto a la seguridad perimetral están definidas de forma clara y precisa.					
	DIMENSIÓN: Control de accesos					
P 05	Las OGTISE lleva el control de las identificaciones y controles de acceso como parte de la seguridad perimetral.					
P 06	Las OGTISE gestiona las claves de acceso como parte de la seguridad perimetral (Registros).					
P 07	Las OGTISE hace uso de los sistemas biométricos de acceso a las instalaciones que deben estar aseguradas como la sala de servidores, gabinetes como parte de la seguridad perimetral					
P 08	Las OGTISE lleva el registro de los accesos del personal interno a las instalaciones que salvaguardan los activos de telecomunicación.					
	DIMENSIÓN: Seguridad en la Operación					
P 09	Las OGTISE realiza respaldo y registro de la información de base de datos					

P 10	Las OGTISE realiza registro de los respaldos de las bases de datos.
P 11	Las OGTISE gestiona los sistemas de contingencia a nivel físico y lógico de sus instalaciones.
	DIMENSIÓN: Seguridad en las Telecomunicaciones
P 12	El respaldo para el acceso a internet es.
P 13	El servicio de intranet es.
P 14	El servicio de extranet es.
P 15	El proceso de verificaciones de IP entrantes salientes y de aplicaciones es.
P 16	La frecuencia monitorización de tráfico en la LAN es.
P 17	La frecuencia monitorización de tráfico en la red Wireless es.
P 18	La cantidad de implementaciones de pasarelas antivirus y antispan es.
P 19	El nivel de detección y bloqueo de SPAM es.
P 20	El nivel de testeo basado en DNS, DNS Block list.
P 21	La cantidad de implementaciones de pasarelas antivirus y antispan es.
P 22	El nivel de detección y bloqueo de SPAM.
P 23	El nivel de testeo basado en DNS, DNS Block list.
	DIMENSIÓN: Adquisición, desarrollo y mantenimiento de los sistemas de información
P 24	La OGTISE forma parte del comité de evaluación y adquisiciones de soluciones relacionados a la seguridad perimetral
P 25	La OGTISE registra los datos de personal externo que ingresa a las instalaciones para el trabajo de mantenimiento de las soluciones de TI.
	DIMENSIÓN: Gestión de incidentes en la seguridad de la información
P 26	Las OGTISE lleva el registro de incidencias de copias de seguridad de datos y aplicaciones.
P 27	Las OGTISE lleva el registro de incidencias en las telecomunicaciones, clasificados por tipo o medio.
	VARIABLE 2: Gestión de Servicios de TI
	DIMENSIÓN: Personal y Organización
P 28	Se tiene definido la cultura organización a nivel de la OGTISE.
	DIMENSIÓN: Información y tecnología
P 29	La OGTISE cuenta con servidores adecuados para la necesidad de la Universidad

P 30	La OGTISE cuenta con sistemas de almacenamiento adecuando para necesidad de la Universidad
	DIMENSIÓN: Proveedores y Socios
P 31	La OGTISE cuenta con la cantidad de proveedores de TI de acuerdo a sus necesidades.
P 32	La OGTISE cuenta con una base de datos de proveedores de TI.
P 33	La OGTISE cuenta con interconexiones estrategias con otras Instituciones
	DIMENSIÓN: Flujo de valor y Procesos
P 34	La OGTISE cuenta con flujos de trabajo aprobados

Anexos N° 4: Validación de los instrumentos por expertos

I. DATOS PERSONALES

1.1. APELLIDO Y NOMBRE DEL INFORMANTE: .....
1.2. GRADO ACADÉMICO: .....
1.3. INSTITUCIÓN DONDE LABORA: .....
1.4. TÍTULO DE LA INVESTIGACIÓN: .....
.....
1.5. AUTOR DEL INSTRUMENTO: .....
1.6. NOMBRE DEL INSTRUMENTO: .....

II. ASPECTO A EVALUAR: (CALIFICACIÓN CUANTITATIVA)

INDICADORES DEL INSTRUMENTO DE EVALUACION	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-13)	Bueno (14-16)	Muy bueno (17-18)	Excelente (19-20)
01. CLARIDAD	Está formulado con lenguaje apropiado.					
02. OBJETIVIDAD	Está expresado con conductas observables.					
03. ACTUALIDAD	Adecuado al avance de la ciencia y calidad.					
04. ORGANIZACIÓN	Existe una organización lógica del instrumento.					
05. SUFICIENCIA	Valora los aspectos en cantidad y calidad.					
06. INTENCIONALIDAD	Adecuado para cumplir con los objetivos.					
07. CONSISTENCIA	Basado en el aspecto teórico científico del tema de estudios.					
08. COHERENCIA	Entre las hipótesis, dimensiones e indicadores.					
09. METODOLOGIA	Las estrategias responden al propósito del estudio.					
10. OPORTUNIDAD	Genera nuevas pautas para la investigación y construcción de teorías.					
Sub Total						
TOTAL						

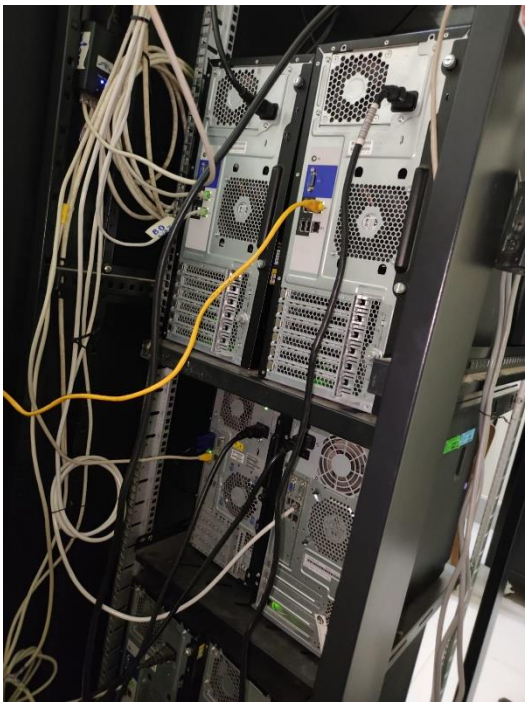
Valoración cuantitativa (total x0.4) .....
Valoración cualitativa .....
Valoración de aplicabilidad .....

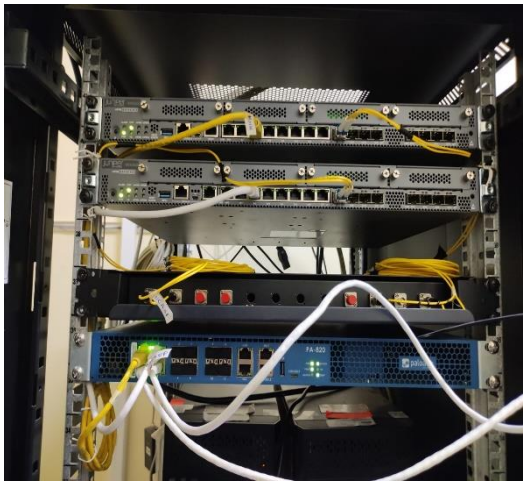
Leyenda:
01-13 Importante
14-16 Aceptable con recomendación
17-20 Aceptable

Lugar y Fecha: .....
Firma y Post – Firma del Experto: .....
DNI: .....

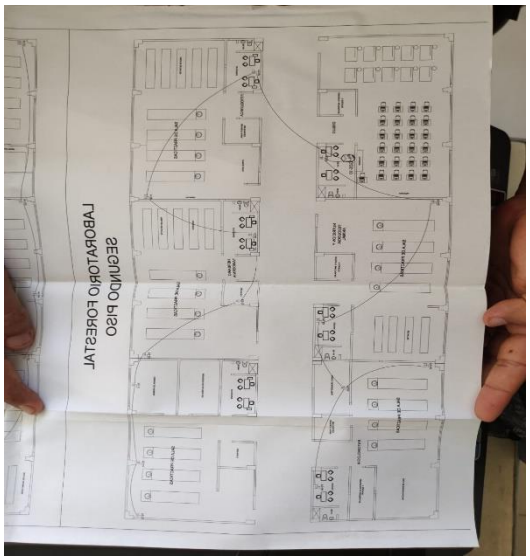
Anexos N° 5: Evidencias en la Universidad Nacional de Ucayali

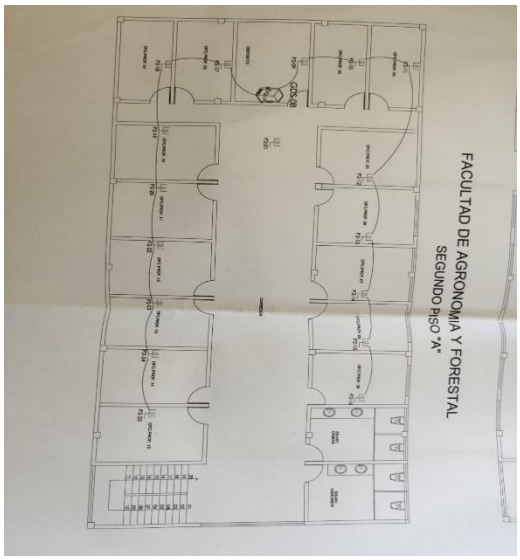












Anexos N° 6: Evidencias en la Universidad Nacional Intercultural de la Amazonia





Anexos N° 7: Constancias de ejecución de proyecto

CONSTANCIA DE EJECUCION DE PROYECTO DE INVESTIGACION

El que suscribe, Ing. CARLOS IVAN YNGUIL SANCHEZ. Otorga la presente constancia de ejecución del proyecto de investigación a:

Erick Erasmo Loli Romero, bachiller en Ingeniería de Sistemas, de la Facultad de Ingeniería de sistemas e Ingeniería Civil de la Universidad Nacional del Ucayali, de la promoción 2010 -I, con código de matrícula 0002100927, identificado con DNI Nro. 46471896.

Quien realizó la ejecución de su proyecto de investigación **"Seguridad Perimetral Informática y la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana"** para la obtención del título profesional, bajo mi supervisión, en el Periodo, desde el 02 de febrero hasta el 01 de setiembre del Año en Curso.

El tesista **Erick Erasmo Loli Romero** completó satisfactoriamente su investigación y mostró en todo momento eficiencia, puntualidad, responsabilidad y buena formación académica.

Se otorga la presente constancia para fines que el interesado considere conveniente.

Pucallpa, 21 de Octubre de 2022

UNIVERSIDAD NACIONAL INTERCULTURAL DE LA AMAZONIA
Ing. Carlos Iván Ynguil Sánchez
Jefe de la Unidad de Tecnologías de la Información

CONSTANCIA DE EJECUCION DE PROYECTO DE INVESTIGACION

El que suscribe, Ing. CARLOS IVAN YNGUIL SANCHEZ. Otorga la presente constancia de ejecución del proyecto de investigación a:

Jack Junior Torres Reátegui, bachiller en Ingeniería de Sistemas, de la Facultad de Ingeniería de sistemas e Ingeniería Civil de la Universidad Nacional del Ucayali, de la promoción 2010 -I, con código de matrícula 0002100960, identificado con DNI Nro. 72814818

Quien realizó la ejecución de su proyecto de investigación **"Seguridad Perimetral Informática y la Gestión de Servicios de TI en las Universidades Públicas de la Amazonía Peruana"** para la obtención del título profesional, bajo mi supervisión, en el Periodo, desde el 02 de febrero hasta el 01 de setiembre del Año en Curso.

El tesista **Jack Junior Torres Reátegui**, completó satisfactoriamente su investigación y mostró en todo momento eficiencia, puntualidad, responsabilidad y buena formación académica.

Se otorga la presente constancia para fines que el interesado considere conveniente.

Pucallpa, 21 de Octubre de 2022

UNIVERSIDAD NACIONAL INTERCULTURAL DE LA AMAZONIA
Ing. Carlos Iván Ynguil Sánchez
Jefe de la Unidad de Tecnologías de la Información