UNIVERSIDAD SEÑOR DE SIPÁN

ESCUELA DE POSGRADO

TESIS

METODOLOGÍA ADAPTATIVA BASADA EN UN MODELO DE SEGURIDAD INFORMÁTICA EN REDES PRIVADAS VIRTUALES PARA MEJORAR EL INTERCAMBIO DE INFORMACIÓN ACADÉMICA CONTEXTUALIZADA EN ENTORNOS DE CONEXIONES PÚBLICAS

PARA OBTENER EL GRADO ACADÉMICO DE DOCTOR EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS

Autor

Mg. Gilberto Carrión Barco

Asesor

Dr. Cristian Abraham Dios Castillo

Línea de Investigación:

Redes y Sistemas Distribuidos

Pimentel – Perú

2018

UNIVERSIDAD SEÑOR DE SIPÁN

ESCUELA DE POSGRADO

DOCTORADO EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS

"METODOLOGÍA ADAPTATIVA BASADA EN UN MODELO DE SEGURIDAD INFORMÁTICA EN REDES PRIVADAS VIRTUALES PARA MEJORAR EL INTERCAMBIO DE INFORMACIÓN ACADÉMICA CONTEXTUALIZADA EN ENTORNOS DE CONEXIONES PÚBLICAS"

AUTOR

Mg. GILBERTO CARRIÓN BARCO

PIMENTEL – PERÚ

2018

METODOLOGÍA ADAPTATIVA BASADA EN UN MODELO DE SEGURIDAD INFORMÁTICA EN REDES PRIVADAS VIRTUALES PARA MEJORAR EL INTERCAMBIO DE INFORMACIÓN ACADÉMICA CONTEXTUALIZADA EN ENTORNOS DE CONEXIONES PÚBLICAS

APROBACIÓN DE LA TESIS

_____

Dr. Callejas Torres Juan Carlos
Asesor Metodólogo

_____

Dr. Jorge Luis Gutiérrez Gutiérrez
Presidente del Jurado de Tesis

_____

Dr. Callejas Torres Juan Carlos
Secretario del Jurado de Tesis

_____

Dr. Dios Castillo Christian Abraham
Vocal del Jurado de Tesis

ÍNDICE

DEDICATORIA 11
AGRADECIMIENTO 12
RESUMEN 13
ABSTRACT 14
INTRODUCCIÓN 15
PRIMERA PARTE 26
METODOLOGÍA Y FUNDAMENTACIÓN DE LA INVESTIGACIÓN 26
CAPÍTULO 1. CONSTRUCCIÓN DEL MARCO TEÓRICO 27
Introducción 27
1.1. Caracterización del proceso de seguridad informática y su dinámica en redes privadas virtuales 27
1.2. Determinación de tendencias históricas del proceso de seguridad informática y su dinámica en redes privadas virtuales 41
Conclusiones parciales 59
CAPÍTULO 2. JUSTIFICACIÓN DEL PROBLEMA Y CARACTERIZACIÓN DEL CAMPO DE ACCIÓN 60
Introducción 60
2.1. Justificación del Problema 60
2.2. Diagnóstico del estado actual del proceso de seguridad informática y su dinámica en redes privadas virtuales de la Universidad Nacional Pedro Ruiz Gallo. 67
2.3. Marco conceptual 90
Conclusiones parciales 94
CAPÍTULO 3. HIPÓTESIS Y DISEÑO DE LA EJECUCIÓN 95
Introducción 95
3.1. Definición de la hipótesis 95
3.2. Determinación y conceptualización de las variables de la hipótesis 96
3.3. Diseño de la ejecución 97
3.3.1. Métodos de investigación científica y selección de técnicas, instrumentos, fuentes de verificación 97
a. Tipo de estudio y diseño de contrastación de hipótesis 97
b. Métodos, técnicas e instrumentos de recolección de datos 97
3.3.2. Universo 99
3.3.3. Selección de la muestra 99
3.3.4. Forma de tratamiento de los datos 100
Conclusiones parciales 100

SEGUNDA PARTE 102
CONSTRUCCIÓN DE LOS APORTES 102
CAPÍTULO 4. ELABORACIÓN DE UN MODELO DE SEGURIDAD INFORMÁTICA EN REDES PRIVADAS VIRTUALES 103
Introducción 103
4.1. Fundamentación del aporte teórico 103
4.2. Descripción argumentativa del aporte teórico 104
Conclusiones parciales 115
CAPÍTULO 5. ELABORACIÓN DE UNA METODOLOGÍA ADAPTATIVA PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD INFORMÁTICA EN REDES PRIVADAS VIRTUALES 116
Introducción 116
5.1. Relación entre aporte teórico y aporte práctico 116
5.2. Construcción del aporte práctico 117
A. Fundamentación 118
B. Diagnostico 119
C. Objetivo General 120
D. Etapas 120
ETAPA 1: DIMENSIÓN DE LA GESTIÓN DE CONECTIVIDAD DE LA RED 120
ETAPA 2: DIMENSIÓN DE LA GESTIÓN DE SEGURIDAD INFORMÁTICA 127
ETAPA 3: SEGUIMIENTO Y CONTROL 133
Conclusiones parciales 138
TERCERA PARTE 139
VALIDACIÓN DE LOS RESULTADOS 139
CAPÍTULO 6. VALORACIÓN Y CORROBORACIÓN DE LOS RESULTADOS 140
Introducción 140
6.1. Valoración de los resultados 140
6.2. Ejemplificación de la aplicación del aporte práctico 142
6.3. Corroboración estadística de las transformaciones logradas 146
6.4. Pre y Post Test de la variable dependiente: Intercambio de información académica contextualizada 147
Conclusiones parciales 148
CONCLUSIONES GENERALES 149
RECOMENDACIONES 151
REFERENCIAS BIBLIOGRÁFICAS 152
ANEXOS 155
Anexo 1. Matriz de consistencia 156

Anexo 2. Operacionalización de variables 157
Anexo 3. Encuesta a especialistas en tecnologías de la información de la entidad 158
Anexo 4. Encuesta a empleados administrativos de la entidad 160
Anexo 5. Validación del instrumento. Encuesta a especialistas en TI de la entidad 162
Anexo 6. Validación del instrumento. Encuesta a empleados administrativos de la entidad 163
Anexo 7. Validación del instrumento. Guía de observación.....164
Anexo 8. Modelo de encuesta aplicada a posibles expertos para determinar su nivel de competencia 165
Anexo 9. Validación de los aportes de la investigación a través de la selección de expertos ...167
Anexo 10. Identificación de usuarios 170
Anexo 11. Servicios de red.....171

ÍNDICE DE TABLAS

Tabla 1. *Comparación de protocolos para VPN*.....64
Tabla 2. *Puntuación de los Ítems en la escala de Likert*.....67
Tabla 3. *¿Considera usted, que los directivos o jefes inmediatos se involucran o comprometen en el desarrollo de proyectos relacionados a las TIC?* 68
Tabla 4. *¿Cree usted, que los especialistas en TIC de la Universidad, son responsables de sugerir nuevos proyectos en TIC?*.....69
Tabla 5. *¿Considera importante, realizar un diseño topológico de la red que permita el intercambio de información académica entre la Universidad sede Lambayeque y el Centro Pre Universitario Sede Chiclayo?* 70
Tabla 6. *¿Considera importante, que para conectarse a una red privada virtual desde el lugar donde se encuentre, es necesario contar con componentes móviles (conexión a internet, computador y software VPN instalado en la PC)?*.....71
Tabla 7. *¿Considera importante que, para conectarse a una red privada virtual desde una sede central o remota, es necesario contar con componentes corporativos (routers VPN, firewall, concentrador VPN)?* 72
Tabla 8. *¿Considera necesario, la identificación y aceptación de riesgos que se puedan presentar en la red telemática?*.....73
Tabla 9. *¿Cree usted, que la mitigación de riesgos contribuye a mejorar la seguridad informática en la red telemática?*.....74
Tabla 10. *¿Considera necesario, establecer controles de acceso físico a los ambientes de procesamiento de información?* 75
Tabla 11. *¿Considera necesario, establecer políticas de mantenimiento de equipamiento para los usuarios de la red telemática?*.....76
Tabla 12. *¿Cree usted necesario, establecer políticas de escritorios y pantallas limpias para los usuarios de la red telemática?* 77
Tabla 13. *¿Cree usted necesario implementar políticas de resguardo de información para los usuarios de la red telemática?* 78
Tabla 14. *¿Considera necesario, establecer controles de seguridad de los datos entre los usuarios de la red telemática?* 79
Tabla 15. *¿Considera importante que, como empleado de la entidad, usted es responsable de generar y consumir información?* 80
Tabla 16. *¿Cree usted, que ante la implementación de un nuevo proyecto de red es necesario que, como usuario, pueda indicar sus requerimientos para este proyecto?* 81

Tabla 17. *¿Considera usted, que los servicios de red (Telefonía IP, acceso a los sistemas de información, autenticación de usuarios) se han definido en función de los requerimientos del usuario?* 82
Tabla 18. *¿En la entidad, considera que cada de empleado accede de manera segura para conectarse a la red telemática?* 83
Tabla 19. *¿Considera que la información debe viajar encriptada y que no esté sujeta a interceptaciones por parte de usuarios maliciosos?* 84
Tabla 20. *¿Se siente seguro al enviar información por la red de la Universidad?* 85
Tabla 21. *¿Cree usted, que su información puede ser interceptada por algún otro usuario de la red Telemática?* 86
Tabla 22. *¿Se siente preparado para asumir algún tipo de riesgo frente a la perdida, alteración o robo de información?* 87
Tabla 23. *¿Ha recibido algún de capacitación por parte de la entidad referente a políticas de seguridad de la información?* 88
Tabla 24. *¿Considera necesario, que el intercambio de información entre los usuarios de la red telemática tendría estar normada por protocolos de seguridad?* 89
Tabla 25. *Identificación de usuarios* 122
Tabla 26. *Identificación de requerimientos* 123
Tabla 27. *Identificación de servicios* 124
Tabla 28. *Detalle de equipamiento para la infraestructura tecnológica* 126
Tabla 29. *Identificación de riesgos* 128
Tabla 30. *Identificación de protocolos de seguridad* 132
Tabla 31. *Actividades de seguimiento y control* 134
Tabla 32. *Grado de Conocimiento del Experto* 140
Tabla 33. *Grado de Influencia del Experto en relación a las Fuentes de Argumentación* 141
Tabla 34. *Resultados de la valoración de la competencia a expertos* 142
Tabla 35. *Identificación de usuarios de la Organización* 143
Tabla 36. *Identificación de requerimientos de la Organización* 144
Tabla 37. *Identificación de servicios de la Organización* 144

ÍNDICE DE FIGURAS

Figura 1. Ciclo PDCA 30
Figura 2. Formas de Cifrado (1) 31
Figura 3. Formas de Cifrado (2) 32
Figura 4. Red Privada Virtual 34
Figura 5. VPN de sitio a sitio 35
Figura 6. VPN de sitio a sitio 36
Figura 7. Protocolo PPTP 37
Figura 8. Protocolo L2TP 37
Figura 9. Funcionamiento de AH 39
Figura 10. Funcionamiento de ESP (1) 39
Figura 11. Funcionamiento de ESP (2) 40
Figura 12. Método Atbash 42
Figura 13. Escítala 43
Figura 14. Cifrado de Polibios. 44
Figura 15. Cifrado de César. 44
Figura 16. Cifrado de Vigenère. 46
Figura 17. Servicio Telegráfico 46
Figura 18. Servicio Telegráfico 47
Figura 19. Máquina Enigma 48
Figura 20. Red Conmutada 50
Figura 21. División de ARPANET 51
Figura 22. Navegador Mosaic 52
Figura 23. Framework IPsec 55
Figura 24. Red NSFNET 57
Figura 25. Evolución de las Normas ISO 58
Figura 26. Involucramiento de los jefes inmediatos 68
Figura 27. Responsabilidad de los especialistas en TIC 69
Figura 28. Importancia del diseño topológico de la red 70
Figura 29. Importancia de contar con componentes móviles 71
Figura 30. Importancia de contar con componentes corporativos 72
Figura 31. Necesidad de identificar y aceptar los riesgos 73
Figura 32. Mitigación de riesgos para mejorar la seguridad informática 74
Figura 33. Necesidad de establecer controles de acceso físico 75

Figura 34. Necesidad de establecer políticas de mantenimiento de equipos 76
Figura 35. Necesidad de establecer políticas de escritorio y pantallas limpias 77
Figura 36. Necesidad de establecer políticas de resguardo de información 78
Figura 37. Necesidad de establecer controles de seguridad de los datos 79
Figura 38. Responsabilidad de los empleados con la información 80
Figura 39. Necesidad de indicar los requerimientos de usuario 81
Figura 40. Consideraciones para los servicios de red 82
Figura 41. Consideraciones de acceso seguro a la red 83
Figura 42. Consideraciones de encriptación de la información 84
Figura 43. Percepción de seguridad al enviar la información por la red de la Universidad 85
Figura 44. Percepción de que la información pueda ser interceptada por otro usuario de la red.86
Figura 45. Sensación de asumir riesgos ante la pérdida, robo o alteración de información 87
Figura 46. Capacitación por parte de la entidad en políticas de seguridad de la información 88
Figura 47. Necesidad de normar el intercambio de información entre los usuarios de la red 89
Figura 48. Dimensión de gestión de conectividad de la red.....105
Figura 49. Dimensión de gestión de seguridad informática.....109
Figura 50. Modelo de seguridad informática en redes privadas virtuales 114
Figura 51. Diseño de la Metodología para redes privadas virtuales.....118
Figura 52. Topología física de la red 125
Figura 53. Topología lógica de la red.....125
Figura 54. Diagrama de topología física de la red 145
Figura 55. Diagrama de topología lógica de la red 145

DEDICATORIA

A mí querida Madre Adelaida, que desde cielo me sigue iluminando y guiando por el sendero de la vida. A mí Padre por su ejemplo como persona. En especial a mí esposa Jessica a mis hijos Fernanda, Mayte y Renzo con que son el motor y motivo que me impulsan a seguir en el camino de la superación personal y el logro de objetivos profesionales.

MSc. Gilberto Carrión Barco

AGRADECIMIENTO

A mí gran Dios Padre Celestial, a mis Docentes del Doctorado por sus consejos y sabias enseñanzas, un agradecimiento especial a mi asesor metodólogo Dr. Juan Carlos Callejas Torres por su paciencia y motivación para seguir adelante y para mi asesor especialista Dr. Christian Abraham Dios Castillo por compartir conmigo sus amplios conocimientos y ayudarme a culminar mi trabajo de investigación doctoral de la mejor manera. A todos ellos, Gracias totales.

MSc. Gilberto Carrión Barco

RESUMEN

La información al viajar por una red pública como Internet, está expuesta a que cualquier persona o intruso pueda acceder a ella, por lo que se debe garantizar la seguridad de la información durante el envío. Las redes privadas virtuales permiten que la información viaje segura por entornos de conexiones públicas, ante esta situación se desarrolla la presente investigación la cual tiene como objetivo elaborar una metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para la Universidad Nacional Pedro Ruiz Gallo que permita mejorar el intercambio de información académica contextualizada en un entorno de conexiones públicas, en donde el tipo de investigación es cuantitativa-explicativa y el diseño de contrastación de la hipótesis es cuasiexperimental, al diagnosticar el estado actual del proceso de seguridad informática y su dinámica en redes privadas virtuales en la entidad, conllevó a que se proponga un modelo de seguridad informática en redes privadas virtuales como aporte teórico y la elaboración de una metodología adaptativa para la implementación del modelo como parte del aporte práctico. La metodología propuesta se encuentra estructurada en tres etapas y siete fases, las mismas que fueron validadas por juicio de expertos. Así mismo, se concluye que tanto las diversas tareas de investigación como la aplicación parcial de la metodología la cual está relacionada con la variable dependiente (intercambio de información académica contextualizada) revela que los indicadores: tipos de usuarios, requerimientos y servicios de red y topología de red han pasado de un estado actual a un estado proyectado lo que demuestra un cambio favorablemente positivo en la variable notándose la diferencia en ambos estados.

Palabras clave: información, seguridad informática, Internet, redes privadas virtuales, metodología, intercambio de información contextualizada.

ABSTRACT

The information when traveling on a public network such as the Internet, is exposed to any person or intruder can access it, so you must ensure the security of information during the shipment. Virtual private networks allow information to travel safely through public connections environments, in view of this situation the present investigation is developed which aims to develop an adaptive methodology based on a computer security model in virtual private networks for the National University Pedro Ruiz Gallo that allows to improve the exchange of contextualized academic information in an environment of public connections, where the type of research is quantitative-explanatory and the test design of the hypothesis is quasi-experimental, when diagnosing the current state of the information security process and its dynamics in virtual private networks in the entity, led to propose a computer security model in virtual private networks as a theoretical contribution and the development of an adaptive methodology for the implementation of the model as part of the practical contribution. The proposed methodology is structured in three stages and seven phases, which were validated by expert judgment. Likewise, it is concluded that both the diverse tasks of investigation and the partial application of the methodology which is related to the dependent variable (exchange of contextualized academic information) reveals that the indicators: types of users, requirements and network services and topology network have moved from a current state to a projected state which shows a positive change in the variable, noting the difference in both states.

Keywords: information, computer security, Internet, virtual private networks, methodology, contextualized information exchange.

INTRODUCCIÓN

En los últimos tiempos las redes computacionales han pasado a ser parte fundamental para las organizaciones. Cada vez en mayor medida, las redes informáticas comparten información trascendental, es por ello que dichas redes tienen que cumplir ciertas características tales como seguridad, confiabilidad, escalabilidad, cobertura y tolerancia a fallos.

En la actualidad se ha comprobado que las redes computacionales reducen distancias, tiempo y costo para las organizaciones, eso ha contribuido a que organizaciones sobre todo las que cuentas con oficinas remotas a varios kilómetros de distancia puedan estar conectadas en tiempo real, más aún también es innegable que estas redes remotas han incitado la curiosidad de algunas personas mal intencionadas que se dedican a buscar vulnerabilidades en los servidores y las redes para obtener información confidencial. Debido a esto la seguridad de las redes computacionales es de suma importancia, es por eso que escuchamos hablar tanto de los populares cortafuegos y de las redes privadas virtuales.

Muchas organizaciones hoy en día intercambian información entre sus empleados, teletrabajadores, proveedores, sucursales u oficinas remotas, para que la información viaje de manera segura, se necesita de una red que sea capaz de garantizar la seguridad de la información y eliminar la constante amenaza de que nuestros datos sean robados o modificados, una solución de bajo costo es implementar una red privada virtual (VPN).

La forma en que una VPN proporciona seguridad depende de los protocolos que se utilizan para garantizar en envío confiable de información, estos protocolos pueden ayudar con el cifrado de los datos mientras que otros protocolos pueden

estar destinados a mejorar la autenticación. El beneficio que se requiera en una VPN depende en gran medida del tipo de información a enviar.

La Universidad Nacional Pedro Ruiz Gallo, cuenta con la Red Telemática órgano dependiente de la Oficina General de Sistemas Informáticos y está a la vez depende del Rectorado, encargada de diseñar, planificar, actualizar y supervisar los procesos informáticos académicos, administrativos y de investigación de la Universidad (UNPRG, 2017). Una de las funciones de la red telemática es *"Formular, dirigir, organizar y hacer cumplir la Política de Seguridad Informática de la Universidad"*.

La Universidad Nacional Pedro Ruiz Gallo ubicada en la Ciudad de Lambayeque, se interconecta remotamente con su Centro Pre Universitario ubicado en la Ciudad de Chiclayo, esta conexión se establece utilizando una Red Privada Virtual haciendo uso de la red pública de Internet, permitiendo el intercambio de información entre ambos sitios; sin embargo, después de haber realizado un análisis fáctico en la red telemática, permitió detectar las siguientes **manifestaciones**:

- Los datos transmitidos son alterados durante el envío.
- Perdida de información académica sensible.
- Información dispersa y almacenada en discos duros locales de cada estación de trabajo.
- La calidad de servicio se ve afectada al interactuar con aplicaciones críticas.
- Conexiones lentas y bloqueadas.
- Cuanto mayor es la cantidad de usuarios conectados a la red privada virtual, menor es el ancho de banda para los usuarios individuales.

- La información tarda mucho tiempo en enviarse.
- No todos los equipos actualmente instalados poseen facilidades para realizar conexiones a una red privada virtual.
- Contraseñas genéricas y débiles para el acceso a la información.

Lo que indica que existen ciertos indicios sobre la red privada virtual donde las conexiones y el intercambio de información académica contextualizada entre los diferentes sitios se ven afectadas.

Estas manifestaciones se sintetizan en el **problema científico**: insuficiencias en el acceso seguro entre los sitios de la universidad, limitan el intercambio de información académica contextualizada.

Lo que conlleva a plantear posibles **causas** del problema antes mencionado:

- Existe una gran variedad de marcos de trabajo para el aseguramiento de la información sin embargo no existe un proceso de seguridad informática orientado principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información de manera integral en entornos de conexiones públicas.
- Limitaciones teóricas en el proceso de seguridad informática para mejorar el desarrollo e implementación de redes privadas virtuales haciendo uso adecuado de los protocolos de seguridad encapsulados que permitan el intercambio de información de forma rápida y estable en entorno de conexiones públicas.
- Carencias de políticas, normas y estándares para la implementación del proceso de seguridad informática en redes privada virtuales.

- Deficientes referentes prácticos en el desarrollo de una metodología adaptativa en el proceso de seguridad informática para la implementación de redes privadas virtuales bajo un modelo que garantice el intercambio de información en un entorno de conexiones públicas.

Estas **valoraciones causales** sugieren profundizar en el proceso de la seguridad informática para redes computacionales en entornos públicos, **objeto** de la presente investigación.

En relación con el proceso de seguridad informática para redes computacionales, podemos citar a importantes autores que han aportado con este tema; (Areitio, 2008) nos dice: Actualmente, las organizaciones empresariales soportan su actividad de negocio en tecnologías de la información y de la comunicación, por lo que necesitan dotar a sus sistemas e infraestructuras informáticas en red de las políticas y medidas de protección que garanticen el desarrollo y sostenibilidad de su actividad de negocio. Mantener la confidencialidad, la integridad, la disponibilidad y la usabilidad autorizada de la información cobra especial importancia y plantea la necesidad de disponer de profesionales capaces de asegurar, gestionar y mantener la seguridad de la información en sus sistemas ante amenazas presentes y futuras.

La seguridad de la información es un proceso en el que se da cabida a un creciente número de elementos: aspectos tecnológicos, de gestión organizacionales, de recursos humanos, de índole económica, de negocios, de tipo legal, de cumplimiento, etc.; abarcando no sólo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medioambientales, humanos, etc.

Las empresas y organizaciones necesitan conectar sus centros de producción, oficinas y puntos de venta para intercambiar datos en tiempo real sobre la situación de los stocks, los pedidos realizados o los servicios solicitados por los clientes y los empleados por citar algunos de los casos más habituales (Gómez, 2014).

El tener que conectar diferentes sitios conlleva a requerir de enlaces dedicados de alta capacidad los cuales proporcionan un medio de comunicación altamente confiable; no obstante, estas líneas tienen un costo bástate elevado por lo que las pequeñas y medianas empresas no disponen de los recursos financieros para su implementación.

Frente a ello surge una alternativa mucho más económica, fácil de implementar y administrar, está tecnología es conocida como Red Privada Virtual (VPN), el cual es un sistema de telecomunicación que consiste en una red de datos restringida (privada) para un grupo de usuarios predeterminados, permitiendo una extensión segura de la red de área local (LAN) sobre una red de acceso público no controlada como Internet. Permitiendo además que la red de la organización (LAN) envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

Por lo tanto, una VPN puede contribuir de forma decisiva para mejorar el intercambio de información en la organización que la utiliza, facilitando así mismo la integración de los principales operadores y clientes a través de conexiones VPN, aportando múltiples ventajas para los usuarios: información en tiempo real sobre pedidos, integración de los sistemas informáticos, intercambio electrónico de documentos, entre otros.

Sin embargo, una VPN basada en redes públicas puede presentar problemas relacionados con la seguridad de las comunicaciones, el ancho de banda

disponible o la calidad de servicio. Dado que las redes públicas brindan soporte a las redes privadas virtuales y además que comparte el canal de comunicación con una gran cantidad de usuarios que podrían tener acceso a los datos si no se empleasen las medidas y protocolo de seguridad adecuados, es por ello de se debe establecer un modelo de seguridad basado en protocolos de encapsulamiento para redes privadas virtuales que permitan garantizar la confidencialidad, integridad y disponibilidad de los recursos informáticos de la organización.

Las organizaciones requieren redes seguras, confiables y rentables para interconectar varias redes, por ejemplo, para permitir que las sucursales y los proveedores se conecten a la red de la oficina central de una empresa. Además, con el aumento en la cantidad de trabajadores a distancia, hay una creciente necesidad de las empresas de contar con formas seguras, confiables y rentables para que los empleados que trabajan en oficinas pequeñas y oficinas domésticas (SOHO), y en otras ubicaciones remotas se conecten a los recursos en sitios empresariales (Cisco Networking Acadamy, 2014).

Las organizaciones utilizan las VPN para crear una conexión de red privada de extremo a extremo a través de redes externas como Internet o las extranet. El túnel elimina la barrera de distancia y permite que los usuarios remotos accedan a los recursos de red del sitio central. Una VPN es una red privada creada mediante tunneling a través de una red pública, generalmente Internet.

Las primeras VPN eran exclusivamente túneles IP que no incluían la autenticación o el cifrado de los datos. Por ejemplo, la encapsulación de routing genérico (GRE) es un protocolo de tunneling desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquetes de protocolo de capa de red dentro de los

túneles IP. Esto crea un enlace virtual punto a punto a los routers Cisco en puntos remotos a través de una internetwork IP (Cisco Networking Acadamy, 2014).

En la actualidad, las redes privadas virtuales generalmente se refieren a la implementación segura de VPN con cifrado, como las VPN con IPsec; sin embargo, no existe un modelo que indique la forma de diseñar una VPN de tal manera que garantice la confidencialidad, integridad y disponibilidad de la información de manera segura, haciendo uso de los protocolos de encapsulamiento.

Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos) son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información. Por tanto, actualmente se considera aceptado que la seguridad de los datos y la información comprende tres aspectos fundamentales (Costas, 2014).

- Confidencialidad, es decir, no desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales)
- Integridad, permite asegurar que los datos no se han falseado.
- Disponibilidad, esto es, que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.

Hay que tener en cuenta que tanto las amenazas como los mecanismos para contrarrestarlas, suelen afectar a estas características de forma conjunta. Así, por ejemplo, fallos del sistema que hacen que la información no sea accesible pueden llevar consigo una pérdida de integridad. Generalmente tienen que existir los tres aspectos descritos para que haya seguridad.

Así mismo también podemos citar algunas investigaciones que de alguna manera citan a los protocolos de seguridad para redes privadas virtuales, teniendo por ejemplo a (Lawas, Vivero, & Sharma, 2016), se centra en la evaluación y rendimiento de los protocolos VPN, principalmente el Secure Socket Tunneling Protocol (SSTP) e Internet Key Exchange versión 2 (IKEv2). Para comparar los protocolos se realizaron mediciones de rendimiento, fluctuación de fase y retardo durante envío de paquetes los cuales fueron enviados desde los clientes VPN a otro cliente VPN en un entorno de pruebas. Como resultado de la investigación, se logró determinar que IKEv2 tenía un resultado significativamente mejor con respecto al SSTP en relación con el rendimiento, la fluctuación de fase y el retardo.

En su artículo (Narayan, Ishrar, Kumar, Gupta, & Khan, 2016) proporciona una visión general del comportamiento de los mecanismos de transición, con y sin protocolos VPN. Las métricas de rendimiento relacionadas con las redes se han obtenido a partir de implementaciones de una red de pruebas. Los dos mecanismos de transición a evaluar son 4to6 y 6to4. Ambos mecanismos tienen ciertas ventajas y desventajas. Los protocolos VPN, PPTP e IPsec se configuraron en el mecanismo de transición y se compararon con métricas de redes seleccionadas. Las métricas de red clave que se capturaron en esta investigación fueron rendimiento, retraso, jitter, rendimiento de DNS, retraso de DNS, jitter de DNS, tanto para protocolos TCP como UDP. También se midió y discutió el rendimiento de VoIP. La red de pruebas constaba de dos enrutadores Cisco con capacidades para IPv4 e IPv6 y dos máquinas que ejecutaban Windows 7 y Windows Server 2012.

Por último (Zhiyong, Guixin, & Hongzhuo, 2014) diseñaron e implementaron un modelo de red VPN seguro y confiable sobre la base del estudio de la red VPN.

Este modelo utiliza un protocolo de autenticación con certificado digital y cifrado AES para transferir datos y tiene la función de ataque anti repliegue. Las pruebas realizadas muestran que el modelo soporta una variedad de protocolos de red, lo que es adecuado para las necesidades de desarrollo de la red. Este artículo presenta el diseño e implementación de una red VPN simple y segura, con lo que se logra un sistema de prototipos VPN. La forma de configurar la red VPN es simple y práctico, pues tiene una buena perspectiva de aplicación en la transmisión segura a distancia.

De lo analizado por varios autores se evidencia que no existen referentes teóricos y prácticos relacionados con un modelo de seguridad informática para redes privadas virtuales que permita el intercambio de información de manera confiable.

Por lo tanto, se plantea como **objetivo**: Elaborar una metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para la Universidad Nacional Pedro Ruiz Gallo que permita mejorar el intercambio de información académica contextualizada en un entorno de conexiones públicas.

Por lo que se determina como **campo de acción**: proceso de seguridad informática y su dinámica en redes privadas virtuales.

Es así que existe una **brecha epistémica** en donde el estudio del objeto y el campo de acción revelan, que no ha sido lo suficientemente aplicada la metodología para implementar una red privada virtual en un entorno de conexiones públicas, desde una lógica que integre los procesos de seguridad informática, los protocolos de encapsulamiento y las políticas de seguridad de la organización.

Hipótesis: Si se elabora una metodología adaptativa basada en un modelo de seguridad informática para redes privadas virtuales que tenga en cuenta la relación entre la lógica de integración del proceso de seguridad informática, la lógica

funcional de los protocolos de encapsulamiento y las políticas de seguridad de la organización, entonces se contribuye al mejoramiento del intercambio de información académica contextualizada en entornos de conexiones públicas de la Universidad Nacional Pedro Ruiz Gallo.

Para darle cumplimiento al objetivo y la hipótesis se planifica las siguientes **tareas de investigación**:

- Caracterizar epistemológicamente el proceso de seguridad informática en redes privadas virtuales.
- Determinar las tendencias históricas del proceso de seguridad informática en redes privadas virtuales.
- Diagnosticar el estado actual de la dinámica del proceso de seguridad informática de redes privadas virtuales en la Universidad Nacional Pedro Ruiz Gallo.
- Elaborar un modelo seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en la Universidad Nacional Pedro Ruiz Gallo.
- Elaborar una metodología adaptiva para la implementación del modelo de seguridad informática para redes privadas virtuales.
- Corroborar la factibilidad y valor científico de los resultados de la investigación mediante criterios de expertos.
- Ejemplificar parcialmente la aplicación de la metodología adaptativa del modelo de seguridad informática para redes privadas virtuales.

Como **métodos** y **técnicas** de investigación se utilizarán:

- Del nivel teórico (análisis-síntesis, inducción-deducción, histórico-lógico, sistémico-estructural-funcional) para la caracterización de los antecedentes teóricos e históricos del proceso de seguridad informática y del intercambio de información académica contextualizada y la construcción del aporte.
- Del nivel empírico, para la caracterización del estado actual del intercambio de información académica contextualizada de la Universidad Nacional Pedro Ruiz Gallo (encuestas, entrevistas, análisis documental, talleres de capacitación), la corroboración de la factibilidad y el valor científico-metodológico de los resultados de la investigación (criterios de expertos) y la ejemplificación de una metodología para el diseño e implementación de redes privadas virtuales para la Universidad Nacional Pedro Ruiz Gallo.

La **significación práctica,** radica en el impacto social al contribuir al mejoramiento del intercambio de información académica contextualizada en entornos de conexiones públicas en la región.

La **novedad científica,** radica en relevar la lógica de integración del proceso de seguridad informática haciendo uso de protocolos de seguridad encapsulados para redes privadas virtuales que tenga en cuenta la lógica funcional de las políticas de seguridad de la organización y la aplicabilidad de una metodología adaptativa.

PRIMERA PARTE

METODOLOGÍA Y FUNDAMENTACIÓN

DE LA INVESTIGACIÓN

CAPÍTULO 1. CONSTRUCCIÓN DEL MARCO TEÓRICO

Introducción

En este capítulo se abordan los referentes teóricos contextuales, a partir de la caracterización del proceso de seguridad informática y su dinámica en redes privadas virtuales, se consideran los fundamentos teóricos que ofrecen una panorámica de la problemática investigada y se describen las categorías esenciales del objeto y del campo de acción; finalmente se determinan las tendencias históricas del proceso de seguridad informática en redes privadas virtuales, con el objeto de proporcionar hitos a lo largo del tiempo a través de indicadores de análisis y etapas definidas.

1.1. Caracterización del proceso de seguridad informática y su dinámica en redes privadas virtuales

Dentro del proceso de seguridad informática y su dinámica en redes privadas virtuales, se puede afirmar que la información es uno de los activos más valiosos para cualquier empresa, después del activo humano. El hombre genera las órdenes y la información, pero ésta necesita fluir hacia las partes ejecutoras para que las compañías cobren vida y comiencen su actividad. El problema es que esa información, tanto en los seres vivos como en las empresas, corre el riesgo de ser dañada o su flujo puede ser obstruido, lo que da lugar a un mal funcionamiento del ser vivo o de la organización. Es por ello que la **seguridad informática** es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y la privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos físicos como lógicos, a los que está expuesta (Baca, 2016).

Para que la seguridad informática se aplique de manera correcta, se necesita de mismo un **Sistema de Gestión de Seguridad de la Información (SGSI),** según la norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información (Gómez & Álvarez, 2012).

La norma **UNE-ISO/IEC 27001**, está pensada para que se emplee en todo tipo de organizaciones (empresas privadas y públicas, entidades sin fines de lucro, etc.), sin importar el tamaño o la actividad. Esta norma explica como diseñar un SGSI y establecer los controles de seguridad, de acuerdo con las necesidades de una organización o de partes de la misma, pero no aclara mediante qué procedimientos se ponen en práctica.

Mientas tanto la norma **UNE-ISO/IEC 27002 Tecnologías de la Información. Código de buenas prácticas para la gestión de la seguridad de la información**, establece las directrices y principios generales para el comienzo, la implementación, el mantenimiento y la mejora de la gestión de la seguridad de la información en una organización. Los objetivos de control y los controles de esta norma internacional tienen como fin servir de guía para el desarrollo de pautas de seguridad internas y prácticas efectivas de gestión de la seguridad.

La implementación de un Sistema de Gestión de Seguridad de la Información supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar como información documentada (Gómez & Fernández, 2015)

Fundamentalmente se distinguen dos tipos de procesos:

- Procesos de gestión. Controlan el funcionamiento del propio sistema de gestión y su mejora continua.
- Procesos de seguridad. Se centran en los aspectos relativos a la propia seguridad de la información.

Para establecer y gestionar un SGSI se utiliza el ciclo PDCA (conocido también como ciclo Deming), tradicional en los sistemas de gestión de calidad. El modelo **PDCA** o "Planificar – Hacer – Verificar – Actuar" (Plan – Do – Check – Act, de sus siglas en ingles), tiene una serie de fases y acciones que permiten establecer un modelo de indicadores y métricas comparables en el tiempo, de manera que se pueda cuantificar el avance en la mejora de la organización:

- **Plan.** En esta fase se planifica la implantación del SGSI. Se determina el contexto de la organización, se definen los objetivos y las políticas que permitirán alcanzarlos. Se correspondería con los capítulos 4, 5, 6 y 7 de la Norma UNEISO/ IEC 27001:2014.
- **Do.** En esta fase se implementa y pone en funcionamiento el SGSI. Se ponen en práctica las políticas y los controles que, de acuerdo al análisis de riesgos, se han seleccionado para cumplirlas. Para ello debe de disponerse de procedimientos en los que se identifique claramente quién debe hacer qué tareas, asegurando la capacitación necesaria para ello. Se correspondería con el capítulo 8 de la Norma UNE-ISO/IEC 27001:2014.
- **Check.** En esta fase se realiza la monitorización y revisión del SGSI. Se controla que los procesos se ejecutan de la manera prevista y que además permiten alcanzar los objetivos de la manera más eficiente. Se correspondería con el capítulo 9 de la Norma UNE-ISO/IEC 27001:2014.

- **Act.** En esta fase se mantiene y mejora el SGSI, definiendo y ejecutando las acciones correctivas necesarias para rectificar los fallos detectados en la anterior fase. Se correspondería con el capítulo 10 de la Norma UNE-ISO/IEC 27001:2014.

A la hora de diseñar el SGSI, se debe tener en cuenta que sobre el mismo se aplicará un proceso de mejora continua, con lo que conviene partir de una primera versión del mismo adaptado a las necesidades, operativas y recursos de la organización, con unas medidas de seguridad mínimas que permitan proteger la información y cumplir con los requisitos de la norma. Así, el SGSI será mejor adoptado por las personas implicadas, evolucionando de manera gradual y con un menor esfuerzo.

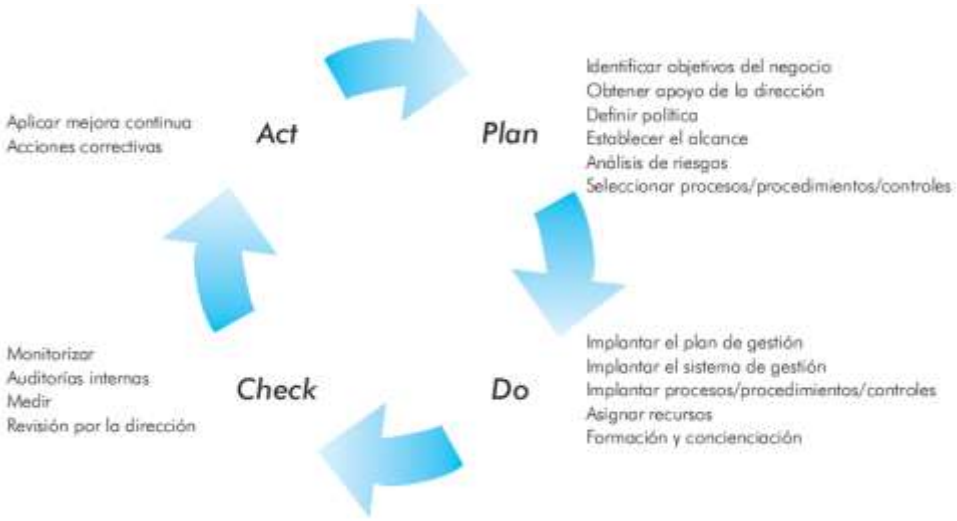


Figura 1. Ciclo PDCA

Así mismo, la **seguridad informática** se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información. Estos principios son muy comunes en el ámbito de la seguridad. Junto a estos tres principios fundamentales se suelen estudiar conjuntamente la autenticación y el no repudio en los sistemas de información (Costas J., 2014).

Confidencialidad, se trata de la cualidad que debe poseer un documento o archivo para que este solo se entienda de manera comprensible o sea leído por la persona o

sistema que ese autorizado. De esta manera se dice que un documento (archivo o mensaje) es confidencial si y sólo si puede ser comprendido por la persona o entidad a quien va dirigida o *autorizada*. En el caso de un mensaje esto evita que exista una interceptación de éste y que pueda ser leído por una persona no autorizada.

Por ejemplo, si Andrea quiere enviar un mensaje a Bruno y que sólo pueda leerlo Bruno, Andrea cifra el mensaje con una clave (simétrica o asimétrica), de tal modo que sólo Bruno sepa la manera de descifrarlo, así ambos usuarios están seguros que sólo ellos van a poder leer el mensaje.

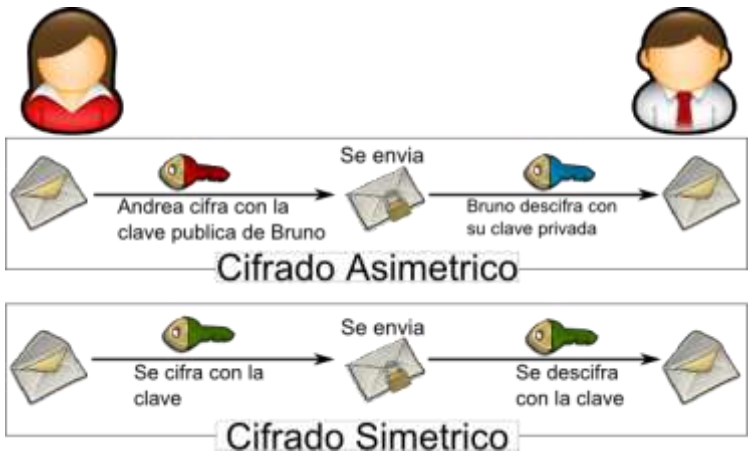


Figura 2. Formas de Cifrado (1)

Integridad, es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original. Aplicando a las bases de datos sería la correspondencia entre los datos y los hechos que refleja.

Por ejemplo, si Andrea envía un mensaje a Bruno, tendría que viajar el propio mensaje como un resumen cifrado del mismo. Finalmente, Bruno en el lado del receptor, compara el mensaje como resumen (aplicando la misma función que Andrea) y el resumen cifrado enviado. Si en el transcurso de la comunicación el

mensaje ha sido alterado por fallos en el canal de comunicaciones o por algún usuario intruso, la comparación será errónea, y si ésta da como resultado "iguales", quiere decir que no ha existido manipulación del mensaje.

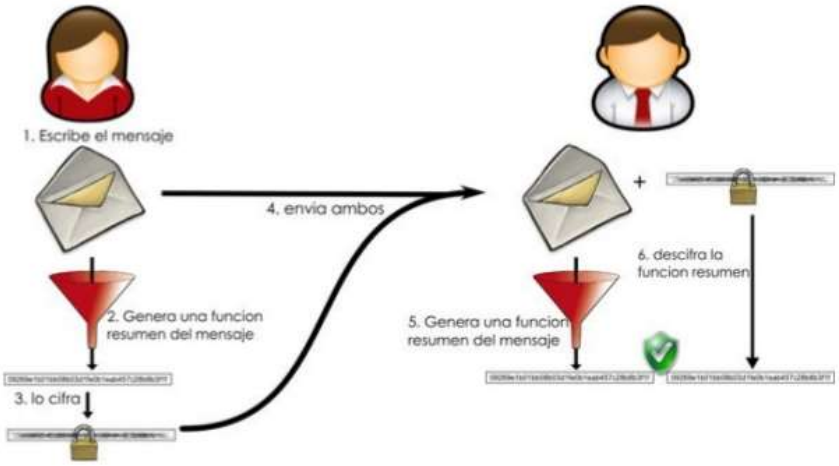


Figura 3. Formas de Cifrado (2)

Disponibilidad, se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando éstos lo requieran. También se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

Las herramientas de disponibilidad deben permitirnos disponer de nuestros equipos funcionando 24 horas al día, 7 días a la semana, ofreciéndonos la seguridad de que, bajo cualquier supuesto, nuestro sistema de producción estará disponible inmediatamente. En el actual entorno de negocios, la alta disponibilidad de nuestros sistemas se ha convertido en una necesidad y no en un lujo.

Autenticación, es la situación en la cual se puede verificar que un documento ha sido elaborado o pertenece a quien el documento dice.

Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado.

No repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce fuera a un tercero.

Para brindar una comunicación segura entre dos sucursales de la empresa u organización, se pueden emplear diversas soluciones. Una opción consiste en emplear líneas de comunicación que sean de propiedad de la empresa, esperando que ningún agente ajeno acceda a ellas en ningún punto del recorrido. Esto tiene un coste muy elevado, y normalmente solo será viable para empresas muy grandes, o para distancias muy pequeñas.

Una solución más económica consiste en alquilar las líneas de comunicaciones a sus propietarios (operadores de telecomunicaciones), de manera que las comunicaciones se sigan cursando por una línea dedicada, confiando en que ninguna otra empresa ni persona tenga acceso. En ambos casos (propiedad o alquiler) se está usando una **red privada**, con la ventaja adicional de que el medio no se comparte con ningún otro usuario, de forma que todo el ancho de banda esté disponible, y las comunicaciones puedan ser muy rápidas (Giménez A., 2014).

Con la popularización de los accesos de banda ancha a internet, se plantea resolver esta necesidad de comunicar de manera segura y rápida dos extremos, pero a un coste mucho menor. Para ello, se emplean técnicas que construyen una **red privada**

virtual, que como su nombre lo indica, es una construcción ficticia, en la que el emisor y receptor disponen de una conexión extremo a extremo, dedicada y segura. Visualmente es como si se tratará de un túnel que atraviesa internet, por el que las comunicaciones viajan protegidas del resto de usuarios.

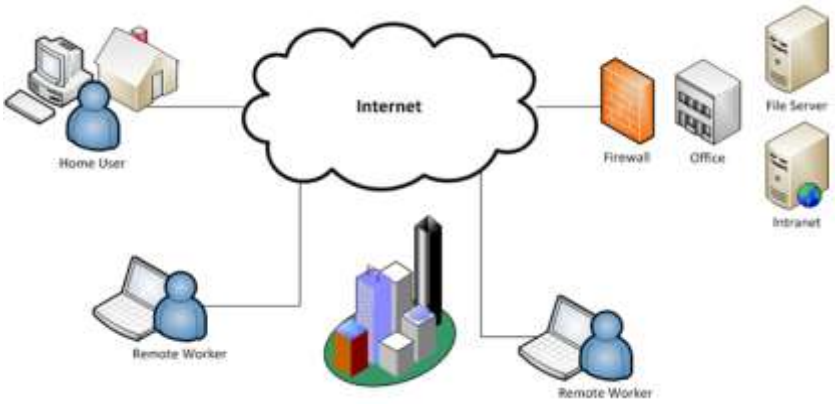


Figura 4. Red Privada Virtual

Habitualmente, estas redes privadas virtuales se construyen para operar de forma transparente, desde el firewall de un extremo al firewall del otro extremo. Lo expuesto para el transporte por redes WAN también puede emplearse para el transporte de información por la red interna, o para el transporte entre determinadas subredes, e incluso para las comunicaciones entre una pareja concreta de equipos emisor – receptor.

Se deben añadir medidas de seguridad que protejan la información transmitida cuando un atacante tanga acceso a ella, como es el caso del transporte por redes públicas no seguras, como internet.

Las redes privadas virtuales (VPN) surgen para proporcionar una conexión segura a través de redes públicas no seguras, aunando el uso de criptografía, mecanismo de autenticación y encapsulación de protocolos. El resultado final es que se logra extender la red privada sobre una red pública sin problemas de seguridad, de manera que un usuario que emplee VPN para conectarse a la red privada de su empresa

logra operar todos los efectos, como si su estación de trabajo estuviera en la red privada de la empresa (Giménez Albacete, 2014).

Existen muchos criterios para clasificar las VPN; uno de los más sencillos es clasificarlas en dos tipos, según el uso que se realiza de la conexión segura.

Una **VPN de sitio a sitio**, permite conectar diferentes oficinas en una misma empresa, que precisen intercambiar datos confidenciales, evitando el alquiler de circuitos dedicados, considerablemente más costosos (pero con otras ventajas)

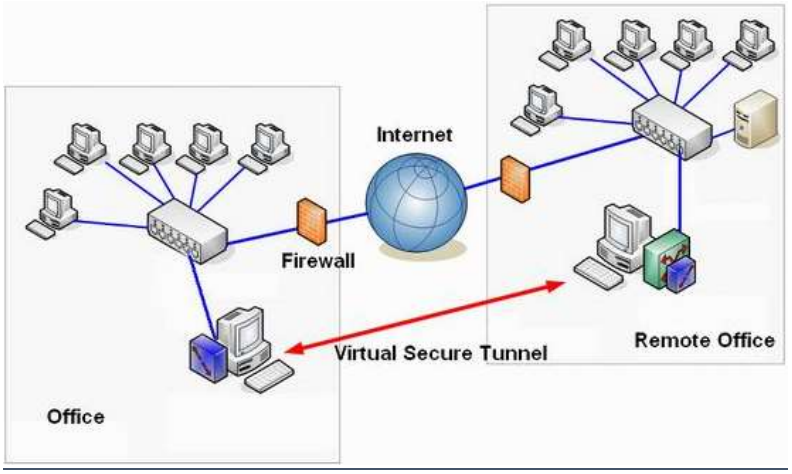


Figura 5. VPN de sitio a sitio

Mientras que **VPN de acceso remoto**, se utiliza para permitir el teletrabajo sin comprometer la seguridad. Es posible tener acceso computador a una red, o bien acceso de computador a computador. En ambos casos, existe un cliente y un servidor, y la VPN puede ser iniciada por el cliente (estación remota externa a la LAN), o por el servidor de la red privada.

La principal desventaja del empleo de VPN es la perdida de rendimiento, derivada del coste de cifrado criptográfico, y derivada del coste de la encapsulación que se emplea (un protocolo se envía como si fueran datos de otro protocolo); además, como todas las contramedidas, se introducen nuevas vulnerabilidades. Por ejemplo, una VPN de acceso remoto, para un teletrabajador que accede desde su domicilio,

se traslada a una ubicación sin medidas de control ni seguridad física un equipo que tendrá acceso lógico a la red privada de la empresa.

Para construir una red privada virtual, ambos extremos deben emplear el mismo protocolo (protocolos de red privada virtual o protocolo VPN). Existen varios protocolos VPN aceptados y estandarizados que se introducen a continuación, además de soluciones comerciales que facilitan la configuración y puesta en marcha de esta tecnología.

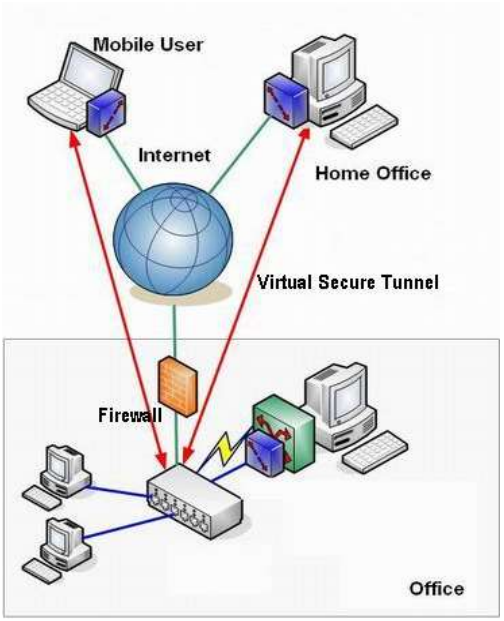


Figura 6. VPN de sitio a sitio

Los primeros protocolos de tunneling fueron Point to Point Tunneling Protocolo (PPTP – Protocolo para Túneles en Conexiones Punto a Punto), desarrollado por Microsoft y Layer 2 Forwarding (L2F – Reenvío a Nivel de capa 2 de modelo de referencia OSI), de Cisco (Gómez, 2014).

El protocolo **PPTP** encapsula paquetes PPP (*Point to Point Protocol*, el protocolo más utilizado para el acceso remoto a Internet a través de conexiones punto a punto) en "datagramas" del protocolo IP (protocolo a nivel de red). PPTP ha tenido una importante difusión gracias a su incorporación en los sistemas operativos de

Microsoft. Entre sus características más destacadas se encuentran la de implementar un control de flujo que permite evitar saturaciones de tráfico tanto en clientes como en servidores, mejorando el rendimiento al minimizar el número de paquetes descartados y, por lo tanto, las retrasmisiones.

Figura 7. Protocolo PPTP

Por su parte el protocolo **L2F** utiliza protocolos de capa 2 como Frame Relay o ATM para la creación de túneles, por lo que se considera una solución más extensible que PPTP, que trabaja exclusivamente sobre el protocolo IP, en la capa 3 de la arquitectura de redes. Además, a diferencia de PPTP, el protocolo L2F ofrece autenticación de los extremos y soporta varias comunicaciones independientes a través de un único túnel.

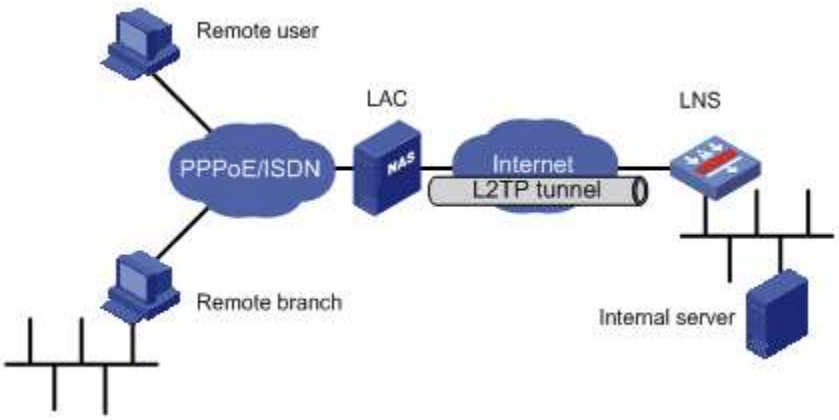


Figura 8. Protocolo L2TP

Gracias a un acuerdo alcanzado por todas las compañías, ambos protocolos han convergido en un nuevo denominado *Layer 2 Tunneling Protocol* (LT2P – Protocolo para Túneles a Nivel de Capa2), que permite aprovechar las mejores características de PPTP y de L2F. De este modo L2TP ofrece múltiples túneles

simultáneos en un solo cliente, lo que será de gran importancia en el futuro, cuando los túneles soporten reserva de ancho de banda y calidad de servicio (QoS).

Para mejorar la seguridad del protocolo IP y facilitar la construcción de redes privadas virtuales sobre Internet, el *Internet Engineering Task Force* (IETF), entidad independiente y de reconocido prestigio, responsable de la mayoría de los protocolos de Internet, ha desarrollado una nueva versión de IP (dentro del proyecto IPv6), denominado **IPSec** (Internet Protocol Security, RFC 2401), planteado como un lenguaje universal independiente de los protocolos propuestos por distintos fabricantes.

IPSec es una ampliación del protocolo IP que puede funcionar de modo transparente en las redes existentes, y que además permite establecer conexiones seguras en redes privada virtuales, mediante la creación de túneles seguros y garantizando la autenticación de los equipos. IPSec se considera como una opción en IP4, pero su utilización será obligatoria en la nueva versión IPv6.

El protocolo IPSec proporciona confidencialidad, autenticidad del remitente, la integridad de los datos y opcionalmente, protección contra reenvío no autorizados de datos. Para ello consta de tres protocolos:

- *Authentication Header* (AH. RFC 2402): proporciona la autenticación del remitente, la integridad de los datos y opcionalmente, protección contra el reenvió.
- *Encapsulating Security Payload* (ESP, RFC 2406): se encarga del cifrado de los datos para garantizar la confidencialidad. También puede proporcionar las funciones de autenticación del remitente, de integridad de los datos remitidos y de protección contra el reenvío, cuando ESP se utiliza conjuntamente con AH.

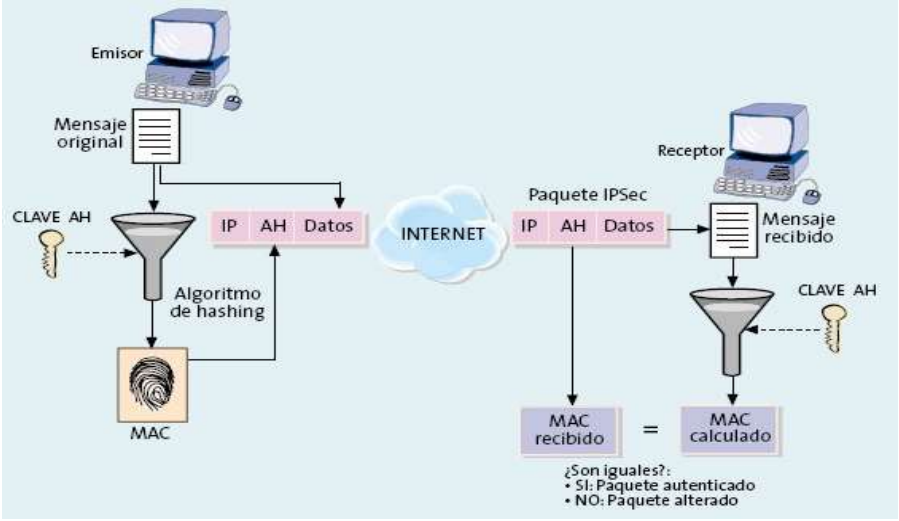


Figura 9. Funcionamiento de AH

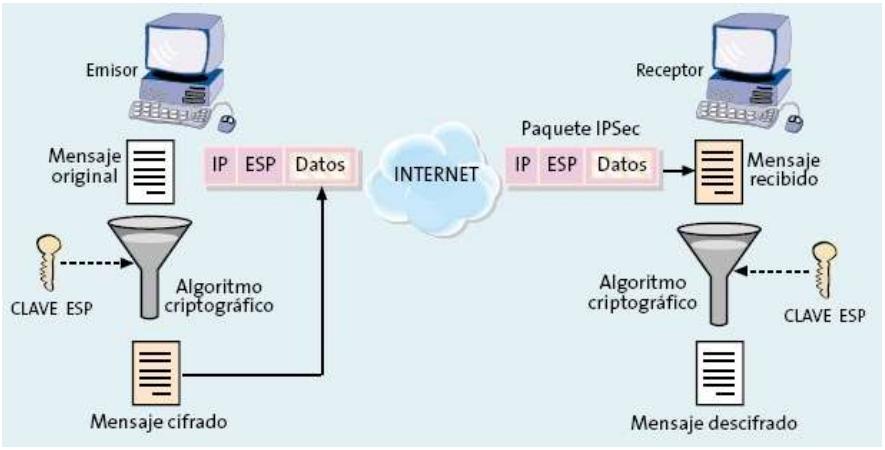


Figura 10. Funcionamiento de ESP (1)

- *Security Association* (SA -Asociación de Seguridad-): permite el conjunto de políticas y claves para establecer y proteger una conexión, es decir, qué protocolos y algoritmos criptográficos se emplean, cuáles son las claves de sesión establecidas y cuál es el periodo de validez de la conexión. Una asociación de seguridad queda determinada mediante un valor conocido como *Security Parameter Index* (SPI), una dirección IP de destino y un identificador de protocolo.

Estos protocolos emplean métodos criptográficos como DES (*Data Encryption Standard*) o Triple-DES para el cifrado y mecanismo de forma electrónica para la autenticación mediante funciones resumen (como MD5 o SHA-1).

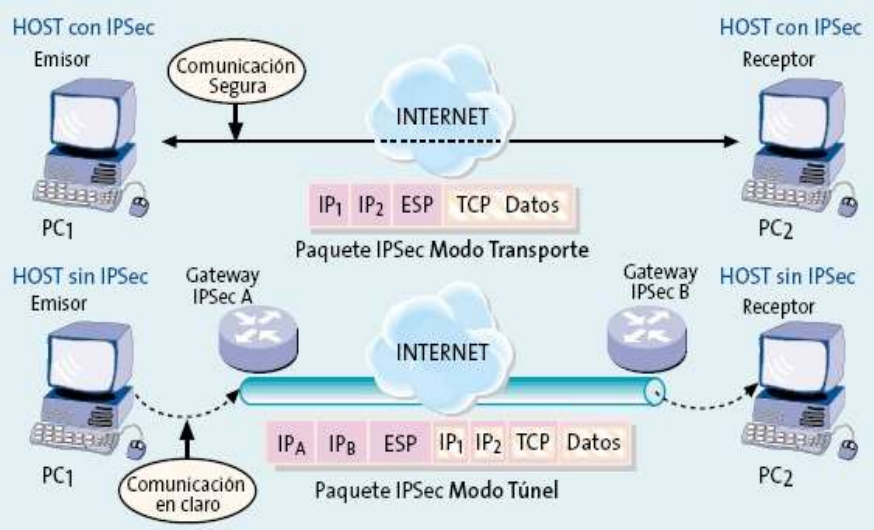


Figura 11. Funcionamiento de ESP (2)

En el protocolo IPSec se han previsto dos modos de funcionamiento (Penflip, 2014):

- **Modo transporte:** en este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.
- **Modo túnel:** en éste el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través

de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

1.2. Determinación de tendencias históricas del proceso de seguridad informática y su dinámica en redes privadas virtuales

Debido al creciente uso de internet, cada vez más empresas, compañías e instituciones permiten a sus socios, proveedores, usuarios remotos, entre otros acceder a sus sistemas de información, pero para ello se debe asegurar que este acceso se establezca de manera correcta y se utilice de acuerdo a las políticas de seguridad implementadas por la empresa.

Es por ello que a lo largo de la historia se tratado en todo momento de proteger la información. Para poder determinar las tendencias históricas del proceso de seguridad informática en redes privadas virtuales, se tiene los siguientes indicadores de análisis: confidencialidad, integridad, autenticación, protocolos de encapsulación y políticas de seguridad de la información.

ETAPA 1: La seguridad informática en la edad antigua (1900 A.C. – Siglo V D.C.)

Desde la antigüedad hasta nuestros días, números protocolos y mecanismos criptográficos han ido desarrollándose. La primera forma de seguridad de la información tiene que ver con la criptografía**. La criptografía** es una de las es una parte de la disciplina encargada del estudio de la seguridad secreta o criptografía.

El primer texto relacionado con la Criptografía del que se tiene conocimiento data aproximadamente del año 1900 a.C. Es del antiguo Egipto; es un grabado en una piedra de la cámara principal de la tumba de un noble de la ciudad de Menet Khufu, a las orillas del Nilo. En él se cuentan los actos más relevantes de la vida de ese noble (López, García, & Ortega, 2005).

Los escribas de la antigua Mesopotamia también cambiaron en ocasiones los signos cuneiformes de su escritura por otros, coincidiendo así con sus colegas egipcios en esta forma de alterar la escritura. Pero a diferencia de los egipcios, los escribas mesopotámicos sí tuvieron intención de ocultar el significado de la escritura.

Saltando ya al siglo VI a.C., en algunos antiguos textos hebreos, entre los que están los bíblicos, figuran nombres de personas y ciudades que han sido transformados mediante ciertas sustituciones de unas letras por otras. La más frecuente es la denominada "atbash". En el "atbash" la primera letra del alfabeto hebreo se cambia por la última y viceversa, la segunda por la antepenúltima y así sucesivamente, según el esquema que se muestra en la Figura. Otra sustitución similar es el "albam".

Atbash Cipher																				
A	B	G	D	H	V	Z	Ch	T	Y	K	L	M	N	S	O	P	Tz	Q	R	Sh	Th
Th	Sh	R	Q	Tz	P	O	S	N	M	L	K	Y	T	Ch	Z	V	H	D	G	B	A

Figura 12. Método Atbash

Una curiosa forma de enviar secretamente mensajes se produjo en la antigua China. Generalmente, la diplomacia china y su ejército transmitían la información de forma oral, memorizando los mensajes. Pero en ocasiones se escribía el texto de forma minuciosa en fina seda que después se enrollaba y se sellaba con cera. El mensajero lo ocultaba en su propio cuerpo, tragándoselo. Este modo de enviar secretamente información ocultando el propio mensaje recibe el nombre de esteganografía.

Otro ejemplo histórico de esteganografía es la manera en que los griegos del siglo V a. C. se enteraron a tiempo del plan de invasión de Persia. Cuenta el historiador Heródoto en su obra "Las Historias" que Demarato, un exiliado griego en Persia,

grabó los planes persas en un par de tablillas de madera y después las cubrió con cera, ocultando así el mensaje. Las tablillas partieron desde la ciudad persa de Susa hasta Esparta sin ser interceptadas por el camino. Ya en su destino, Gorgo, esposa del rey Leónidas, adivinó que debajo de la cera debería esconderse algo escrito. Después que el mensaje fue leído, Esparta comunicó las intenciones persas al resto de las ciudades griegas. Gracias a ello, los griegos pudieron armarse a tiempo y derrotar a los persas en las batallas de las Termópilas, Salamina y Platea.

Fueron precisamente los espartanos de ese mismo siglo V a.C. quienes diseñaron el primer criptosistema para uso militar: fue la **escítala,** que como muchos otros sistemas que posteriormente se desarrollarían, el objetivo de este sistema era **cifrar** la información, es decir, hacer incomprensible el contenido del mensaje a terceros no autorizados.

Figura 13. Escítala

Esencialmente, se trata de un bastón de madera con un diámetro concreto. Para cifrar un texto, bastaba con enrollar una tira a lo largo del bastón y escribir en ella el mensaje. Posteriormente, se desenrollaba la tira para transportarla a su destinatario. El mensaje resultaba inteligible para cualquiera que no tuviese un bastón del mismo diámetro. La técnica subyacente a la escítala es la **transposición**, que consiste en cambiar el orden en que los caracteres aparecen en el texto (González & Fuentes, 2014).

En la Grecia clásica, el escritor Polibios describe en el siglo II a. C. un curioso sistema de señales que puede ser adoptado también como método criptográfico. Polibios dispone las letras en un cuadrado, como el que sigue a continuación:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I, J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Figura 14. Cifrado de Polibios.

En este método criptográfico cada letra puede ser representada por dos números. Por ejemplo: A con 11, R con 42. Polibios sugería transmitir estos números por medio de señales luminosas procedentes de antorchas y así poder enviar mensajes desde largas distancias

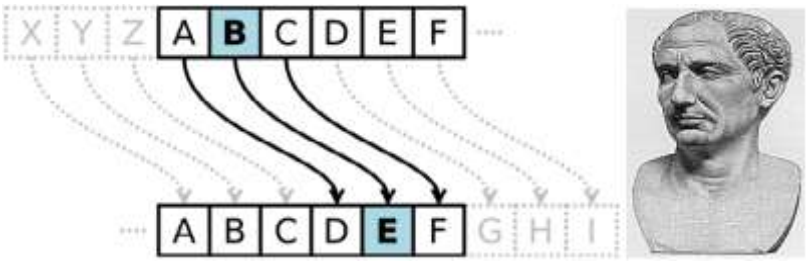


Figura 15. Cifrado de César.

Siglos más tarde surge uno de los métodos de cifrado clásico más conocidos: el **cifrado de César.** En este sistema, cada una de la de las letras del mensaje era sustituida por la situada tres posiciones más adelante en el alfabeto. Así, la letra 'C' del mensaje original era sustituida por la 'F'. Con el surge una completa familia de sistemas de cifrado denominados sistemas por sustitución monoalfabética. La característica de estos sistemas es que cada letra del mensaje original se sustituye por una misma letra.

Con este esquema, la famosa frase de Cesar ‘veni, vidi, vinci’ se cifraría ‘YHPL, YLGL, YLPFL’.

En esta primera etapa se puede observar que el único indicador de análisis en el proceso de seguridad informática es la confidencialidad a través de los métodos del cifrado de datos.

ETAPA 2: La seguridad informática en la edad media y el post renacimiento (Siglo V – Siglo XIX)

En el siglo XV después de Cristo se desarrollaron otros sistemas de cifrado: los cifrados por sustitución polialfabéticos. En ellos, cada letra no siempre se sustituye por otra fija, sino que la sustitución depende de la posición de la original en el texto. Uno de los más conocidos es el **cifrado de Vigenère**, en el que se utiliza una palabra como clave. Cada letra del mensaje se suma a la que aparece en la posición correspondiente de la clave. Por ejemplo, las letras ‘a’ (posición 1 del alfabeto) y ‘c’ (posición ‘3’ del alfabeto) se sumarían resultando en la ‘d’ (posición 4). Si la clave es más corta que el mensaje a transmitir, la propuesta clásica de Vigenère específica que la clave debe repetirse tantas veces como sea necesario.

Pero los métodos clásicos mono y polialfabéticos distan mucho de ser completamente seguros. En algunos casos, basta hacer un simple cálculo estadístico para desentrañar los mensajes ocultos. Si se confronta la frecuencia habitual de las letras en el lenguaje común con la de los signos del criptograma, puede resultar relativamente sencillo descifrarlo. Factores como la longitud del texto, el uso o no de más de una clave o la extensión de esta juegan un papel muy importante, así como la intuición, un arma esencial para todo criptoanalista (rompedor de cifrados). En el siglo XIX Friederich Kasiski, un militar prusiano, publicó un ataque basado en métodos estadísticos que rompía los cifrados por sustitución polialfabética.

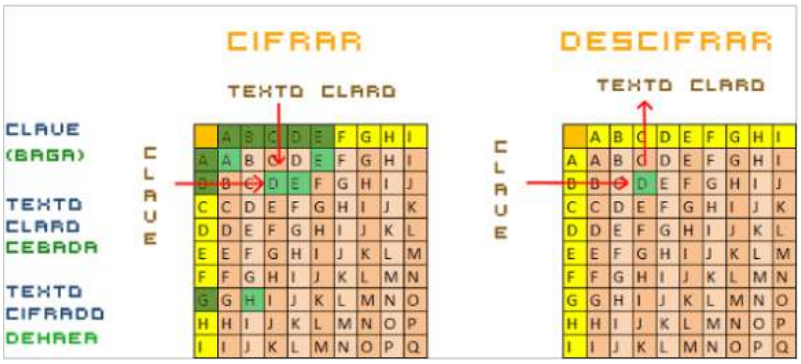


Figura 16. Cifrado de Vigenère.

En 1834 Charles Babbage, profesor de matemáticas de la Universidad de Cambridge, Inglaterra, desarrolla el concepto de un artefacto, que él denomina **"máquina analítica".**

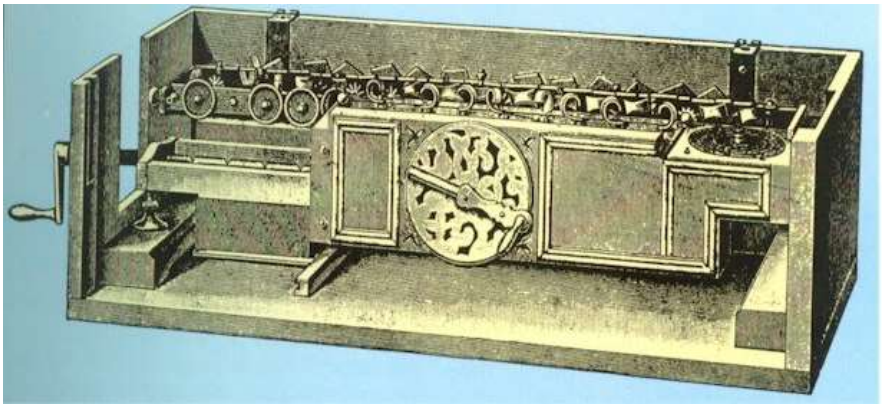


Figura 17. Servicio Telegráfico

La máquina estaba concebida para realizar cálculos, almacenar y seleccionar información, resolver problemas y entregar resultados impresos. Babbage imaginó su máquina compuesta de varias otras, todas trabajando armónicamente en conjunto: los receptores recogiendo información; un equipo transfiriéndola; un elemento almacenador de datos y operaciones; y finalmente una impresora entregando resultados. Pese a su increíble concepción, la máquina de Babbage, que se parecía mucho a una computadora, no llegó jamás a construirse. Los planes de Babbage fueron demasiado ambiciosos para su época. Demasiado y demasiado

pronto. Este avanzado concepto, con respecto a la simple calculadora, le valió a Babbage ser considerado como el precursor de la computadora.

El **servicio telegráfico** es posiblemente el primer y más antiguo servicio telemático del mundo. Fue Morse el que desarrolló el primer sistema de transmisión empleando señales eléctricas. En el sistema radioelectrónico, la información transmitida eran mensajes de texto codificados en el sistema Morse. En los primeros momentos, la telegrafía fue un medio de comunicación por el cual una persona que tenía un mensaje que enviar, entregaba dicho mensaje en forma escrita en la oficina de telégrafos más cercana y desde aquí, el mensaje se transmitía a la siguiente oficina. El proceso hasta alcanzar la oficina destino. El mensaje era enviado de la oficina al destinatario mediante un mensajero (Santos Gonzáles, 2014).

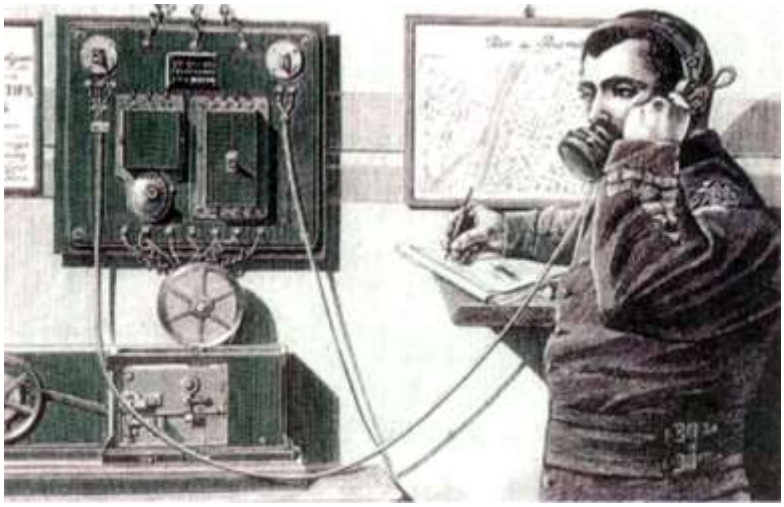


Figura 18. Servicio Telegráfico

La evolución del servicio telegráfico es la evolución de la propia telemática. Primero con la llegada de los teleimpresores, dispositivos capaces de interpretar las señales eléctricas e imprimir el mensaje sin necesidad de un operador.

El **servicio Télex** es un servicio público para la comunicación de datos (texto) entre abonados en la cual la información transmitida se imprime en dispositivos

conocidos como teleimpresores o terminales télex. El servicio Télex normalmente está asociado a las comunicaciones telegráficas entre abonados.

En esta segunda etapa se puede observar que la confidencialidad de la información se sigue desarrollado y mejorando, así mismo se puede distinguir que la integridad empieza a tomar protagonismo como indicador de análisis en el proceso de seguridad informática.

ETAPA 3: La seguridad informática en el Siglo XX (1900 – 1980)

Los siglos posteriores darían lugar a la creación de sofisticados sistemas de cifrado. Por su relevancia histórica, es necesario detenerse en el cifrado de la máquina **Enigma**, cuya invención data del año 1918. Esta máquina fue empleada por el ejército alemán en la Segunda Guerra Mundial. Se trata de una máquina compuesta por varios rotores (o ruedas dentadas), cada uno de los cuales dispone de 26 dientes.

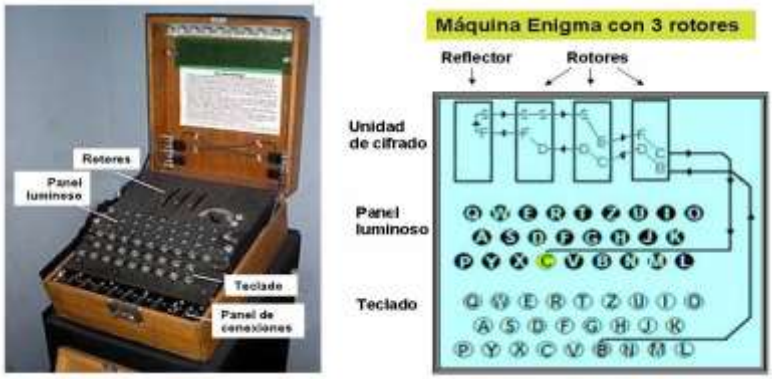


Figura 19. Máquina Enigma

Cada diente representa la correspondencia entre el carácter de entrada y el de salida. Por cada letra del mensaje original que se cifrase, se gira el rotor una posición. Cada vez que un rotor completaba una vuelta, el de su izquierda se movía una posición. Este sistema es mucho más complejo que los anteriores, ya que las combinaciones posibles son mucho más.

En 1976 los investigadores Whitfield Diffie y Martin Hellman propusieron un sistema para establecer una clave compartida a través de un canal inseguro. Poco tiempo más tarde surgiría una aproximación completamente distinta a lo anterior: la **criptografía de clave pública**. En 1978, Ron Rivest, Adi Shamir y Leonard Adelman publicaron en sistema **RSA**. Dicho sistema, como cualquier otro de clave pública, asume que cada comunicante dispone de un par de claves. En dicho par, una es conocida por todos (pública) mientras que la contraria es privada y solo conocida por el poseedor.

Día a día se vienen desarrollando mecanismos basados en criptografía de curvas elípticas, cuya ventaja principal es su extrema rapidez. En lo referente al futuro próximo, la criptografía cuántica plantea un escenario totalmente revolucionario en el que los mensajes intercambiados se corresponderían con fotones (elementos constituyentes de la luz), los cuales no pueden ser observados sin ser eliminados o modificados.

No hay consenso claro de en qué momento nace Internet. Algunos autores sitúan este momento en el nacimiento de **ARPANET** en 1969. Es así como ARPANET que nació como un proyecto militar, se puede considerar el embrión de Internet por ser el primer intento de unir los computadores situados en distintos lugares, pero no se puede considerar Internet todavía. Sería más correcto señalar como el nacimiento de Internet a la puesta en servicio de la NSFNET, una red que ya utiliza los protocolos TCP/IP y cuya misión es la de ser troncal para la conexión de redes. Este hecho se produce en 1986 aun cuando ARPANET sigue en servicio.

La red **NSFNET** la crea Estados Unidos una fundación llamada NSF (National Science Foundatioin, Fundación Nacional de Ciencia), que es algo así como una agencia de investigación científica financiada por el propio gobierno de los Estados

Unidos. Por tanto, NFS se puede considerar el organismo responsable de los primeros pasos de **Internet**.

En setiembre de 1969, se establece la primera conexión de computadoras a través de ARPANET. Los nodos eran minicomputadoras Honeywell DDP-516 con 12K en memoria con líneas telefónicas de 50 kbps. Posteriormente en febrero de 1970, la universidad de Hawaii desarrolla la primera **red conmutada** (Jcor, 2013).

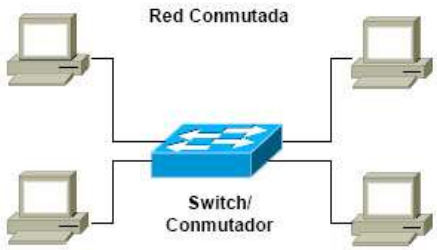


Figura 20. Red Conmutada

Un grupo de investigadores bajo la dirección de Norman Abramson, en la Universidad de Hawaii, en 1971 crearon el primer sistema de conmutación de paquetes mediante una red de comunicación por radio, dicha red se llamó ALOHA. Tres años después Vinton Cerf and Bob Kahn publican "A Protocol for Packet Network Intercommunication" el cual especifica la arquitectura de un programa de control de transmisión (Transmission Control Program, **TCP**), luego en 1978 TCP se divide en **TCP/IP.**

En esta tercera etapa caracterizada por la segunda guerra mundial y la guerra fría se puede distinguir que la confidencialidad, la integridad y los primeros protocolos de seguridad empiezan a formar los cimientos de la seguridad de la información dentro el proceso de seguridad informática.

ETAPA 4: La seguridad informática en la era de la información (1980 – Actualidad)

En 1980, se da la primera definición de **Seguridad de la Información**, en este año, James P. Anderson escribe un documento titulado 'Computer Security Threat Monitoring and Surveillance'. Lo más interesante de este documento es que James Anderson da una definición de los principales agentes de las amenazas informáticas. En mayo de 1983 ARPANET se divide en ARPANET y MILNET. The military network, MILNET. 68 nodos de los 113 fueron mudados a MILNET.

Figura 21. División de ARPANET

En 1990 se desmantela definitivamente ARPANET quedando NSFNET como el único troncal de la Red. Sin embargo, el gran desarrollo de Internet comienza cuando algunas empresas empiezan a implementar sus propias redes y a ofrecer servicios de conexión de Internet a través de ellas.

En paralelo a estos acontecimientos, se produce otro hecho fundamental en la evolución de Internet. En 1989, Tim Berners-Lee, un licenciado en física que trabajaba en el **Laboratorio Europeo de Física de Partículas** (CERN), propuso un proyecto para creación de un sistema de gestión de la información. Tres años más tarde, en 1992, empezaban a funcionar los primeros servicios para compartir información a través de la Red, era el nacimiento de **Word Wide Web** (www) o

simplemente Web. El impulso definitivo del servicio web se produjo cuando apareció el primer navegador con capacidades gráficas llamado Mosaic en 1993.

Mientras tanto, la NFS decide ceder el control del backbone de Internet a las empresas proveedoras de los servicios de conexión. Esta decisión implica que el control de Internet dejaba de estar en manos de un país para ser una rede descentralizada. Esta característica ha sido fundamental en el desarrollo posterior de la Red.

Como veíamos, a pesar de que Internet ofrecía casi desde sus inicios diferentes servicios basados todos en la arquitectura TCP/IP, como correo electrónico, transferencia de archivos, búsqueda de información, etc., fue el servicio Web el que hizo explotar definitivamente el potencial de la Red a nivel comercial. El primer navegador que se ejecutó en un entorno gráfico fue **Mosaic**, desarrollado por Marc Andersen, el cual tuvo una gran debido sobre todo a que era gratuito.

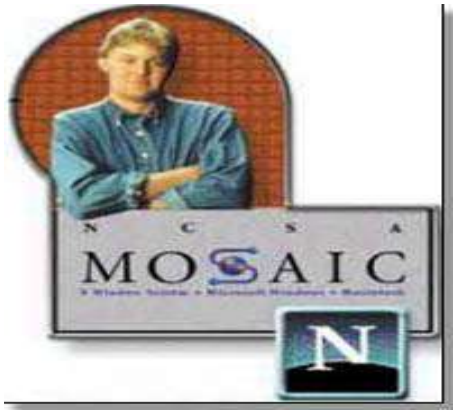


Figura 22. Navegador Mosaic

Unos años más tarde, Microsoft desarrolla su propio navegador Web llamado Internet Explorer, también gratuito y Mosaic se convierte en Netscape, estableciéndose una competencia entre ellos. Actualmente el servicio Web es, con diferencia, el servicio más utilizado en Internet debido sobre todo a los grandes avances técnicos conseguidos en la tecnología de navegación que permite a su vez

la visualización o ejecución de numerosos formatos multimedia y es capaz de proporcionar a los documentos web un alto grado de dinamismo.

Para que haya una Red Privada Virtual **(VPN)** y seguridad en Internet, primero tiene que haber Internet, así que, empecemos por ahí. Había computadores y redes de computadoras antes de internet, pero fue el trabajo realizado en nombre del Departamento de Defensa de los Estados Unidos, que llevó a Internet al uso que tiene hoy en día. La investigación sobre un método electrónico para comunicarse con ubicaciones remotas comenzó ya en la década de 1960 por la inteligencia militar de Estados Unidos. Ellos crearon una red de conmutación de paquetes llamada ARPANET (Advanced Research Projects Agency Network) y el primer uso de **TCP/IP**. TCP/IP significa Transfer Control Protocol/Internet Protocol, las dos unidades funcionales de la primera red de redes (LE VPN, 2017).

El conjunto de protocolos TCP/IP estableció el estándar para redes de computadores como las conocemos hoy en día; HTML, hipervínculos. Finalmente, esta investigación condujo a la institución de la Familia de Protocolos de Internet como un estándar de comunicación militar en 1982 y la posterior adopción del estándar por la industria de informática comercial en 1985. Muchas de las grandes corporaciones, como IBM y AT&T, adoptaron rápidamente la nueva tecnología, aunque sus propias redes internas eran diferentes porque hicieron de la interconectividad de las redes dispares una realidad y algo fácil.

TCP/IP detalla cómo toda la información se empaqueta, aborda, transmite y recibe a través de Internet. Opera en 4 capas; enlace, internet, transporte y aplicación. Las capas de enlace es donde los dispositivos dentro de una red funcionan y donde están más seguras. La capa de internet es donde las redes locales y dispositivos se conectan a otros sitios web y a internet en general, y donde corren el mayor riesgo.

Cuando los paquetes de datos son enviados desde una red local a una red de destino, el paquete se marca con información identificando dónde se originó y hacia dónde se dirige. El sistema funciona bien, pero es deficiente en cuanto a que las miradas indiscretas pueden monitorear el tráfico, interceptar los datos e incluso seguir el flujo de datos de nuevo a la fuente e identificarlo.

Obviamente, a esta altura, la necesidad de contar con una red y seguridad en Internet es clara. La tecnología de seguridad fue investigada por primera vez en 1993 por John Loannidis y sus contemporáneos en grupos de reflexión como la Universidad de Columbia y AT&T Bell Labs. Su trabajo condujo al Software IP Encryption Protocol, también conocido como **SWIPE**, la primera forma de **VPN**. Fue un trabajo experimental que pretendía proporcionar confidencialidad, integridad y autenticación para los usuarios de la red.

A raíz de este trabajo, Xu Wei comenzó su propia investigación en 1994, se centró en la seguridad IP y mejoró los protocolos IP que, finalmente, condujeron al desarrollo del sistema **IPsec**. IPsec es una familia de protocolos de seguridad de internet que autentica y cifra cada paquete de información compartido a través de internet. A medida que la tecnología fue avanzando, de la misma manera lo hizo la velocidad de la conexión. IPSec y una mayor velocidad de conexión, junto con el desarrollo de la función plug-and-play, es lo que hizo realidad la disponibilidad de la VPN en el mercado.

Al mismo tiempo que se creó IPsec, el trabajo en la Biblioteca de Investigación NAVAL, con un subsidio de DARPA, creó el Protocolo de Seguridad de Encapsulación. Se trata de una extensión de seguridad para **SIPP**, adaptado más adelante para sistemas más avanzados, y otro avance para la seguridad en internet y la tecnología VPN. La Carga de Seguridad Encapsulada, **ESP**, ofrece la

autenticidad, integridad y protección de la confidencialidad de los paquetes de datos. Soporta configuraciones de solo encriptación o sólo autenticación, pero hay menos seguros que usar ambos. Este protocolo es similar pero diferente de los Encabezados de Autenticación y proporciona una segunda capa de seguridad para las conexiones a Internet.

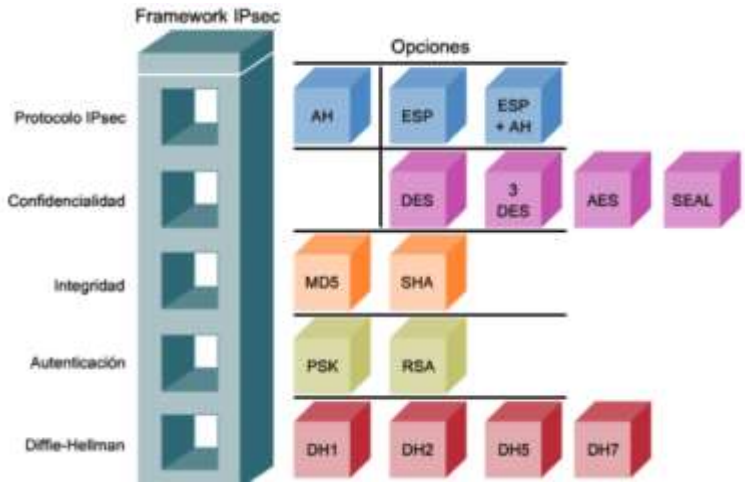


Figura 23. Framework IPsec

En 1995, se creó el grupo de trabajo de IPsec dentro de la **IETF**. El IETF, Internet Engineering Task Force, es una comunidad global de ingenieros de Internet, desarrolladores, programadores, proveedores y otras personas interesadas en la evolución de internet y su buen funcionamiento. Este grupo de trabajo ha trabajado durante años para crear un conjunto estandarizado de protocolos disponibles libremente y examinados abordando los componentes, extensiones y la implementación de IPsec.

El protocolo IPsec utiliza tres sub-protocolos para su implementación; Encabezados de Autenticación, Encapsulating Security Payloads y Asociaciones de Seguridad.

El protocolo de túnel, Modo Túnel, es lo que permite a las VPN funcionar como lo hacen. Permite a un usuario conectarse de forma remota a una red, entre otras

cosas, con una dirección IP que no es parte de la red local. La tunelización funciona alterando la forma de datos, es decir, encriptando y encapsulando, lo que proporciona un tercer y muy buscado beneficio: el anonimato y la privacidad. La forma en que funciona es un poco más compleja, los paquetes que contienen la información que realiza el cifrado y el servicio de entrega se llevan a cabo dentro de la carga útil del mensaje original, pero operan a un nivel más alto que la propia carga útil, creando un escudo formado desde dentro y seguro de las influencias externas. Los mejores servicios cifrarán todo el paquete, el marcador de identificación y todo; a continuación, volverán a encapsularlo con una nueva dirección IP y marca de identificación para obtener una completa privacidad.

La necesidad de una VPN es clara. Internet no es un lugar seguro, en muchos aspectos es el salvaje oeste de las redes, los dispositivos, los usuarios buenos y los usuarios malos. Las conexiones están en riesgo de piratería informática, los sitios web pueden descargar malware, los datos personales son cazados y el flujo de información se ve impedido. Incluso en lugares donde internet es relativamente seguro, encontrarás actividad restrictiva que bloquea el libre flujo de información, que va desde noticias mundiales a los programas de televisión más populares estadounidenses y británicos.

Esto significa que las VPN son tan importantes para la seguridad en internet y el uso de internet como nunca antes lo han sido, y que más personas deberían utilizarlas. La creación de la VPN continuará avanzando junto con internet y, a medida que sus beneficios sean más conocidos, más será su uso.

En 1983, el ingeniero eléctrico estadounidense Fred Cohen, que entonces era estudiante universitario, acuñó el término **"virus"** para describir un programa

informático que se reproduce a sí mismo. Al año siguiente se introdujo el termino **DNS** (Sistema de Nombres de Dominio) (Jcor, 2013)

En el año 1985, aparecieron los primeros Virus Troyanos (caballo de troya), escondidos como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE-LA. En 1986 se crea la gran red de interconexión **NSFNET** para interconectar redes.

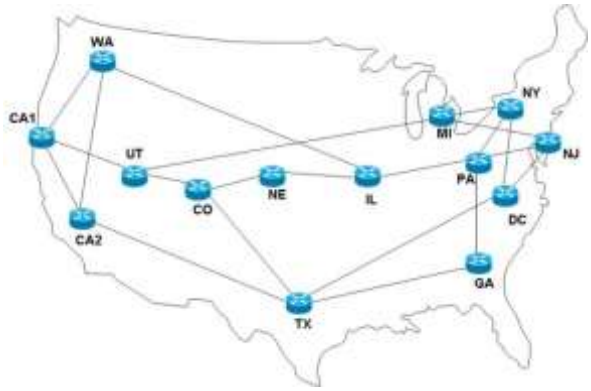


Figura 24. Red NSFNET

El 3 de noviembre de 1988, se produce el primer **Ataque Informático.** Robert Morris, hijo de un experto de computación de la National Security Agency, envía un gusano a través de la red, afectando a 6,000 de los 60,000 hosts existentes. Él programó el gusano para reproducirse a sí mismo y filtrarse a través de los computadores conectados. El tamaño de los archivos llenaba la memoria de las máquinas deshabilitándolas.

Ante la fiebre de la Red, en 1997, bancos e inversionistas volcaron miles de millones de dólares al financiamiento de todo tipo de empresas basadas en la Red, conocidas como **'punto-com'**. Sin embargo, varias de ellas no tenían un modelo de negocio rentable (era baja la penetración de Internet y de los sistemas de pago virtuales) y en el 2001 estalló una gran crisis que llevó a la quiebra a la mayoría.

Fue durante el año 2004 cuando se informó de la existencia del primer código malicioso para plataformas móviles.

Las normas de seguridad de la información ISO 27001, tienen inicio en el año de 1995 a través de la norma BS 7799, con el objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

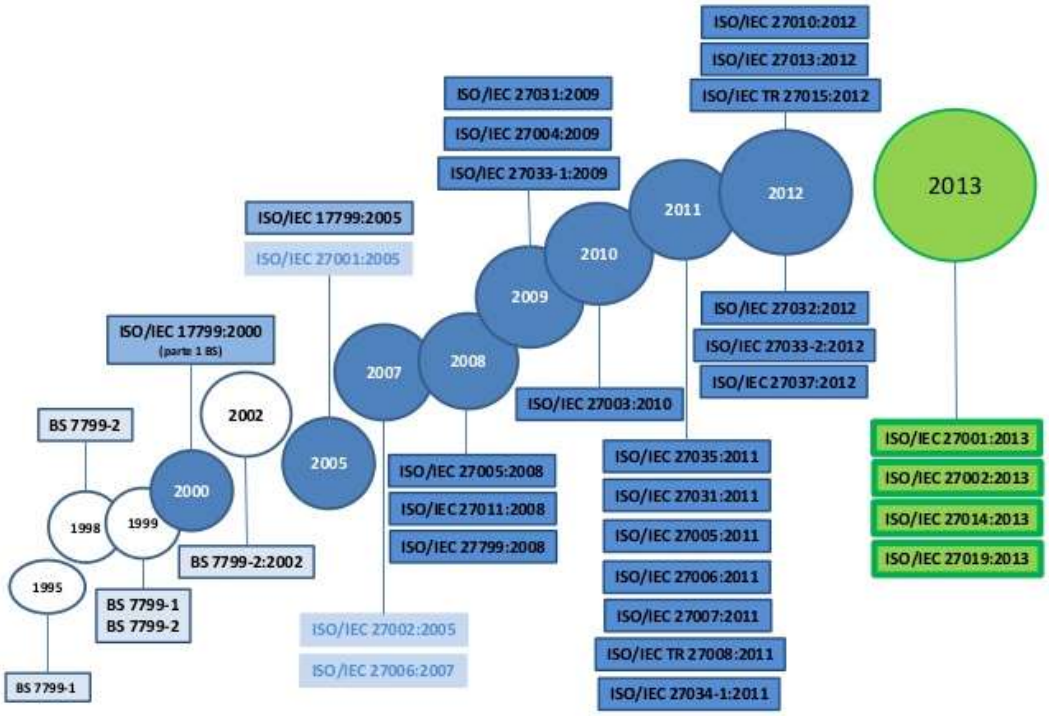


Figura 25. Evolución de las Normas ISO

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente. (ISO 27000.es, 2016)

Qué duda cabe que actualmente Internet al igual que la seguridad informática son los paradigmas de los sistemas telemáticos y, por extensión, una gran parte de los

servicios proporcionados por la telemática se proporcionan a través de la red de redes.

Llegado a este punto se puede se aprecia que ha habido una evolución del proceso de seguridad informática, sobre todo en la última etapa con el despliegue y crecimiento exponencial de Internet, pero aún no se ha profundizado en una metodología para implementar una red privada virtual en un entorno de conexiones públicas que integre los procesos de seguridad informática, los protocolos de encapsulamiento y las políticas de seguridad de la organización.

Conclusiones parciales

- Se realiza una fundamentación del proceso de seguridad informática y su dinámica en redes privadas virtuales, a través del estudio realizado del objeto y el campo de investigación, donde se definen las categorías tales como; confidencialidad, integridad y disponibilidad de la información, autenticación de usuarios, políticas de seguridad y protocolos de seguridad; que luego son retomadas para la elaboración del aporte teórico.
- Para caracterizar los antecedentes históricos del proceso de seguridad informática y su dinámica en redes privadas virtuales, se realizó una revisión por etapas de este proceso que se resume en indicadores de análisis, los cuales denotan que ha habido una evolución del proceso de seguridad informática, sobre todo en la última etapa con el despliegue y crecimiento exponencial de Internet, pero aún no se ha profundizado en una metodología para implementar una red privada virtual en un entorno de conexiones públicas que integre los procesos de seguridad informática, los protocolos de encapsulamiento y las políticas de seguridad de la organización.

CAPÍTULO 2. JUSTIFICACIÓN DEL PROBLEMA Y CARACTERIZACIÓN DEL CAMPO DE ACCIÓN

Introducción

En este capítulo se revelan las deficiencias en el intercambio de información académica contextualizada entre la Universidad Nacional Pedro Ruiz Gallo y el Centro Pre Universitario de dicha entidad; así se determinan los requerimientos y servicios del usuario; los riesgos que generan el intercambio de información a través de las redes informáticas y los mecanismos de seguridad a través de políticas y protocolos en lo fundamental para el aseguramiento de la información, en donde emerge el problema de investigación. Así mismo se caracteriza la situación actual que presenta el proceso de seguridad informática y su dinámica en redes privadas virtuales.

2.1. Justificación del Problema

Está investigación es de mucha relevancia para el intercambio de información académica, debido a que al implementar una metodología adaptativa en base a un modelo seguridad informática para el envío de datos, permitirá mejorar considerable el intercambio de información sobre un medio inseguro como internet.

En el **contexto internacional** la seguridad de la información es uno de los factores fundamentales y de éxito para las organizaciones con la utilización de protocolos y algoritmos de encriptación se garantiza en todo momento que las comunicaciones sean fiables. La seguridad de la información hace uso de métodos de autentificación en la implementación de redes privadas virtuales, asegurando que sólo los usuarios autorizados accedan a ella.

La necesidad de estar comunicados e intercambiar información se puede asociar al trabajo a distancia. El trabajo a distancia consiste en trabajar fuera del lugar de

trabajo tradicional, por ejemplo, desde una oficina doméstica. Los motivos para elegir el trabajo a distancia son diversos e incluyen desde cuestiones de conveniencia personal hasta permitir que los empleados tengan la oportunidad de continuar trabajando cuando están enfermos o tienen una discapacidad (Cisco Networking Academy, 2014).

Muchas empresas modernas tanto en ámbito internacional como en el ámbito nacional, ofrecen oportunidades de empleo para las personas que no pueden trasladarse al trabajo todos los días o para aquellas a las que les resulta más práctico trabajar desde una oficina doméstica.

La seguridad es un motivo de preocupación cuando se utiliza Internet pública para realizar negocios o intercambiar información académica como es el caso de la presente investigación. Las redes virtuales privadas (VPN) se utilizan para garantizar la seguridad de los datos a través de Internet. Se puede proporcionar seguridad a los datos mediante el uso de cifrado en este túnel a través de Internet y con autenticación para proteger los datos contra el acceso no autorizado (Cisco Networking Academy, 2014).

En el **contexto actual** las VPN se configurar con IPsec, este ofrece conectividad flexible y escalable. IPsec es un marco de estándares abiertos que detalla las reglas para las comunicaciones seguras. IPSec no se limita a ningún tipo específico de cifrado, autenticación, algoritmo de seguridad ni tecnología de creación de claves. En realidad, IPsec depende de algoritmos existentes para implementar comunicaciones seguras. IPsec permite que se implementen nuevos y mejores algoritmos sin modificar los estándares existentes de IPsec (Cisco Networking Academy, 2014).

El envío de información de manera segura siempre ha sido un punto crítico en las organizaciones es por ello que se han realizado **diversas investigaciones** como es el caso de (Zhiyong, Guixin, & Hongzhuo, 2014) en este artículo muestran el diseño e implementación un modelo de red VPN seguro y confiable. Este modelo utiliza un protocolo de autenticación con certificado digital y cifrado AES para transferir datos y tiene la función de ataque anti repliegue. Las pruebas realizadas muestran que el modelo soporta una variedad de protocolos de red, lo que es adecuado para las necesidades de desarrollo de la VPN. La forma de configurar la red VPN es simple y práctico, pues tiene una buena perspectiva de aplicación en la transmisión segura a distancia.

Así mismo (Muhamed & Bujar, 2015), manifiesta que al configurar el túnel de encriptación a través de subredes LAN separadas y conectadas por un módem WAN suministrado por el ISP, los resultados indicaron que el aumento del cifrado provoca una disminución significativa en la velocidad de ejecución. Con un conjunto pequeño de registros de tamaño 1000, la diferencia entre la consulta cifrada local y la remota es alta y significativa con respecto a la variable de tiempo. Por ejemplo: La consulta local mostró 0,0052 minutos donde la consulta remota con detalles del protocolo ESP con protocolo de cifrado AES de 256 bits y el protocolo de autenticación MD5 tomó 0,0221 minutos, resultando en más de 400% de tiempo de ejecución más lento al ejecutar el control remoto sobre la consulta local. Mientras ejecutaba una consulta de 100000 registros, la consulta remota era sólo un 15% más lenta. Con 1 millón de consultas ejecutadas remotamente, se requiere un tiempo de ejecución de más del 61% lo que indica un tiempo mayor comparado con el tiempo requerido para ejecutarlo localmente. Teniendo en cuenta que las implementaciones implicaron la creación de un canal cifrado seguro utilizando los protocolos de

seguridad ESP y AH, utilizando algoritmos AES, 3DES y algoritmos de autenticación MD5 y SH1, mayor cantidad de registros demandaron mayores tiempos de ejecución.

Por otro lado (Yadav & Jeyakumar, 2016) en su investigación concluye que el principal reto para la red MPLS es hacer frente a las crecientes necesidades y demandas de varios servicios en cantidad limitada de recursos. Mientras tanto, también debe mantener la calidad de los servicios en términos de pérdida de paquetes, jitter, retraso, privacidad y seguridad. Esta investigación proporciona un diseño para una red tan compleja MPLS habilitado junto con varios criterios y características, demostrando así que también es una tecnología prometedora para el futuro. Cada paso requerido para diseñar una red MPLS VPN de ingeniería de tráfico con protección de trayecto se menciona y se demuestra implementando el escenario en el software GNS3. El uso de este diseño limitará el desperdicio de enlaces no utilizados y en su lugar proporcionará ruta tunelizada para cada cliente en el mismo instante y en la misma infraestructura de red. Esto a su vez demostrará ser rentable para los clientes y el proveedor de servicios. La implementación del diseño propuesto seguramente reducirá parámetros como la pérdida de paquetes y el retraso. La seguridad y la privatización del enlace se logra utilizando MPLS VPN complejas, que imponen restricciones a la conectividad con clientes no deseados. La funcionalidad de conmutación por error se proporciona para el servicio garantizado a los clientes al proporcionar protección de ruta a los túneles de ingeniería de tráfico importantes.

Por último, la empresa Golden frong de España (Golden Frog, 2017), dedicada a brindar soluciones de privacidad y seguridad en Internet, muestra una tabla comparativa de los protocolos para VPN.

Tabla 1. *Comparación de protocolos para VPN*

	PPTP	L2TP/IPSec	OpenVPN	Chameleon
ENCRIPTACIÓN VPN	128-bits	256-bit	160 bits 256-bit	256-bit
COMPATIBLE CON LAS APPS DE VYPRVPN	Windows Router	Windows Mac iOS (Solo IPsec/IKEv2)	Windows Mac Android Router Anonabox	Windows Mac Android Router
COMPATIBLE CON CONFIGURACIÓN MANUAL	Windows Mac OS X Linux iOS Android Synology	Windows Mac OS X iOS Android Blackberry 10 (Solo IPsec) Chromebook	Windows, Mac OS X Linux iOS Android DD-WRT OpenWRT AsusWRT/Merlin Synology	Configuración manual no compatible

SEGURIDAD VPN	Encriptación básica	La máxima encriptación. Comprueba la integridad de los datos y encapsula los datos dos veces.	La máxima encriptación. Autentifica los datos con certificados digitales.	La máxima encriptación. Autentifica los datos con certificados digitales.
VELOCIDAD DE VPN	Rápido debido a la encriptación más baja.	Necesita más proceso de la CPU para encapsular los datos dos veces.	Protocolo con mejor rendimiento. Velocidades elevadas, incluso en conexiones con alta latencia y a grandes distancias.	El protocolo que ofrece mejor rendimiento. Frustra la inspección profunda de paquetes. Altas velocidades incluso en conexiones con alta latencia y en grandes distancias.
ESTABILIDAD	Funciona bien en la mayoría de puntos de acceso Wi-Fi, muy estable.	Compatible con dispositivos NAT.	La más fiable y estable, incluso tras routers inalámbricos, en redes no fiables, y en puntos de acceso Wi-Fi.	Oculta el tráfico de VPN para que no pueda ser identificada como una conexión VPN (por medio de la inspección profunda de paquetes) ni bloqueada.

COMPATIBILIDAD	Nativo en la mayoría de los sistemas operativos de dispositivos de sobremesa, portátiles y tablets.	Nativo en la mayoría de los sistemas operativos de dispositivos de sobremesa, portátiles y tablets.	Compatible con la mayoría de los sistemas operativos de computadores de sobremesa y dispositivos Android móviles y tabletas.	Compatible con la mayoría de los sistemas operativos de computadores de sobremesa y dispositivos Android móviles y tabletas.
CONCLUSIÓN	Es un protocolo rápido, fácil de usar. Es una buena elección si su dispositivo no soporta OpenVPN.	Es una buena elección si su dispositivo no soporta OpenVPN y la seguridad es la prioridad máxima.	Es el protocolo recomendado para equipos de sobremesa incluyendo Windows, Mac OS X y Linux. El máximo rendimiento - rápido, seguro y fiable.	Es excelente para usuarios de VPN que están siendo bloqueados en países como como China, o si está sufriendo problemas de velocidad debido a la reducción del ancho de banda.

Fuente: (Golden Frog, 2017)

2.2. Diagnóstico del estado actual del proceso de seguridad informática y su dinámica en redes privadas virtuales de la Universidad Nacional Pedro Ruiz Gallo.

Para diagnosticar el estado actual del proceso de seguridad informática y su dinámica en redes privadas virtuales, se encuestó a 8 empleados especialistas en TI de la Oficina General de Sistemas Informáticos (Incluye el aérea de la Red Telemática) y 24 trabajadores administrativos de la Oficina General de Admisión, Oficina de Asuntos Académicos de la Universidad Nacional Pedro Ruiz Gallo y del área Académica del Centro Pre Universitario. La encuesta fue aplicada en el mes de mayo del 2018. A continuación, se presentan los resultados obtenidos.

Para el caso de la encuesta se utilizó un cuestionario, teniendo como medida la escala de Likert, como se puede observar en la tabla N° 2.

Tabla 2. *Puntuación de los Ítems en la escala de Likert*

Puntuación	Denominación	Inicial
1	Totalmente en Desacuerdo	TD
2	Desacuerdo	D
3	Ni en Acuerdo Ni es Desacuerdo	I
4	De Acuerdo	DA
5	Totalmente de Acuerdo	TA

Fuente: Elaboración propia

a. Encuesta a especialistas en Tecnologías de la Información de la entidad

Tabla 3. *¿Considera usted, que los directivos o jefes inmediatos se involucran o comprometen en el desarrollo de proyectos relacionados a las TIC?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	2	25%
Desacuerdo	D	1	13%
Ni en Acuerdo, Ni en Desacuerdo	I	0	0%
De Acuerdo	A	3	38%
Totalmente Acuerdo	TA	2	25%
Total		8	100%

Fuente: Elaboración propia

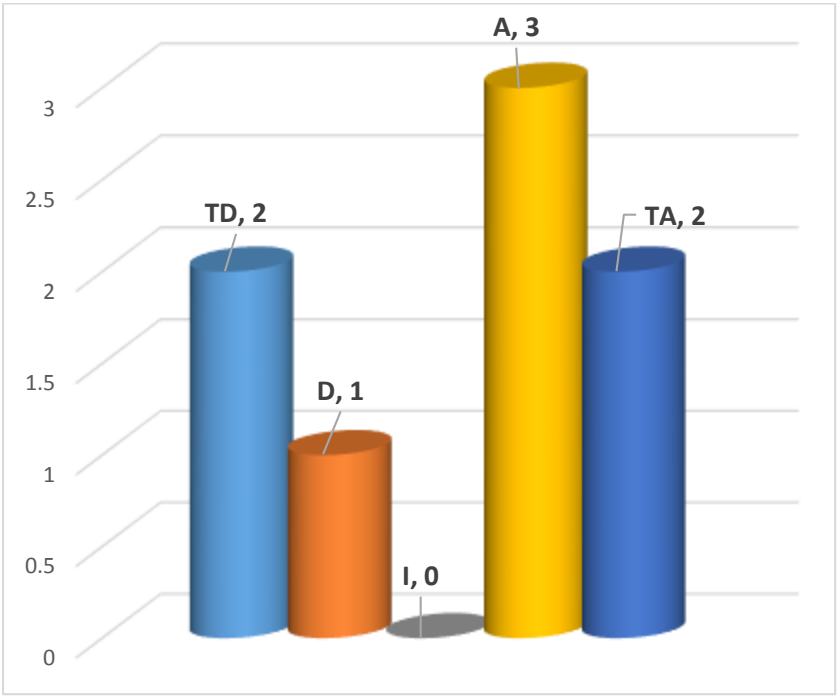


Figura 26. Involucramiento de los jefes inmediatos

Fuente: Elaboración propia

Los encuestados indican que los directivos o jefes inmediatos se involucran en cierta medida, un 63% afirma ello en el desarrollo de los proyectos de TI, mientras que un 38% de los encuestados manifiesta que los directivos o jefes inmediatos no se interesan por el desarrollo de nuevos proyectos relacionados a las TIC.

Tabla 4. *¿Cree usted, que los especialistas en TIC de la Universidad, son responsables de sugerir nuevos proyectos en TIC?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	1	13%
Desacuerdo	D	3	38%
Ni en Acuerdo, Ni en Desacuerdo	I	0	0%
De Acuerdo	A	3	38%
Totalmente Acuerdo	TA	1	13%
Total		8	100%

Fuente: Elaboración propia

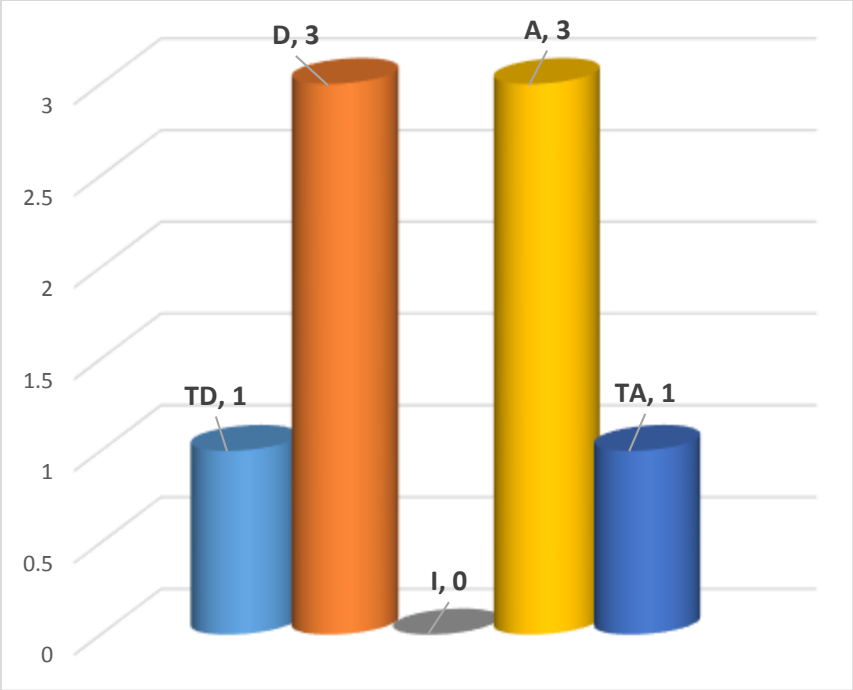


Figura 27. Responsabilidad de los especialistas en TIC

Fuente: Elaboración propia

El 50% de los empleados en TI encuestados, manifiesta que no solo ellos son los responsables de sugerir nuevos proyectos en TIC, mientras que en igual medida el resto de empleados encuestados piensa lo contario, lo que indica que es necesario comprometer a los directivos en la implementación de nuevos y más proyectos en TI.

Tabla 5. *¿Considera importante, realizar un diseño topológico de la red que permita el intercambio de información académica entre la Universidad sede Lambayeque y el Centro Pre Universitario Sede Chiclayo?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	0	0%
Desacuerdo	D	1	13%
Ni en Acuerdo, Ni en Desacuerdo	I	0	0%
De Acuerdo	A	4	50%
Totalmente Acuerdo	TA	3	38%
Total		8	100%

Fuente: Elaboración propia

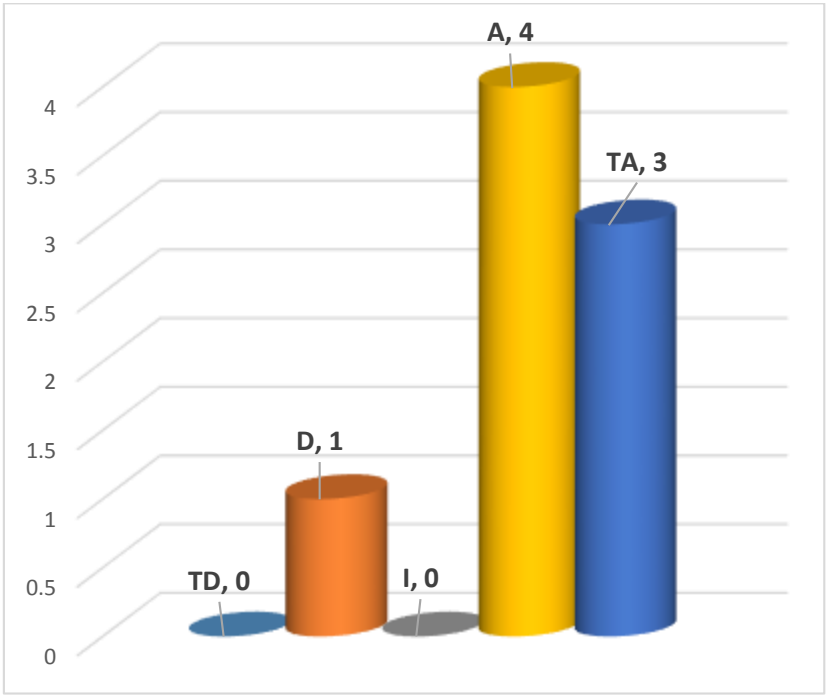


Figura 28. Importancia del diseño topológico de la red

Fuente: Elaboración propia

El 50% y 38% de empleados en TI encuestados está de acuerdo y totalmente de acuerdo respectivamente que se tiene que realizar previamente un diseño topológico de la red que garantice el intercambio de información entre la Universidad sede Lambayeque el Centro Pre Universitario sede Chiclayo.

Tabla 6. *¿Considera importante, que para conectarse a una red privada virtual desde el lugar donde se encuentre, es necesario contar con componentes móviles (conexión a internet, computador y software VPN instalado en la PC)?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	1	13%
Desacuerdo	D	1	13%
Ni en Acuerdo, Ni en Desacuerdo	I	0	0%
De Acuerdo	A	2	25%
Totalmente Acuerdo	TA	4	50%
Total		8	100%

Fuente: Elaboración propia

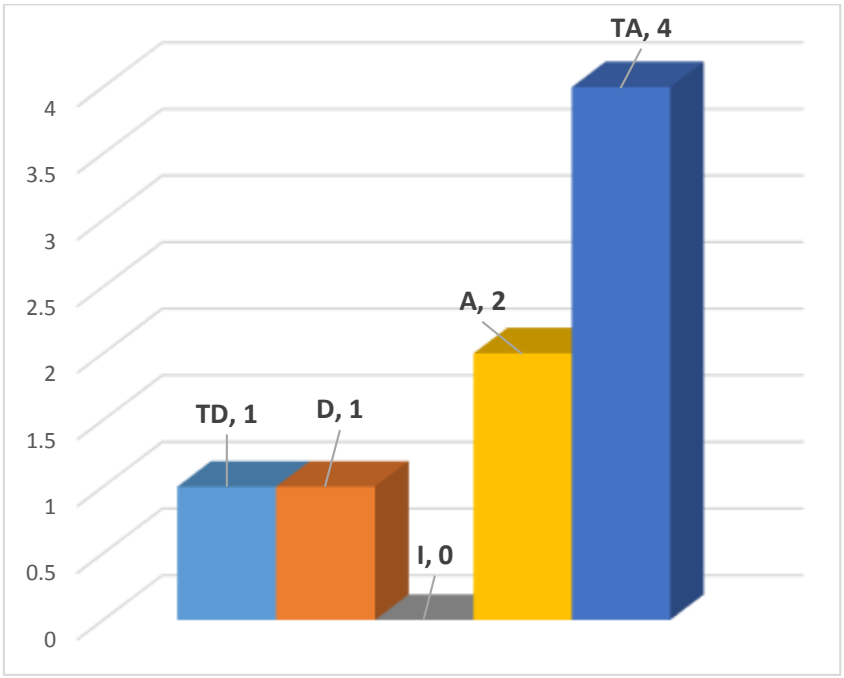


Figura 29. Importancia de contar con componentes móviles

Fuente: Elaboración propia

Del 100% de los encuestados se logró determinar que el 25% de los empleados en TI de la entidad está de acuerdo y el 50% está totalmente de acuerdo, que para conectarse a una VPN de manera remota es necesario que el usuario cuente con componentes móviles (conexión a internet, dispositivo móvil, software VPN instalado, entre otros); mientras que un 26% de los encuestados manifiesta su desacuerdo.

Tabla 7. *¿Considera importante que, para conectarse a una red privada virtual desde una sede central o remota, es necesario contar con componentes corporativos (routers VPN, firewall, concentrador VPN)?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	0	0%
Desacuerdo	D	1	13%
Ni en Acuerdo, Ni en Desacuerdo	I	0	0%
De Acuerdo	A	3	38%
Totalmente Acuerdo	TA	4	50%
Total		8	100%

Fuente: Elaboración propia

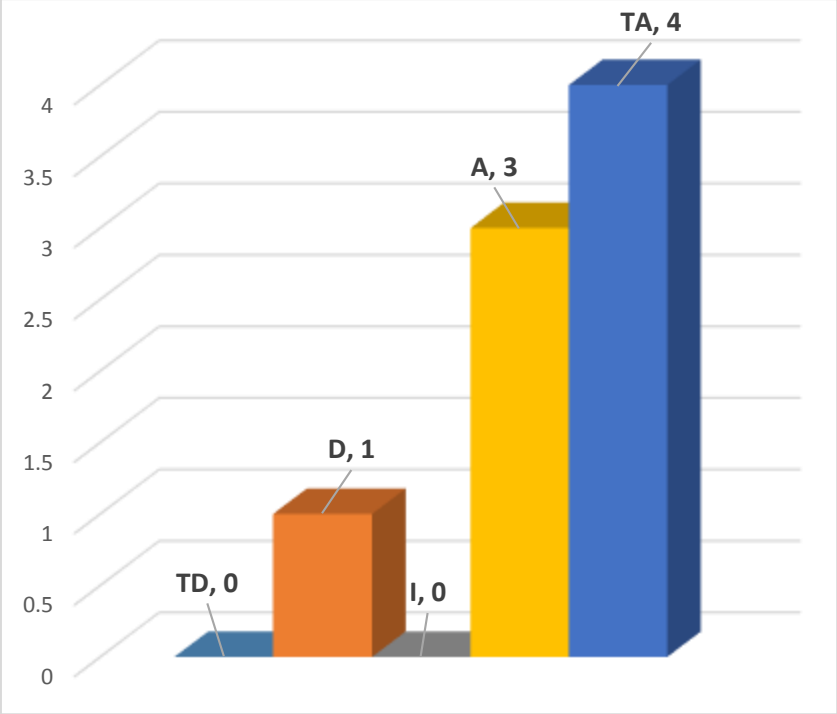


Figura 30. Importancia de contar con componentes corporativos

Fuente: Elaboración propia

Del 100% de los encuestados se logró determinar que el 88% de los empleados en TI de la entidad está de acuerdo, que para conectarse a través de una VPN de sitio a sitio es necesario que las sedes cuenten con componentes corporativos (routers VPN, firewall, concentrador VPN, entre otros); mientras que un 13% de los encuestados manifiesta su desacuerdo.

Tabla 8. *¿Considera necesario, la identificación y aceptación de riesgos que se puedan presentar en la red telemática?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	0	0%
Desacuerdo	D	1	13%
Ni en Acuerdo, Ni en Desacuerdo	I	0	0%
De Acuerdo	A	4	50%
Totalmente Acuerdo	TA	3	38%
Total		8	100%

Fuente: Elaboración propia

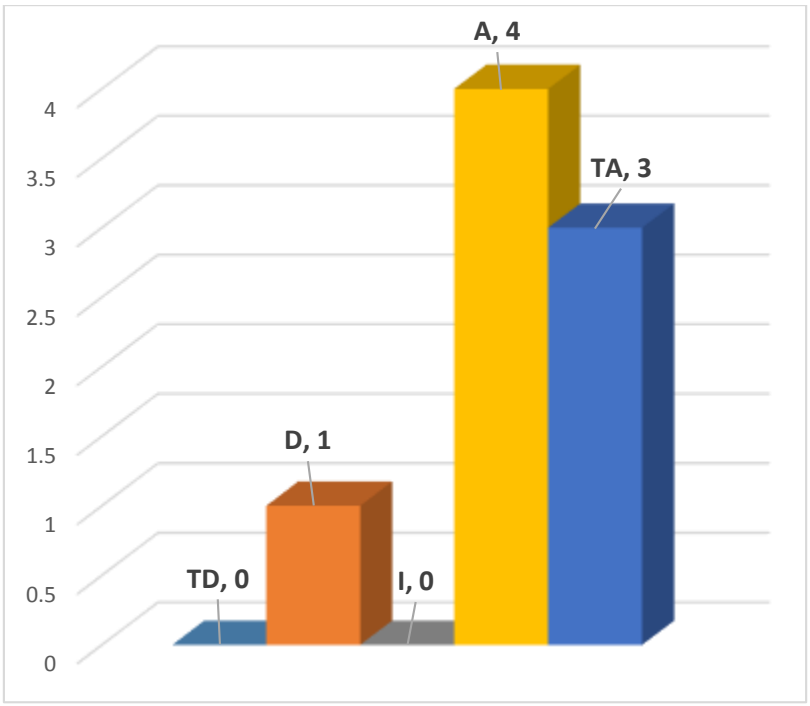


Figura 31. Necesidad de identificar y aceptar los riesgos

Fuente: Elaboración propia

Los resultados nos muestran que el 50% y 38% de los encuestados está de acuerdo y totalmente de acuerdo respectivamente y considera que es muy necesario que se identifiquen y acepten los riesgos que puedan presentarse en la red telemática de la Universidad Nacional Pedro Ruiz Gallo, mientras que un 13% cree todo lo contrario.

Tabla 9. *¿Cree usted, que la mitigación de riesgos contribuye a mejorar la seguridad informática en la red telemática?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	0	0%
Desacuerdo	D	2	25%
Ni en Acuerdo, Ni en Desacuerdo	I	0	0%
De Acuerdo	A	4	50%
Totalmente Acuerdo	TA	2	25%
Total		8	100%

Fuente: Elaboración propia

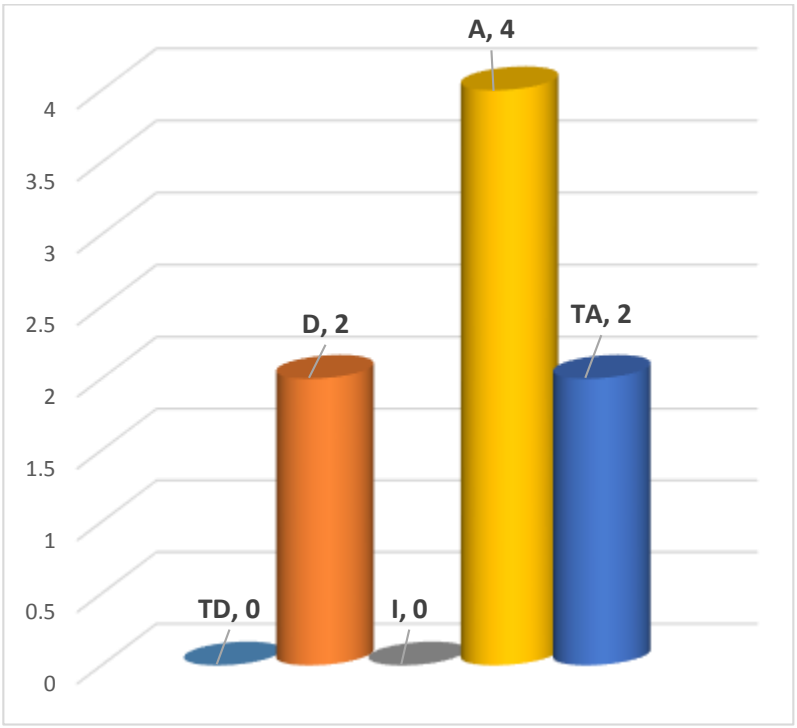


Figura 32. Mitigación de riesgos para mejorar la seguridad informática

Fuente: Elaboración propia

El 75% de los empleados en TI de la Universidad encuestados, precisan que mitigar los riesgos contribuye a mejorar la seguridad informática de la red telemática de la Universidad, lo cual indica que se tiene que definir controles para aquellos riesgos identificados, con la finalidad de reducir el impacto en caso sucedan.

Tabla 10. *¿Considera necesario, establecer controles de acceso físico a los ambientes de procesamiento de información?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	0	0%
Desacuerdo	D	1	13%
Ni en Acuerdo, Ni en Desacuerdo	I	1	13%
De Acuerdo	A	2	25%
Totalmente Acuerdo	TA	4	50%
Total		8	100%

Fuente: Elaboración propia

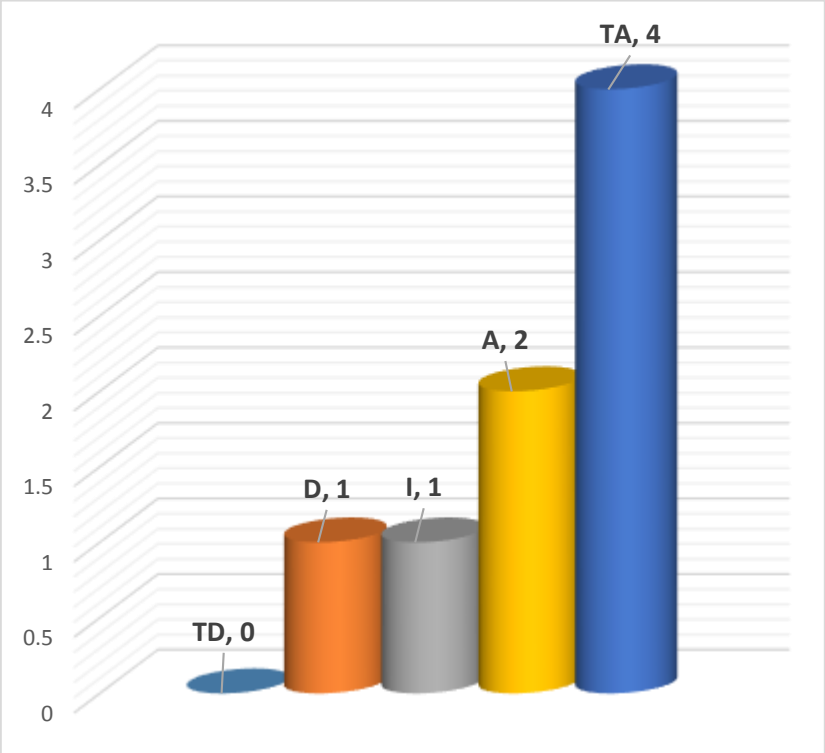


Figura 33. Necesidad de establecer controles de acceso físico

Fuente: Elaboración propia

El 25% y 50% de empleados en TI encuestados está de acuerdo y totalmente de acuerdo respectivamente que es necesario establecer controles de acceso físico a los ambientes de procesamiento de información de la Universidad Nacional Pedro Ruiz Gallo, lo cual contribuye a mejorar la seguridad física de estos ambientes.

Tabla 11. *¿Considera necesario, establecer políticas de mantenimiento de equipamiento para los usuarios de la red telemática?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	0	0%
Desacuerdo	D	1	13%
Ni en Acuerdo, Ni en Desacuerdo	I	0	0%
De Acuerdo	A	4	50%
Totalmente Acuerdo	TA	3	38%
Total		8	100%

Fuente: Elaboración propia

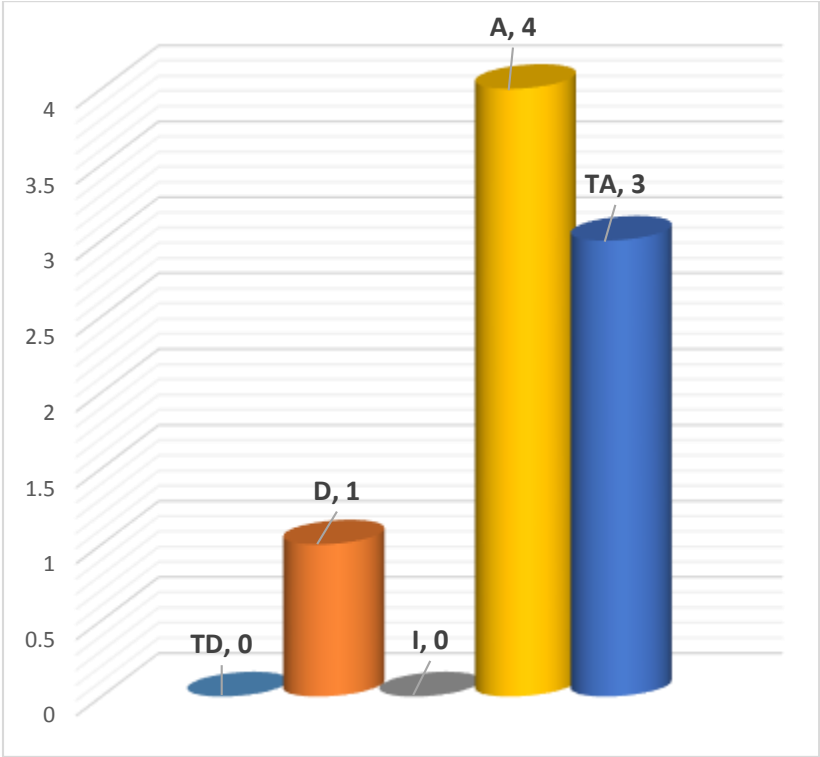


Figura 34. Necesidad de establecer políticas de mantenimiento de equipos

Fuente: Elaboración propia

Los resultados nos muestran que el 50% y 38% de los empleados en TI encuestados están de acuerdo y totalmente de acuerdo respectivamente, al considerar muy necesario establecer políticas de mantenimiento de equipamiento para los usuarios de la red telemática de la Universidad.

Tabla 12. *¿Cree usted necesario, establecer políticas de escritorios y pantallas limpias para los usuarios de la red telemática?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	0	0%
Desacuerdo	D	1	13%
Ni en Acuerdo, Ni en Desacuerdo	I	1	13%
De Acuerdo	A	4	50%
Totalmente Acuerdo	TA	2	25%
Total		8	100%

Fuente: Elaboración propia

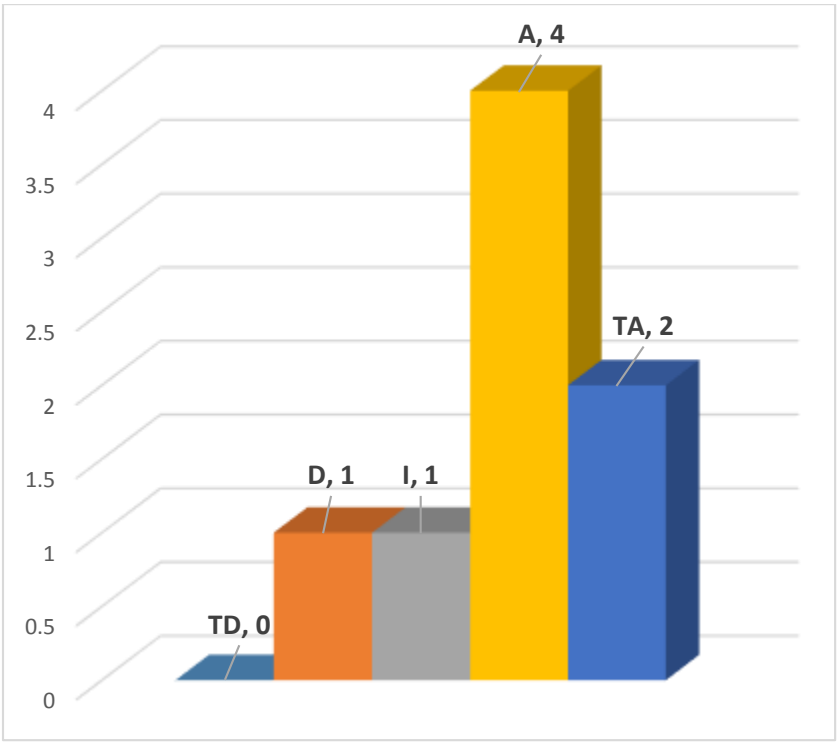


Figura 35. Necesidad de establecer políticas de escritorio y pantallas limpias

Fuente: Elaboración propia

El 75% de empleados en TI encuestados considera que es necesario establecer políticas de escritorio y pantallas limpias para los usuarios de la red telemática de la Universidad Nacional Pedro Ruiz Gallo, por el contrario, un 13% se muestra indiferente ante la consulta planteada.

Tabla 13. *¿Cree usted necesario implementar políticas de resguardo de información para los usuarios de la red telemática?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	0	0%
Desacuerdo	D	0	0%
Ni en Acuerdo, Ni en Desacuerdo	I	1	13%
De Acuerdo	A	4	50%
Totalmente Acuerdo	TA	3	38%
Total		8	100%

Fuente: Elaboración propia

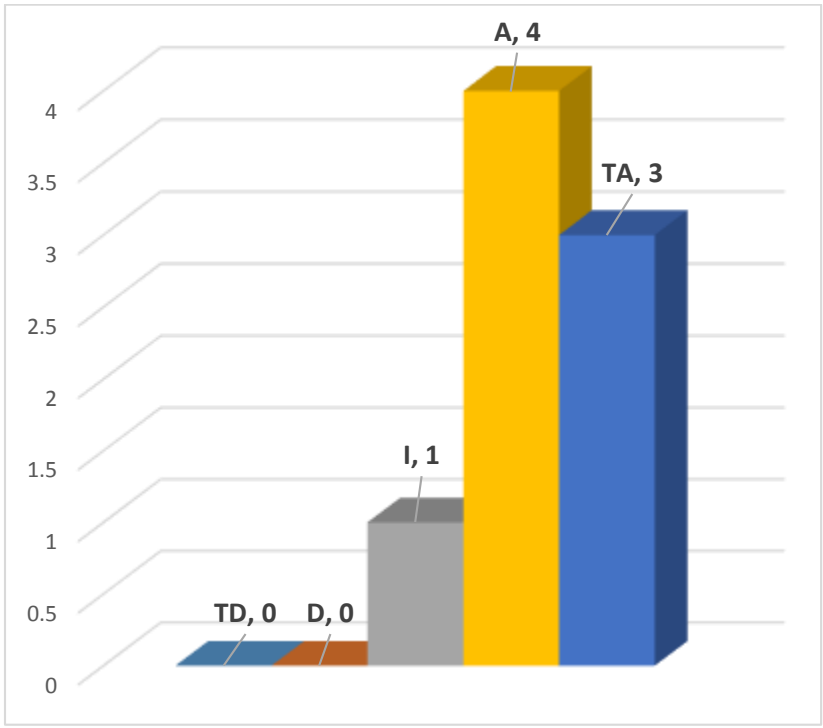


Figura 36. Necesidad de establecer políticas de resguardo de información

Fuente: Elaboración propia

El 88% de empleados en TI encuestados considera que es necesario implementar políticas de resguardo de información para los usuarios de la red telemática de la Universidad Nacional Pedro Ruiz Gallo, lo cual constituye una buena práctica respaldar la información.

Tabla 14. *¿Considera necesario, establecer controles de seguridad de los datos entre los usuarios de la red telemática?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	1	13%
Desacuerdo	D	2	25%
Ni en Acuerdo, Ni en Desacuerdo	I	0	0%
De Acuerdo	A	3	38%
Totalmente Acuerdo	TA	2	25%
Total		8	100%

Fuente: Elaboración propia

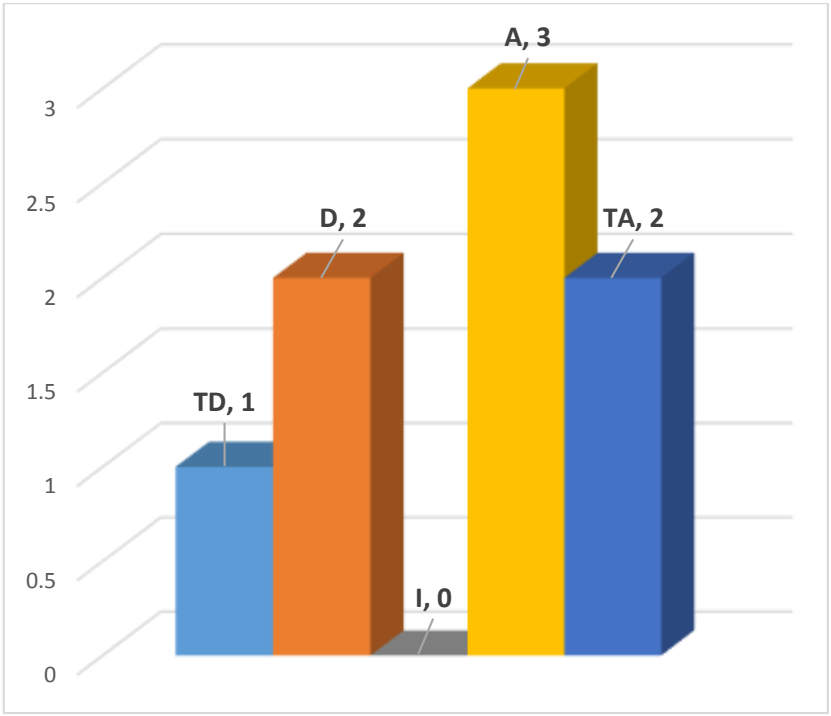


Figura 37. Necesidad de establecer controles de seguridad de los datos

Fuente: Elaboración propia

Del 100% de los encuestados se pudo determinar que el 38% de los empleados en TI de la entidad está de acuerdo y el 25% está totalmente de acuerdo, que es necesario establecer controles de seguridad de los datos para los usuarios de la red telemática de la Universidad Nacional Pedro Ruiz Gallo, mientras que el 33% de los encuestados no cree necesario establecer está política.

b. Encuesta a empleados administrativos de la entidad

Tabla 15. *¿Considera importante que, como empleado de la entidad, usted es responsable de generar y consumir información?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	6	25%
Desacuerdo	D	8	33%
Ni en Acuerdo, Ni en Desacuerdo	I	1	4%
De Acuerdo	A	5	21%
Totalmente Acuerdo	TA	4	17%
Total		24	100%

Fuente: Elaboración propia

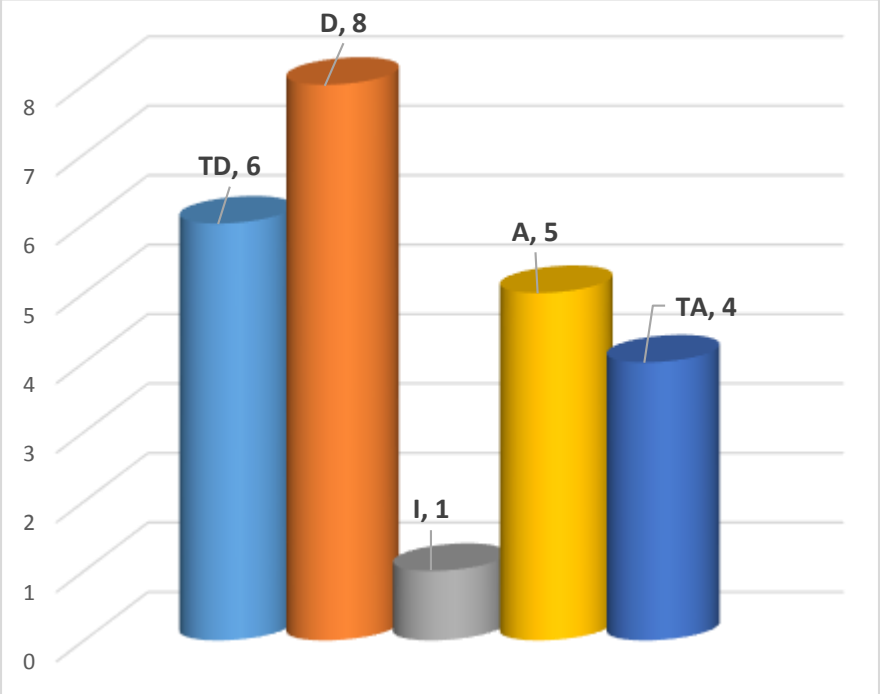


Figura 38. Responsabilidad de los empleados con la información

Fuente: Elaboración propia

El 38% de los encuestados indican que como empleados de la entidad son responsables de generar y consumir información, mientras que el 58% afirma lo contrario, notando un gran desinterés por contribuir con la entidad en los procesos de transformación de información.

Tabla 16. *¿Cree usted, que ante la implementación de un nuevo proyecto de red es necesario que, como usuario, pueda indicar sus requerimientos para este proyecto?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	2	8%
Desacuerdo	D	4	17%
Ni en Acuerdo, Ni en Desacuerdo	I	1	4%
De Acuerdo	A	9	38%
Totalmente Acuerdo	TA	8	33%
Total		24	100%

Fuente: Elaboración propia

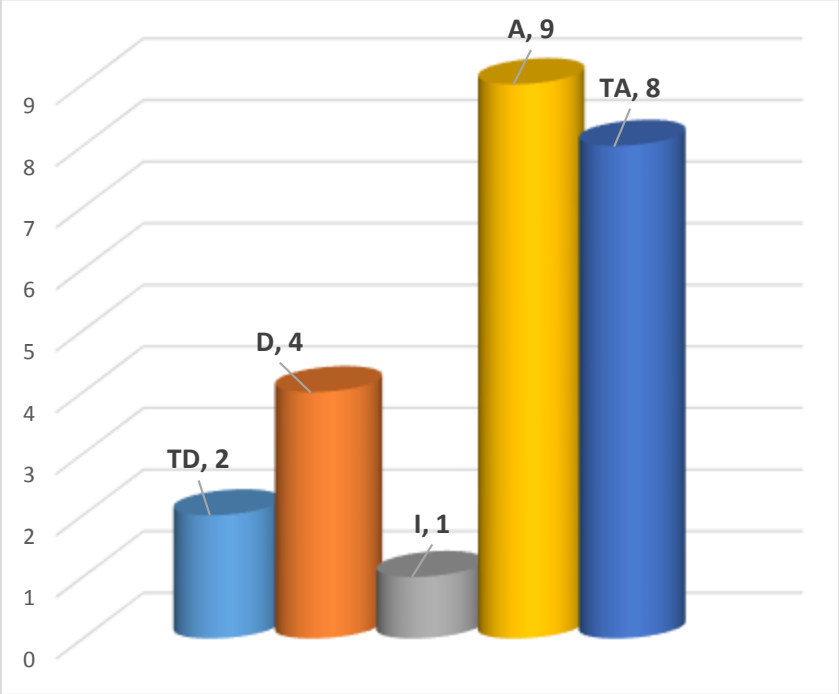


Figura 39. Necesidad de indicar los requerimientos de usuario

Fuente: Elaboración propia

Los resultados nos muestran que el 71% de los encuestados considera de vital importancia manifestar sus requerimientos ante la implementación de un nuevo proyecto de red en la entidad, mientras que el 25% asume que no es necesario ello.

Tabla 17. *¿Considera usted, que los servicios de red (Telefonía IP, acceso a los sistemas de información, autenticación de usuarios) se han definido en función de los requerimientos del usuario?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	3	13%
Desacuerdo	D	5	21%
Ni en Acuerdo, Ni en Desacuerdo	I	1	4%
De Acuerdo	A	8	33%
Totalmente Acuerdo	TA	7	29%
Total		24	100%

Fuente: Elaboración propia

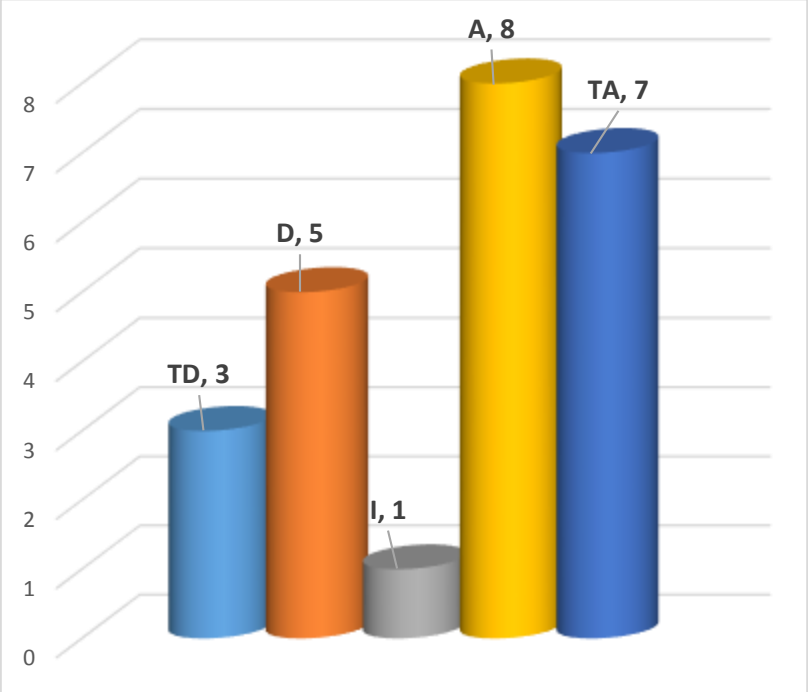


Figura 40. Consideraciones para los servicios de red

Fuente: Elaboración propia

Del 100% de los encuestados se logo determinar que el 63% de los empleados administrativos encuestados indica que los servicios de red como, por ejemplo: telefonía IP, correo, mensajería, acceso a los sistemas de información, entre otros; han sido definidos en función de las necesidades del usuario, mientras que el 33% indica lo contrario.

Tabla 18. *¿En la entidad, considera que cada de empleado accede de manera segura para conectarse a la red telemática?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	7	29%
Desacuerdo	D	9	38%
Ni en Acuerdo, Ni en Desacuerdo	I	2	8%
De Acuerdo	A	3	13%
Totalmente Acuerdo	TA	3	13%
Total		24	100%

Fuente: Elaboración propia

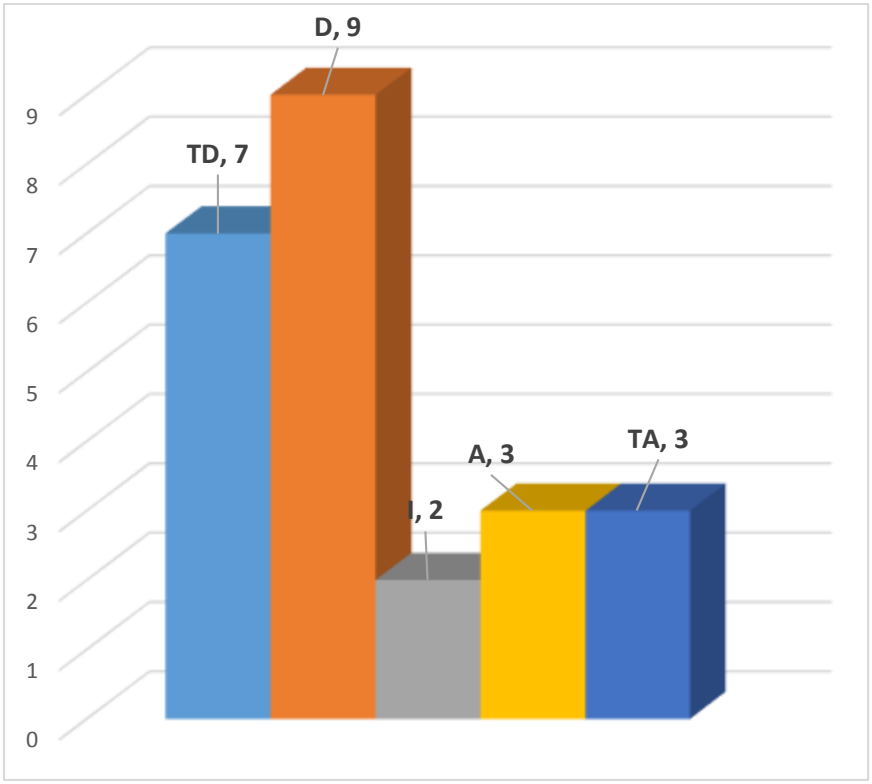


Figura 41. Consideraciones de acceso seguro a la red

Fuente: Elaboración propia

El 67% de los empleados administrativos encuestados en la entidad, considera que no se siente seguro al acceder a los servicios de la red telemática, mientras que un 26% cree sentirse seguro al conectarse a la red de la Universidad Nacional Pedro Ruiz Gallo.

Tabla 19. *¿Considera que la información debe viajar encriptada y que no esté sujeta a interceptaciones por parte de usuarios maliciosos?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	1	4%
Desacuerdo	D	2	8%
Ni en Acuerdo, Ni en Desacuerdo	I	1	4%
De Acuerdo	A	11	46%
Totalmente Acuerdo	TA	9	38%
Total		24	100%

Fuente: Elaboración propia

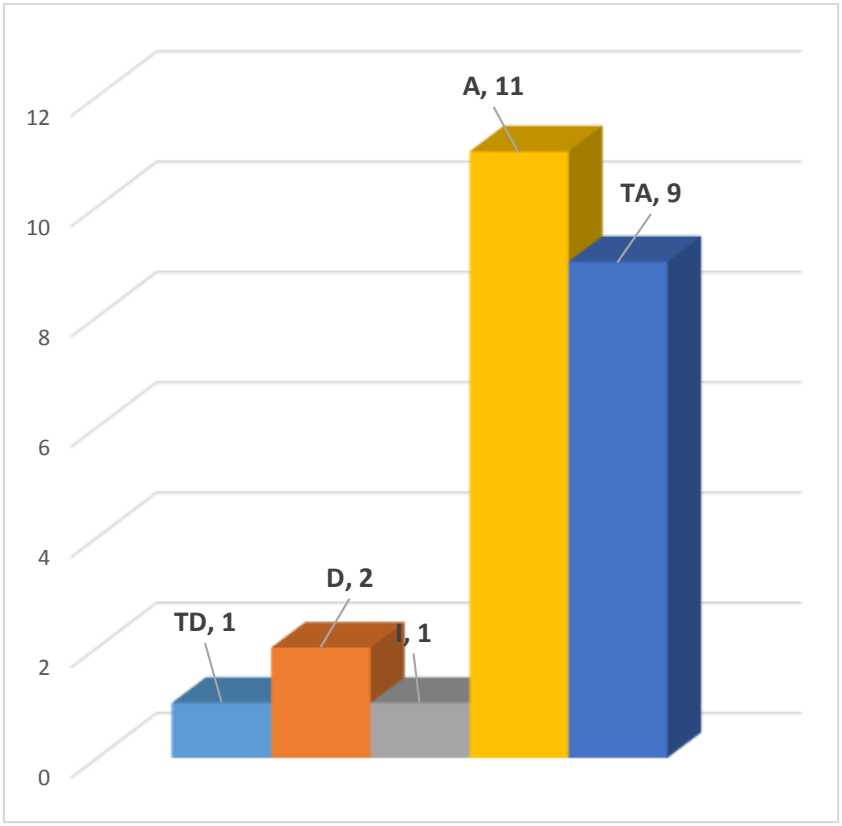


Figura 42. Consideraciones de encriptación de la información

Fuente: Elaboración propia

Los encuestados indican que la información debe viajar encriptada y que no esté sujeta a interceptaciones por parte de usuarios maliciosos, un 83% lo considera así, mientras que un 12% considera que no es necesario aplicar estos métodos de seguridad informática.

Tabla 20. *¿Se siente seguro al enviar información por la red de la Universidad?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	9	38%
Desacuerdo	D	10	42%
Ni en Acuerdo, Ni en Desacuerdo	I	2	8%
De Acuerdo	A	1	4%
Totalmente Acuerdo	TA	2	8%
Total		24	100%

Fuente: Elaboración propia

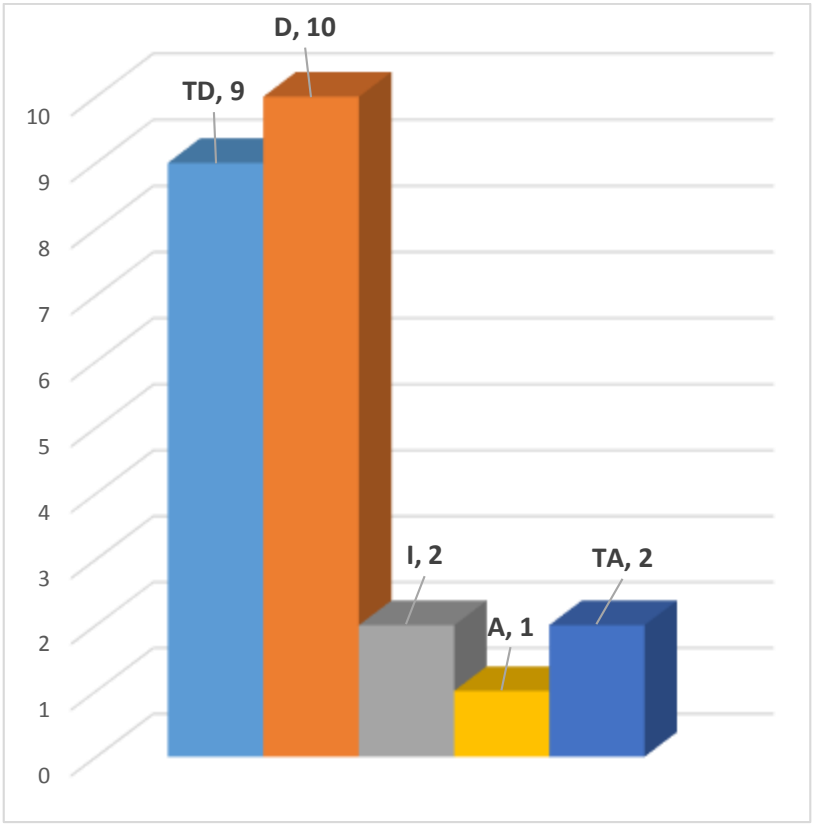


Figura 43. Percepción de seguridad al enviar la información por la red de la Universidad

Fuente: Elaboración propia

Los resultados nos muestran que el 79% de los empleados administrativos encuestados de la entidad, manifiesta que no se sienten seguros al enviar información por la red de la Universidad, con lo que se puede evidenciar una falta de cultura en seguridad informática por parte de los empleados administrativos de la entidad.

Tabla 21. *¿Cree usted, que su información puede ser interceptada por algún otro usuario de la red Telemática?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	8	33%
Desacuerdo	D	9	38%
Ni en Acuerdo, Ni en Desacuerdo	I	2	8%
De Acuerdo	A	3	13%
Totalmente Acuerdo	TA	2	8%
Total		24	100%

Fuente: Elaboración propia

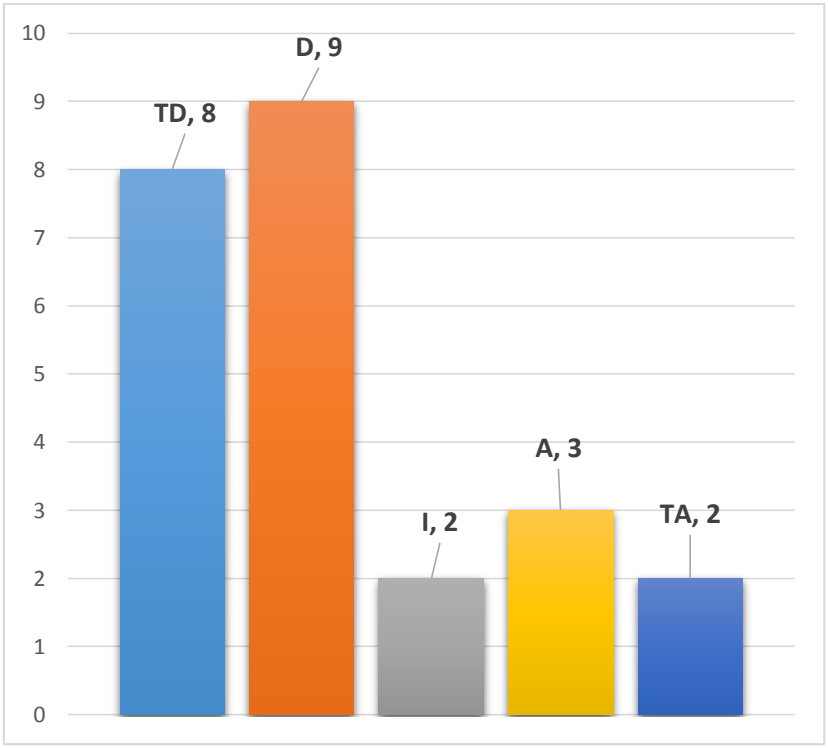


Figura 44. Percepción de que la información pueda ser interceptada por otro usuario de la red

Fuente: Elaboración propia

La percepción de inseguridad por parte de los empleados administrativos encuestados en la entidad continúa, el 71% cree que su información podría ser interceptada por algún otro usuario de la red telemática, situación que conlleva a fortalecer por medio de capacitaciones talleres a usuarios, a despejar los mitos en temas de inseguridad informática.

Tabla 22. *¿Se siente preparado para asumir algún tipo de riesgo frente a la perdida, alteración o robo de información?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	6	25%
Desacuerdo	D	9	38%
Ni en Acuerdo, Ni en Desacuerdo	I	1	4%
De Acuerdo	A	5	21%
Totalmente Acuerdo	TA	3	13%
Total		24	100%

Fuente: Elaboración propia

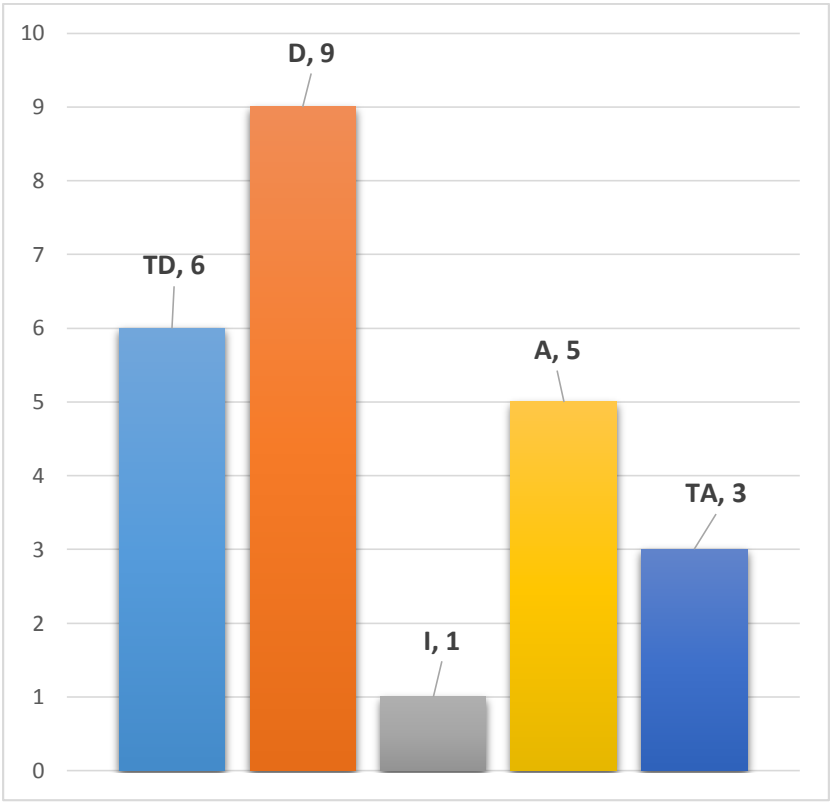


Figura 45. Sensación de asumir riesgos ante la pérdida, robo o alteración de información

Fuente: Elaboración propia

Del 100% de los empleados administrativos encuestados de la entidad, se pudo determinar que solo una tercera parte (34%) de ellos se siente preparado para enfrentar y asumir algún tipo de riesgo frente a la perdida, alteración o robo de información.

Tabla 23. *¿Ha recibido algún de capacitación por parte de la entidad referente a políticas de seguridad de la información?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	9	38%
Desacuerdo	D	12	50%
Ni en Acuerdo, Ni en Desacuerdo	I	0	0%
De Acuerdo	A	1	4%
Totalmente Acuerdo	TA	2	8%
Total		24	100%

Fuente: Elaboración propia

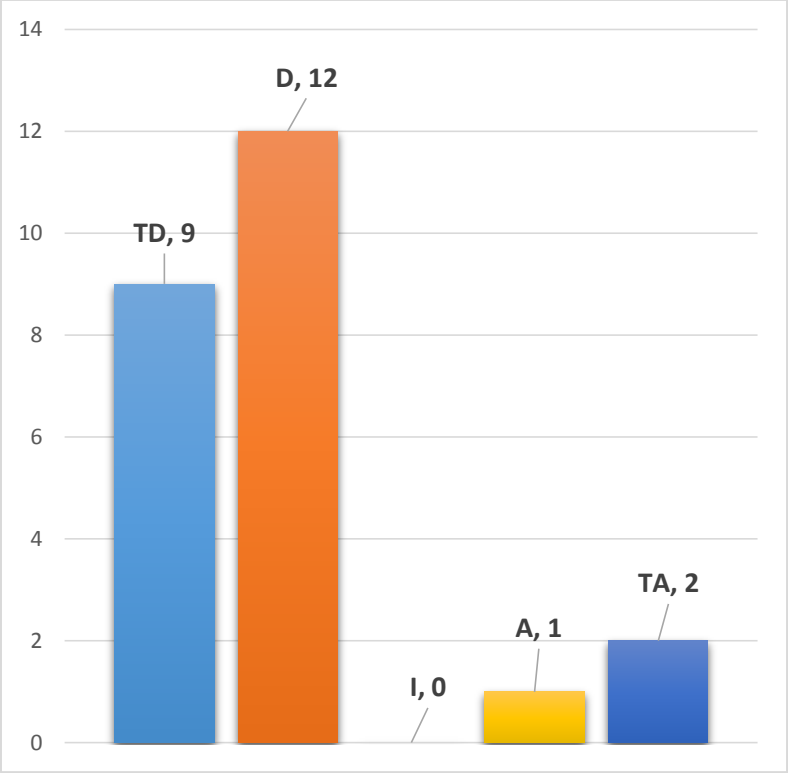


Figura 46. Capacitación por parte de la entidad en políticas de seguridad de la información

Fuente: Elaboración propia

Frente a las sensaciones de inseguridad percibidas por los empleados administrativos de la Universidad, se puede corroborar que el 88% de los encuestados no ha recibido algún tipo de capacitación por parte de la entidad referente a políticas de seguridad de la información, mientras que un 12% indica haber recibido algún tipo de capitación al respecto.

Tabla 24. *¿Considera necesario, que el intercambio de información entre los usuarios de la red telemática tendría estar normada por protocolos de seguridad?*

Escala	Iniciales	Frecuencia	Porcentaje
Totalmente en Desacuerdo	TD	1	4%
Desacuerdo	D	2	8%
Ni en Acuerdo, Ni en Desacuerdo	I	2	8%
De Acuerdo	A	9	38%
Totalmente Acuerdo	TA	10	42%
Total		24	100%

Fuente: Elaboración propia

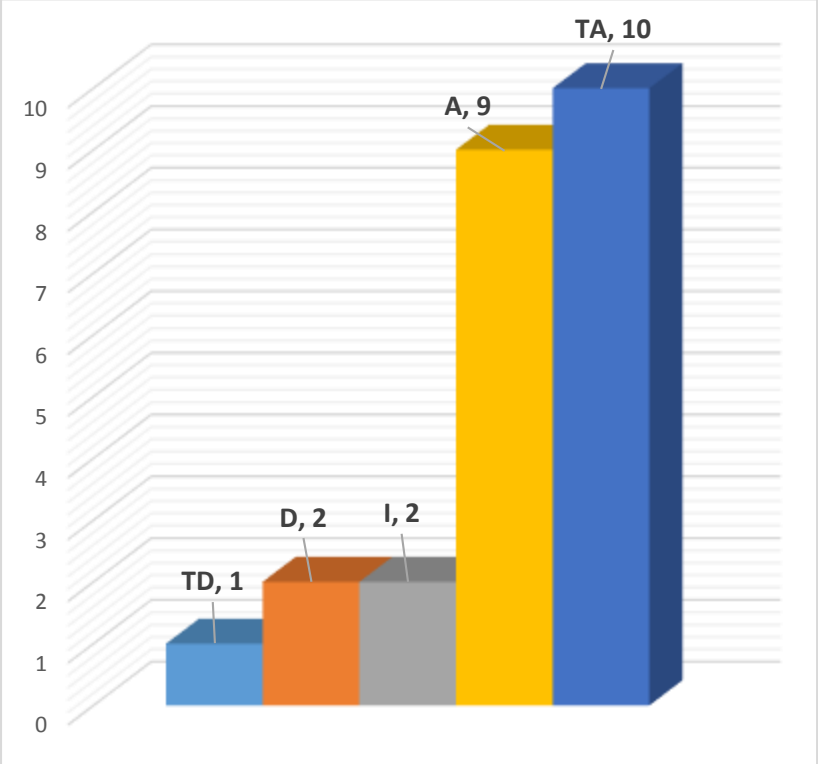


Figura 47. Necesidad de normar el intercambio de información entre los usuarios de la red

Fuente: Elaboración propia

Del 100% de los empleados administrativos encuestados en la entidad, la gran mayoría (79%) considera necesario que el intercambio de información entre los usuarios de la red telemática debería estar normado por protocolos de seguridad.

2.3. Marco conceptual

a. **Autenticación. -** Situación en la cual se puede verificar que un documento ha sido elaborado o pertenece a quien el documento dice.

b. **Cifrado asimétrico. -** Es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella.

c. **Cifrado simétrico. -** Es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes en el emisor y el receptor. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

d. **Confidencialidad. -** Cualidad que debe poseer un documento o archivo para que este solo se entienda de manera comprensible o sea leído por la persona o sistema que ese autorizado

e. **Disponibilidad. -** Capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando éstos lo requieran.

f. **Integridad. -** Cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

g. **IPSec. -** Internet Protocol Security, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando

y/o cifrando cada paquete IP en un flujo de datos. IPSec también incluye protocolos para el establecimiento de claves de cifrado. IPSec está implementado por un conjunto de protocolos criptográficos para asegurar el flujo de paquetes, garantizar la autenticación mutua y establecer parámetros criptográficos.

h. L2TP. - Layer 2 Tunneling Protocol, es un protocolo utilizado por redes privadas virtuales que fue diseñado por un grupo de trabajo de IETF. L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete de datos, incluyendo X.25, Frame Relay y ATM. Al utilizar PPP para el establecimiento telefónico de enlaces, L2TP incluye los mecanismos de autenticación de PPP, PAP y CHAP. De forma similar a PPTP, soporta la utilización de estos protocolos de autenticación, como RADIUS.

i. Metodología adaptativa. - Serie de métodos y técnicas de rigor científico que se aplican de acuerdo al contexto y en función de la información que se disponga en cada momento, e ir adaptando la secuencia de pasos conforme se vaya desarrollando la investigación o proyecto.

j. Metodología. - Serie de métodos y técnicas de rigor científico que se aplican sistemáticamente durante un proceso de investigación para alcanzar un resultado teóricamente válido. En este sentido, la metodología funciona como el soporte conceptual que rige la manera en que aplicamos los procedimientos en una investigación.

k. **Modelo de seguridad. -** Es la expresión formal de una política de seguridad y se utiliza como directriz para evaluar los sistemas de información.

l. **Modelo. -** Un modelo es una abstracción teórica del mundo real que tiene dos utilidades fundamentales: Reducir la complejidad, permitiéndonos ver las características importantes que están detrás de un proceso, ignorando detalles de menor importancia que harían el análisis innecesariamente laborioso; es decir, permitiéndonos ver el bosque a pesar del detalle de los árboles. Hacer predicciones concretas, que se puedan falsar mediante experimentos u observaciones.

m. **PPTP. -** Point-To-Point Tunneling Protocol, permite el intercambio seguro de datos de un cliente a un servidor formando una Red Privada Virtual (VPN), basado en una red de trabajo vía TCP/IP. El punto fuerte del PPTP es su habilidad para proveer en la demanda, multi-protocolo soporte existiendo una infraestructura de área de trabajo, como Internet.

n. **Protocolo de comunicaciones. -** Es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores.

o. **Protocolos de seguridad informática. -** Se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican. Un protocolo de seguridad informática define las reglas que gobiernan estas

comunicaciones, diseñadas para que el sistema pueda garantizar el correcto intercambio de información.

p. **Red privada virtual de acceso remoto. -** Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

q. **Red privada virtual de sitio a sitio. -** Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales.

r. **Red privada virtual. -** Una red privada virtual (VPN) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

s. **Seguridad informática. -** Consiste en aquellas prácticas que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida. También se puede definir como una disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

t. **Seguridad. -** Ciencia interdisciplinaria que está encargada de evaluar, estudiar y gestionar los riesgos que se encuentra sometido una persona, un bien o el ambiente.

Conclusiones parciales

- Se justificó el problema de investigación en lograr el proceso de seguridad informática y su dinámica en redes privadas virtuales en el contexto mundial, nacional y local, considerando las causas que originan el mismo, tomando como base las deficiencias en el intercambio de información académica contextualizada que en la dinámica del proceso de seguridad informática se suscitan en redes privadas virtuales.
- Se procedió a la caracterización del estado actual del proceso de seguridad informática y su dinámica en redes privadas virtuales; usándose para realizar el diagnostico diferentes técnicas e instrumentos de recolección de datos que corroboran las deficiencias en el intercambio de información académica contextualizada entre la Universidad Nacional Pedro Ruiz Gallo y el Centro Pre Universitario de la entidad.

CAPÍTULO 3. HIPÓTESIS Y DISEÑO DE LA EJECUCIÓN

Introducción

En este capítulo se aborda la hipótesis de la presente investigación y que puede definirse como explicaciones tentativas del fenómeno investigado la cual es formulada a través de una proposición cuya veracidad es provisionalmente asumida como solución para dar respuesta al problema de investigación. Así mismo esta investigación es del tipo cuantitativa-explicativa y el diseño de contrastación de la hipótesis es cuasiexperimental. Se hará mención de los métodos analítico, inductivo, histórico, sistémico, funcional y holístico; en donde se ha triangulado las técnicas para la recolección de datos como son; la encuesta, la observación y la entrevista.

Por último, con respecto a la selección de la muestra cabe indicar que el universo al ser significativamente pequeño por ende la muestra también lo será, la cual está conformada por los trabajadores administrativos de las áreas académicas tanto de la Universidad Nacional Pedro Ruiz Gallo como del centro pre universitario.

3.1. Definición de la hipótesis

La hipótesis que asume la investigación y se contrasta se define como: Si se elabora una metodología adaptativa basada en un modelo de seguridad informática para redes privadas virtuales que tenga en cuenta la lógica de integración del proceso de seguridad informática y la lógica funcional de las políticas de seguridad de la organización, entonces se contribuye al mejoramiento del intercambio de información académica contextualizada en entornos de conexiones públicas.

3.2. Determinación y conceptualización de las variables de la hipótesis

Variable independiente: Modelo de seguridad informática para redes privadas virtuales y su metodología adaptativa.

- **Definición conceptual:** Si se toma el concepto de *planificación adaptativa*, implica sencillamente hacer hasta donde tenga sentido planificar, siempre en función de la información que se disponga en cada momento, e ir adaptando la secuencia de pasos conforme el proyecto se va desarrollando, basándose siempre en las experiencias e informaciones útiles y relevantes que se recogieron durante la ejecución. Esto permitirá, de forma clara y objetiva, que se tomen las mejores decisiones para alcanzar el resultado deseado con el mayor grado de efectividad posible. Planificar de forma adaptativa es planificar de forma natural, revisando tanto como el proyecto lo requiera (Masiá, 2015).

Variable dependiente: Intercambio de información académica contextualizada.

- **Definición conceptual:** El intercambio de información académica contextualizada se corresponde con el proceso de proteger la confidencialidad, integridad y disponibilidad de la información, como: matricula de alumnos, listado de alumnos, reporte de pagos, resultados de exámenes, boleta de notas, asistencia a clases, horario docente, entre otros; basado en un contexto académico.

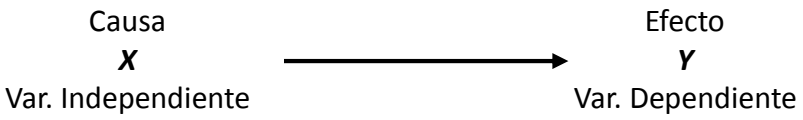
3.3. Diseño de la ejecución

3.3.1. Métodos de investigación científica y selección de técnicas, instrumentos, fuentes de verificación

a. Tipo de estudio y diseño de contrastación de hipótesis

El tipo de investigación es **cuantitativa – explicativa**, dado que está dirigida a responder por las causas de los eventos y fenómenos físicos o sociales (Hernández, Fernández, & Baptista, 2014). Su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta o por qué se relacionan dos o más variables. Es decir, que haya claridad entre los elementos de la investigación que conforman el problema, que sea posible definirlo, limitarlos y saber exactamente dónde se inicia este.

El diseño de contrastación de hipótesis es **cuasiexperimental**, debido a que su resultado recae en una aplicación parcial de la investigación, en donde se manipulará la variable independiente para observar su efecto sobre la variable dependiente (Hernández, Fernández, & Baptista, 2014).



b. Métodos, técnicas e instrumentos de recolección de datos

Entre los **métodos teóricos** de investigación que se utilizarán para analizar, fundamentar y corroborar el proceso de seguridad informática, tenemos los siguientes:

- Método histórico – lógico; para la caracterización de los antecedentes teóricos e históricas en las que se fundamenta el proceso de seguridad informática.
- Método analítico – sintético; para realizar el diagnostico, seleccionar el problema, así como darle solución al mismo.
- Método inductivo – deductivo; para establecer la hipótesis, determinar el campo y objeto de la investigación.
- Método holístico – sistémico; para fundamentar las interrelaciones que se dan en el aporte teórico.
- Método de sistematización; para elaborar, fundamentar y aplicar las fases de la metodología para redes privadas virtuales.
- Método empírico, para la caracterización del estado actual del intercambio de información académica contextualizada de la Universidad Nacional Pedro Ruiz Gallo.

También se tienen los métodos empíricos utilizados para demostrar las deficiencias en el intercambio de información académica contextualizada entre la Universidad Nacional Pedro Ruiz Gallo y el Centro Pre Universitario de la entidad:

- **Encuesta** a los especialistas de la Oficina General de Sistemas Informáticos de la Universidad para conocer los aspectos técnicos, la forma de establecer políticas y protocolos de seguridad informática para la entidad.
- **Encuesta** a los empleados administrativos de la Universidad para conocer la percepción que tienen con respecto a la seguridad informática durante el proceso de intercambio de información.

- **Observación** de lo que ocurre en las áreas relacionadas con la población, así como en la Red Telemática de la Universidad con respecto a las aplicación y cumplimiento de las políticas de seguridad informática.
- **Análisis documental** para recabar información del proceso de seguridad informática y sus tendencias históricas, la justificación de problema y la situación actual de la red informática de la Universidad.

Los instrumentos de recolección de datos, que utilizadas en la presente investigación son: el cuestionario, la ficha de observación y la entrevista.

3.3.2. Universo

El universo se compone del conjunto de elementos que tienen características en común, apreciable y susceptible a ser medidos, por esta razón se define el universo para la presente investigación como el conjunto de empleados, especialistas y directivos de la Oficina General de Sistemas Informáticos, Oficina General de Admisión y Oficina de Asuntos Académicos de la Universidad Nacional Pedro Ruiz Gallo y del área Académica del Centro Pre Universitario; haciendo un total de 32 empleados, dado que ellos son los responsables del intercambio de información académica entre la Universidad y el Centro Pre Universitario.

3.3.3. Selección de la muestra

La muestra, se compone de una o varias de las características de los elementos del universo definido y sobre las cuales se pueden realizar mediciones u observaciones; de esta manera, al contar con un universo

pequeño, se tomará como muestra el mismo valor de la población la cual igual a 32 empleados.

3.3.4. Forma de tratamiento de los datos

La información recolectada a través de los instrumentos, será validada a través del método de consistencia interna (Alfa de Cronbach), luego codificada, seguidamente se ingresará y por último se tabulará para el análisis de los datos, haciendo uso del programa estadístico SPSS y del libro electrónico Microsoft Excel. Los resultados de este análisis serán presentados a través gráficos y tablas estadísticas, así como la interpretación de los resultados tomando como base los indicadores y variables que se medirán.

Conclusiones parciales

- Se definió la hipótesis de la investigación, y se determinaron la variable independiente (modelo de seguridad informática para redes privadas virtuales y su metodología adaptativa), y la variable dependiente (intercambio de información académica contextualizada), el modelo de seguridad informática para redes privadas virtuales y su metodología adaptativa e Intercambio de información académica contextualizada, respectivamente; en las cuales se emplearon los métodos teóricos y empíricos de la investigación.
- Se precisaron indicadores y dimensiones de análisis, lo que posibilito la recolección de datos e información necesaria para triangular la información a través de técnicas de recolección de datos y métodos estadísticos empleados, utilizando procesador estadístico SSPS para el análisis de los datos e información los que se plasmaron en tablas de Microsoft Excel.

- Finalmente se puede precisar que la variable dependiente (intercambio de información académica contextualizada) a través de sus indicadores: tipos de usuarios, requerimientos y servicios de red y topología de red pasarán de un estado actual a un estado proyectado obteniendo un estado diferenciado, lo cual permitirá que la variable cambie significativamente.

SEGUNDA PARTE

CONSTRUCCIÓN DE LOS APORTES

CAPÍTULO 4. ELABORACIÓN DE UN MODELO DE SEGURIDAD INFORMÁTICA EN REDES PRIVADAS VIRTUALES

Introducción

En este capítulo se fundamenta y explica la construcción epistemológica del proceso de seguridad informática para redes privadas virtuales. Se establece la posición teórica del investigador y se fundamentas los aportes que en este aspecto se realizan. Este modelo se materializa en las interrelaciones que se producen entre los usuarios a través de servicios los cuales interactúan intercambiando información académica contextualizada sobre una red privada virtual.

Se organiza en dos epígrafes; en el primero se fundamenta el modelo, en el segundo se realiza la descripción argumentativa del modelo y por último se enuncian las conclusiones parciales del capítulo.

4.1. Fundamentación del aporte teórico

En la modelación del proceso de seguridad informática para redes privadas virtuales que se realiza en la presente investigación, se constituyen en el orden epistemológico de la concepción sistémica la cual según Bertalanffy (1979), creador de la Teoría General de Sistemas, los sistemas pueden ser abiertos o cerrados, funcionan como un todo, presentan la propiedad de circularidad (debido a la interconexión entre los elementos, la causalidad es circular en vez de lineal) y la equifinalidad (una misma causa puede tener diferentes efectos); constituye el apartado teórico esencial, que desde el punto de vista epistemológico permite comprender e interpretar los resultados del modelo a partir de la determinación de sus dimensiones, partiendo de las componentes y las relaciones que se establecen entre ellas, orientada a la seguridad informática en redes privadas virtuales y el intercambio de información que se producen sobre estas.

Este intercambio de información es realizado teniendo como soporte la red privada virtual de sitio a sitio para ello se establece un modelo de seguridad informática para redes privadas virtuales que tenga en cuenta la relación entre la lógica de integración del proceso de seguridad informática, la lógica funcional de los protocolos de encapsulamiento de datos y las políticas de seguridad de la Universidad Nacional Pedro Ruiz Gallo.

> Como fundamentos teóricos se han seleccionado lo referido a las Normas ISO/IEC 27011-2008, cuyo objetivo es definir unas directrices de apoyo a la aplicación de la gestión de la seguridad de la información en las organizaciones de telecomunicaciones. La adopción de esta norma internacional permitirá a las organizaciones de telecomunicaciones definir una línea base para satisfacer las necesidades de gestión de la seguridad de la información en términos de confidencialidad, integridad, disponibilidad y cualquier otra dimensión pertinente de la seguridad. (Fernández & Piattini, 2012, p. 87).

4.2. Descripción argumentativa del aporte teórico

En la presente investigación se realiza la modelación del proceso de seguridad informática en redes privadas virtuales con un enfoque científico y sistémico, que tiene como intencionalidad el envío seguro de información académica contextualizada.

Las relaciones comprometidas con este modelo, sustentan la elaboración de la metodología adaptativa, que tiene en cuenta la relación entre la dimensión de gestión de conectividad de la red y la dimensión de gestión de seguridad informática.

La **dimensión de gestión de conectividad de la red,** detalla de manera general los aspectos que se necesitan para la puesta en marcha de la red privada virtual, teniendo en cuenta que la misma incluye aplicaciones de software cliente / servidor, aplicaciones móviles, aplicaciones de escritorio entres otras necesarias para la transmisión y recepción de datos, teniendo como soporte las redes LAN/WAN y los servidores de la organización, los cuales permiten prestar servicios entre diferentes sitios, locales o remotos (véase figura 48).

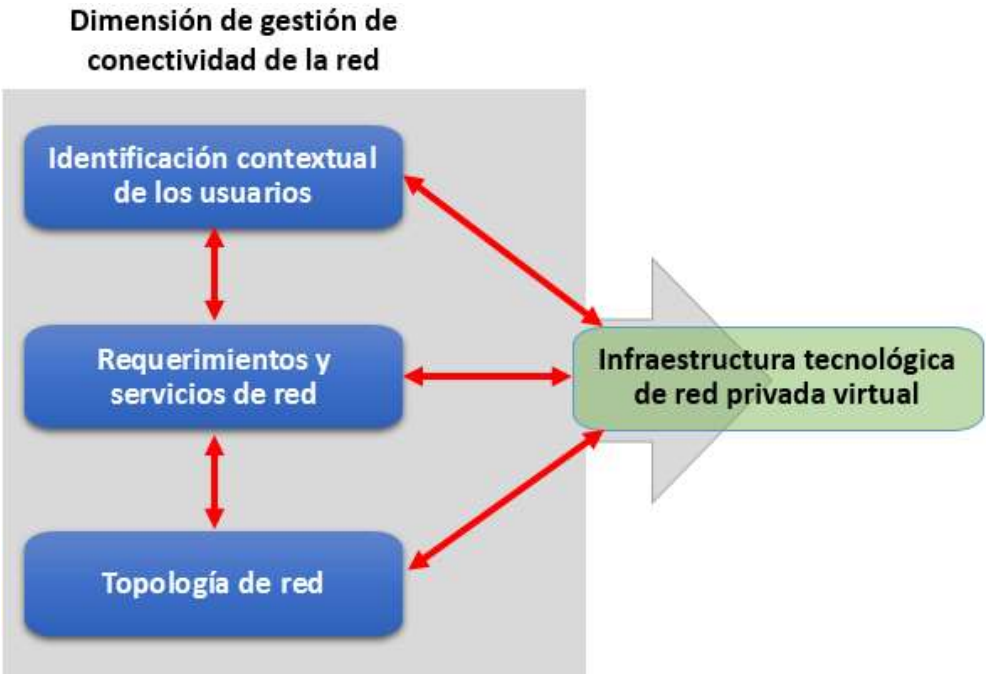


Figura 48. Dimensión de gestión de conectividad de la red

Como punto de partida en necesario realizar la **identificación contextual de los usuarios,** es importante conocer cuál es la importancia de los **usuarios** y el rol que desempeña en una red informática.

> Un **usuario** es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema, además se utiliza para clasificar a diferentes privilegios, permisos a los que tiene acceso un usuario o grupo de usuario, para interactuar o ejecutar con el ordenador o con los programas instalados

> en este. En sentido general, un usuario es el conjunto de privilegios, permisos, recursos o dispositivos, a los cuales se tiene acceso. Es decir, un usuario puede ser tanto una persona como una máquina, un programa, etc. (EcuRed, 2018)

Cabe indicar que, en este contexto, también llamaremos usuarios a las personas con capacidad de decisión y conocimiento de la organización, y también al personal encargado del diseño, implementación, administración y mantenimiento de la red privada virtual.

Dentro de la identificación contextual de los usuarios, también es importante mencionar a los stakeholder.

> Un **stakehokder** es un individuo, grupo u organización que puede afectar, verse afectado, o percibirse a sí mismo como afectado por una decisión, actividad o resultado de un proyecto. Los stakeholder pueden participar activamente en el proyecto o tener intereses a los que puede afectar positiva o negativamente la ejecución o la terminación del proyecto. (PMBOOK, 2013, p. 30)

El análisis de una red informática se enfoca en dos propósitos en primer lugar conocer y escuchar a los usuarios, en segundo lugar, entender las necesidades de estos y de la infraestructura informática. **Los requerimientos de red** o la especificación de estos no es una tarea fácil de llevar a cabo, se necesita de mucha dedicación, concentración y análisis para poder determinar de la mejor manera cada uno de ellos con lo cual incrementará las probabilidades de acierto en las etapas de diseño e implementación de la red.

Los requerimientos de usuario pueden ser expresados en términos de servicios requeridos de red, volumen de tráfico o ancho de banda, capacidad de almacenamiento, disponibilidad de los recursos, entre otros. No es suficiente

preguntar al usuario que es lo que quiere o que es lo que necesita ya que podrían estar dudosos de lo que en el futuro una red informática requerirá, más por el contrario podrían tener una idea exigua de lo que puede o no lograrse desde el punto de vista tecnológico. Entrevistarse con el personal de todos los niveles de la organización ayudará a tener un panorama completo lo cual contribuirá a asegurar que los requerimientos sean específicos.

Para que el trabajo de una red informática empresarial sea efectivo, es necesario implementar una serie de **servicios** de tal manera que los usuarios contribuyen a lograr un mejor desempeño laboral dentro de la organización. Los servicios y los servidores de red se basan en los sistemas operativos de red. Un sistema operativo de red es un conjunto de programas que permiten, controlan y administran el uso de los dispositivos de red por uno o más usuarios.

Los servicios requeridos para una red privada virtual de seguro incluirán servicios de voz IP, servicio de cloud computing, servicio de autenticación de usuarios y acceso remoto, servicio de contenido de correo y web, entre otros. Otros servicios requeridos podría ser aplicaciones de teletrabajo o trabajo a distancia, video conferencias. Estos servicios inevitablemente tienen gran impacto en los requerimientos de ancho de banda y tráficos de datos.

La topología de red es una parte fundamental dentro del esquema de implementación de una red privada virtual ya que con ésta se puede proporcionar un mapa visual que representa como está conectada la red. En función de su alcance y propósito, la topología de red puede contener muchos detalles o solo brindar un panorama amplio. Por ejemplo, un diagrama de una LAN podría mostrar la dirección IP de computadoras individuales, mientras que el diagrama de una VPN podría representar un túnel, entre dos sitios central y remoto. La topología de red

está dividida en dos tipos. El **diseño de red lógico** o **topología lógica**, describe la forma en que la información fluye a través de una red. Así, los diseños de red lógicos, por lo general, muestran subredes (incluidas direcciones, máscaras e ID de VLAN, ID de túneles para VPN), dispositivos de red, como enrutadores y cortafuegos, y protocolos de enrutamiento. Mientras que un **diseño de red físico** o **topología física**, muestra la disposición física real de los componentes que forman la red, incluidos cables y hardware. Por lo general, el diseño ofrece una vista panorámica de la red en su espacio físico, como un plano de planta (Lucidchart, 2015).

El objetivo de una red informática es intercambiar información de manera rápida y segura, sin importar la distancia. Para poder esto, se precisa dotar de una **infraestructura tecnológica de red privada virtual** adecuada. Los **sitios**, conformadas por organizaciones, empresas, entidades, oficinas u otros edificios los cuales intercambiar información de manera segura, confiable y rápida sobre una red pública o no controlada como Internet. Cada **sitio** está constituido por una **Red de Área Local (LAN)** que vienen a ser las redes internas de las organizaciones, es decir las conexiones entre los equipos de una organización particular. Estas redes se conectan cada vez con más frecuencia a Internet mediante un equipo de interconexión. Muchas veces, las empresas necesitan comunicarse por Internet con filiales, clientes o incluso con el personal que puede estar alejado geográficamente. Sin embargo, los datos transmitidos a través de Internet son mucho más vulnerables que cuando viajan por una red interna de la organización, ya que la ruta tomada no está definida por anticipado, lo que significa que los datos deben atravesar una infraestructura de red pública que pertenece a distintas entidades. Por esta razón, es posible que, a lo largo de la línea, un usuario entrometido "escuche" la red o incluso

"secuestre" la señal. Por lo tanto, la información confidencial de una organización o empresa no debe ser enviada bajo tales condiciones.

La primera solución para satisfacer esta necesidad de comunicación segura implica conectar redes remotas mediante líneas dedicadas o líneas arrendadas. Sin embargo, como la mayoría de las organizaciones no pueden conectar dos redes de área local remotas con una línea dedicada, por su elevado costo, a veces es necesario usar Internet como medio de transmisión.

Una buena solución consiste en utilizar Internet como medio de transmisión con un protocolo de túnel, que significa que los datos se encapsulan antes de ser enviados de manera cifrada.

En cuanto a la **dimensión de gestión de seguridad informática**, constituye el núcleo central para la creación, mantenimiento, actualización, protección e intercambio de información entre los sitios de la organización, haciendo uso de una correcta **infraestructura tecnológica de red privada virtual** (véase figura 49).

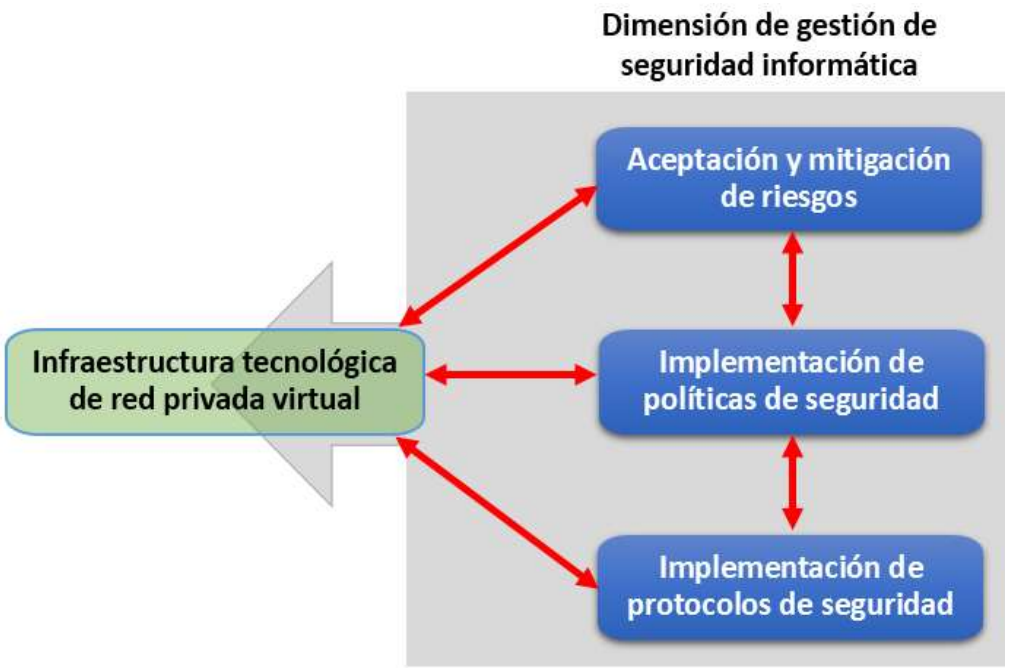


Figura 49. Dimensión de gestión de seguridad informática

El término información es cada vez más ubicuo y lo mismo ha sucedido con las tecnologías de la información que lo procesan. La información se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma ya texto, gráfico, audio, video y en cualquier medio, ya sea magnético, papel, audiovisual u otro. Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para la entidad u organización.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y, por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Es a través de la red privada virtual que se establece el intercambio de información, entiéndase como tal, ordenada, procesada, integra y oportuna, la cual será compartida entre los sitios de la organización.

La seguridad total no existe, lograrla resulta casi imposible, debido a su alto costo económico como a la casi nula posibilidad de conocer y evitar a tiempo todas las posibles amenazas existentes, más aún al intercambiar información entre sitios remotos de una organización, a través de una red privada virtual, sobre la red

pública Internet, lo que conlleva a que se asuman se **acepten y se mitiguen los riesgos**. La gestión del riesgo se define como:

> "Acciones coordinadas para dirigir y controlar una organización respecto a los riesgos". La gestión del riesgo incluye otras acciones, como análisis, estimación, aceptación, evaluación, tratamiento, comunicación, monitorización y revisión del riesgo.
>
> Las definiciones más actuales para estas acciones podemos encontrarlas tanto en la ISO/IEC 27000:2009, como en el informe UNE-ISO Guía 73:2010 IN. Las más destacadas son:
>
> - **Análisis del riesgo:** utilización sistemática de informaciones para identificar las fuentes y estimar el riesgo.
> - **Estimación del riesgo:** actividad para asignar valores a la probabilidad y consecuencias de un riesgo.
> - **Criterios del riesgo:** términos de referencia contra los que la significación de un riesgo es evaluada. Pueden comprender costes y ventajas, requisitos legales y reglamentarios, aspectos socioeconómicos y del entorno, consideraciones de las partes implicadas (stakeholder), prioridades del negocio, etc.
> - **Aceptación del riesgo:** decisión de aceptar un riesgo.
> - **Evaluación del riesgo:** proceso de comparación del riesgo estimado contra los criterios de aceptación para determinar la importancia o significación del riesgo.
> - **Tratamiento del riesgo:** proceso de selección e implementación de medidas para modificar el riesgo. (Fernández & Piattini, 2012, p. 101).

La información es un recurso y un activo muy valioso para toda organización y por consiguiente debe ser debidamente protegida; en ese sentido se tiene que **implementar políticas de seguridad**.

Una **política de seguridad de la información** es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, empresa u organización teniendo como fin primordial proteger información y recursos, garantizando los servicios de la misma. Las políticas son guías para asegurar la protección y la integridad de los datos dentro de los sistemas de información, redes informáticas, instalaciones de cómputo y procedimientos manuales.

Las políticas tienen como objetivo proteger los recursos de información de la entidad u organización y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, intencionadas o accidentales, con el fin de garantizar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confidencialidad de la información.

Así mismo el alcance las políticas se aplica a todo el ámbito de la entidad u organización, a sus recursos y a la totalidad de los procesos que en esta se desarrollan.

La responsabilidad de las políticas recae en todos los directivos, gerentes, jefes y personal subordinado los cuales son los encargados de implementar las políticas de seguridad de la información y dentro de las áreas de gestión u dirigencia, así como del cumplimiento de dichas políticas por parte de su equipo de trabajo.

Como principal activo – la información – de toda organización, estos deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función

a ello, con el objeto de indicar y determinar cómo ha de ser tratada y protegida dicha información.

Mientras que las políticas de seguridad permiten el uso correcto y eficiente de la información, los protocolos garantizan el envío seguro de esta. La **implementación de protocolos de seguridad** para una red privada virtual recae en los protocolos túnel, que permiten cifrar y encapsular los paquetes de datos enviados a través de la red pública. Gracias al encapsulamiento de los datos es posible trabajar con un gran número de protocolos diferentes los cuales se pueden encontrar tanto en la red pública del proveedor como en la red LAN de la organización. Entre los protocolos utilizados para el tunneling se tiene al protocolo GRE y al marco de protocolos IPsec.

El protocolo de encapsulación de routing genérico **GRE**, es considerado un protocolo de encapsulamiento para una VPN de sitio a sitio básico y poco seguro. Su condición de básico y no seguro lo hace un protocolo encapsulado no recomendado para la implementación en redes VPN de sitio a sitio.

En contraparte, el marco de protocolos de seguridad de Internet **IPsec**, ofrece a las VPN conectividad flexible y escalable. IPsec es un marco de estándares abiertos que describe las condiciones para establecer comunicaciones seguras. IPsec no se limita a ningún tipo de cifrado, autenticación, algoritmo de seguridad, ni tecnología de creación de claves. Más, por el contrario, IPsec depende de una serie de algoritmos existentes para implementar comunicaciones seguras.

Para el envío de información segura, IPsec proporciona cuatro funciones primordiales: (Cisco Networking Academy, 2014)

- **Confidencialidad (cifrado):** antes de transmitir los datos a través de la red VPN, estos se deben cifrar. IPsec garantiza la confidencialidad, dado que

proporciona características de seguridad mejoradas, como algoritmos de cifrado seguro. Algoritmos DES, 3DES, AES, RSA, SEAL

- **Integridad de datos:** IPsec garantiza que los datos transmitidos por la VPN, hayan viajado sin ningún tipo de modificación o alteración. Si se detectara alguna alteración el paquete es descartado. Algoritmos DH, MD5, HASH
- **Autenticación:** IPsec utiliza el intercambio de claves de Internet (IKE) para autenticar usuarios y dispositivos que pueden llevar a cabo la comunicación a través de la VPN, de tal manera que se verifique la identidad del origen de los datos y por consiguiente al receptor de estos. Algoritmos PSK, Firmas RSA
- **Protección antirreproduccion:** IPsec tiene la capacidad de detectar y rechazar los paquetes de información duplicados así mismo previene la suplantación de identidad. Los paquetes duplicados y con un tiempo de retardo se rechazan.

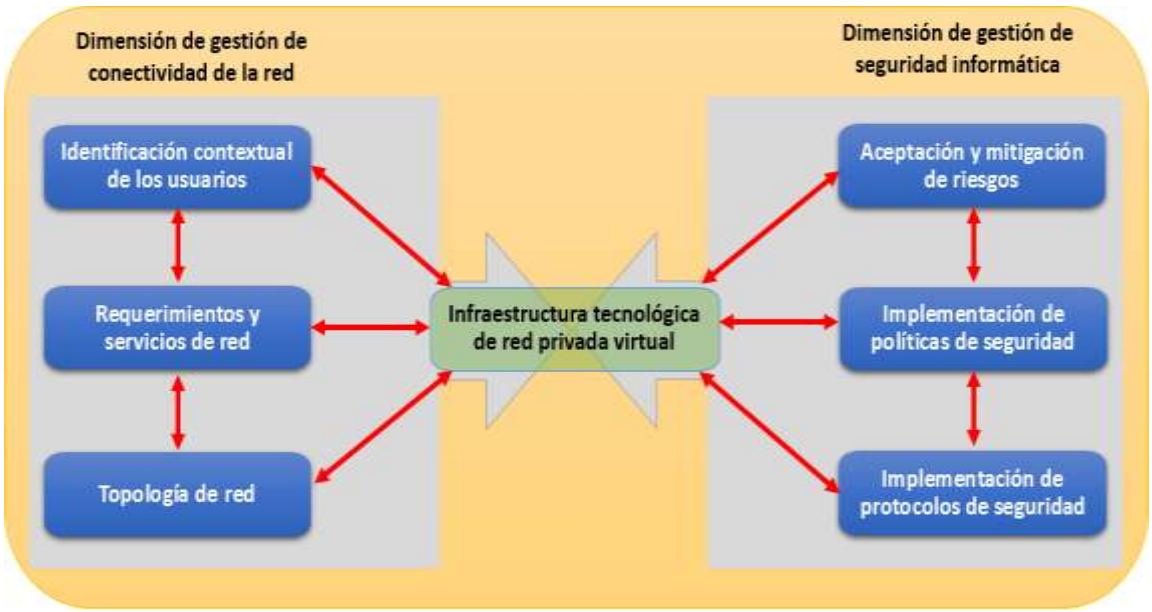


Figura 50. Modelo de seguridad informática en redes privadas virtuales

La modelación de seguridad informática en redes privadas virtuales se sustenta en el eje de la conectividad de la red y el eje se seguridad informática los cuales contribuyen al diseño y posterior implementación de la infraestructura tecnológica de red privada virtual, que sea segura, escalable, de fácil acceso a los recursos de la red y sobre todo garantizando la integridad, confidencialidad y seguridad de los datos (véase figura 50).

Conclusiones parciales

- El modelo de seguridad informática en redes privadas virtuales en entornos de conexiones públicas se sustenta en la teoría general de sistemas de Bertalanffy (1979), la cual se estructura a través de dos dimensiones; la gestión de conectividad de la red y de gestión de seguridad informática.
- La primera dimensión tiene como punto de partida la interrelación entre la identificación contextual de usuarios, los requerimientos y servicios de red y la topología de red; a su vez la segunda dimensión relaciona la aceptación y mitigación de riesgos, la implementación de políticas de seguridad y la implementación de los protocolos de seguridad, en donde ambas dimensiones contribuyen a lograr una infraestructura de tecnológica de red privada virtual.

CAPÍTULO 5. ELABORACIÓN DE UNA METODOLOGÍA ADAPTATIVA PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD INFORMÁTICA EN REDES PRIVADAS VIRTUALES

Introducción

En este capítulo se fundamenta y explica la metodología adaptativa para la implementación del modelo de seguridad informática en redes privadas virtuales, estableciendo dos subsistemas, expresados en tres etapas de la metodología que relacionan la gestión de conectividad de la red, la gestión de seguridad informática y el seguimiento y control. En la metodología se determinan siete momentos para su ejecución los cuales constituyen un conjunto de actividades que integran las principales componentes y dimensiones de modelo teórico propuesto.

5.1. Relación entre aporte teórico y aporte práctico

El proceso de seguridad informática a través del intercambio de información académica contextualizada en entornos de conexiones públicas en la Universidad Nacional Pedro Ruiz Gallo, posibilitó realizar una construcción teórica de este proceso, utilizando la teoría general de sistemas de Bertalanffy, que se concreta en la fundamentación del aporte práctico metodología adaptativa para la implementación del modelo de seguridad informática en redes privadas virtuales, la cual se concibe por etapas, objetivos y tareas las mismas que se desarrollarán teniendo en cuenta los requerimientos del negocio, para alcanzar finalmente los objetivos comprometidos en el intercambio de información académica de manera segura y confiable.

5.2. Construcción del aporte práctico

La metodología adaptativa para redes privadas virtuales que se plantea, deviene de una alternativa que permite guiar a los grupos de interés (directivos, funcionarios, y personal de TI) en la gestión del proceso de seguridad informática para el intercambio de información académica contextualizada en entornos de conexiones públicas, a través de tareas y acciones que contribuyan a mejorar este proceso. Es así que, la lógica entre el aseguramiento de la información en redes privadas virtuales, como resultado de la relación que se establece entre la gestión de conectividad de la red y la gestión de seguridad informática. Este planteamiento permite ofrecer de manera metodológica y sistematizada la implementación de una red privada virtual para garantizar el intercambio de información académica contextualizada en entornos públicos de manera segura y confiable.

Para su elaboración se partió del modelo de seguridad informática en redes privadas virtuales el cual está directamente relacionado con la sistematización de información o datos y con la sistematización de experiencias. El primero se refiere al ordenamiento y la clasificación de datos e información y el segundo a procesos que se desarrollan en un periodo determinado, en un contexto económico-social y dentro de una institución dada (Rodríguez & Pérez, 2017).

De esta manera la estructura general de la metodología, tiene en cuenta los siguientes aspectos:

- Fundamentación
- Diagnóstico
- Objetivo General
- Etapas

- Objetivos Específicos
- Acciones

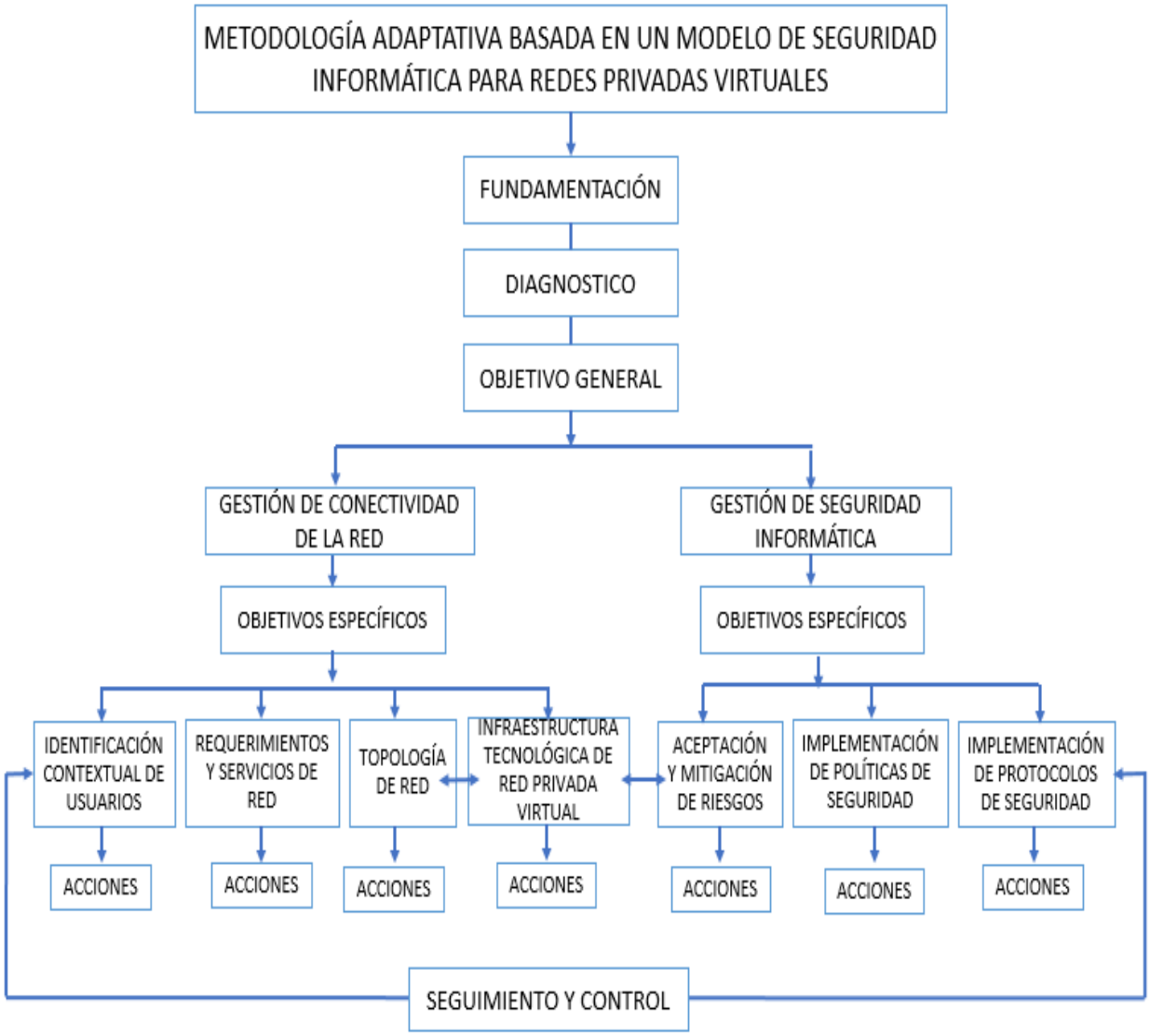


Figura 51. Diseño de la Metodología para redes privadas virtuales

A. Fundamentación

El arma más poderosa que posee el ser humano es la información, en igual proporción, pero en mayor significancia lo es para una empresa u organización, ya que le permite a esta; conocer, predecir, manipular, sobrevivir y, en definitiva, estar un paso por delante con respecto a quien no dispone de ella.

Por esta razón, uno de sus principales objetivos no sólo es poseer la información, sino tener también la capacidad de salvaguardarla de manera segura, es decir, que únicamente permanezca accesible para aquellos interesados o usuarios autorizados.

Garantizar la información antes y durante el envío, pasa por implementar protocolos de encapsulación seguros, establecer políticas de seguridad, conocer los riesgos a los que nos enfrentamos, y es aquí donde toma importancia la implementación de una red privada virtual, ya que como se mencionó en los capítulos anteriores, una VPN utiliza Internet como medio de transmisión de datos, lo que permite un considerable ahorro en términos económicos al reducir los costos de conectividad y, al mismo tiempo, aumentar el ancho de banda de la conexión remota; así mismo las VPN pueden incluir mecanismos de seguridad mediante protocolos de cifrado y autenticación avanzados que protegen los datos contra el acceso no autorizado.

La metodología a plantear que a continuación se va a describir ha sido realizada tomando como experiencia la institución de educación superior Universidad Nacional Pedro Ruiz Gallo y tiene como objetivo ayudar al entendimiento y mejor manejo de la teoría y la práctica en el desarrollo de redes privadas virtuales.

B. Diagnostico

La metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales, admite tener en consideración los documentos normativos relacionados a las políticas de seguridad y los resultados de los instrumentos aplicados al colectivo de empleados especialistas en TI y

empleados administrativos de la Universidad Nacional Pedro Ruiz Gallo de Lambayeque, donde se logró evidenciar el desconocimiento de las políticas y protocolos de seguridad de la información así como las deficiencias para el intercambio de información académica contextualizada entre las Oficinas académicas de la Universidad y el Área académica del Centro Pre Universitario.

Por su parte los empleados especialistas en TI, también evidencian limitaciones técnicas y logísticas al momento de proponer nuevos proyectos de redes y comunicaciones, así mismo se denota limitaciones de estos especialistas con el buen uso de los recursos de TI por parte de los usuarios de la red telemática de la entidad.

C. Objetivo General

Garantizar el intercambio de información académica contextualizada en entornos de conexiones de redes públicas, sustentada en un modelo sistémico de seguridad informática para redes privadas virtuales.

D. Etapas

ETAPA 1: DIMENSIÓN DE LA GESTIÓN DE CONECTIVIDAD DE LA RED

a. Objetivos Específicos

1. Identificar de manera detallada los diferentes tipos de usuarios y su nivel de compromiso que tienen frente al desarrollo exitoso de la red privada virtual.

2. Describir los servicios a desplegar sobre la red privada virtual a partir de los requerimientos del usuario, teniendo en cuenta el acceso y la disponibilidad de los mismos por parte de los usuarios autorizados.
3. Elaborar los diseños de red físico y lógico a desplegar por la red privada virtual.
4. Detallar los equipos de la infraestructura de red necesarios para implementación de la red privada virtual.

FASE 1: Identificación Contextual de Usuarios

En esta fase se debe identificar a los usuarios involucrados directa e indirectamente con el desarrollo del proyecto para la implementación de la red privada virtual. Entre los usuarios identificados tenemos: Los directivos y líderes de la organización, los especialistas y operadores de la red, los generadores y consumidores de información; así como, los usuarios remotos y usuarios móviles.

a. Acciones

- Identificar los tipos de usuarios (directivo, especialista, operador, generador y consumidor de información) que utilizarán la red privada virtual.
- Determinar el nivel de interés de los usuarios, así como sus expectativas, importancia e influencia en el desarrollo de la red privada virtual.

- Describir el nivel de participación de los usuarios identificando sus necesidades y expectativas para lograr su compromiso durante el desarrollo de la red.
- Establecer un canal de comunicación claro y directo con los usuarios a fin de balancear sus expectativas con los objetivos del proyecto de red privada virtual.

Para la identificación de usuarios nos podemos guiar:

Tabla 25. *Identificación de usuarios*

Rol	Expectativa	Influencia	Tipo de Usuario
1. Jefe de la Red Telemática	Tener una VPN eficiente y segura, que responda a la expectativas del usuario	Alta	Especialista
2. Trabajador Administrativo	Intercambiar información de manera rápida y segura.	Media	Generador y consumidor de información,

Fuente: Elaboración propia

FASE 2: Requerimientos y Servicios de Red

Como parte de los requerimientos, estos deben estar en relación con las expectativas del usuario, el correcto funcionamiento y la puesta en marcha de la red privada virtual. Por su parte, los servicios que correrán sobre la red privada virtual serán aquellos que por su naturaleza se necesitan que estén disponibles para los usuarios de la sede remota, garantizando el acceso a los datos de la organización de manera rápida y oportuna.

a. Acciones

- Utilizar técnicas para la obtención de los requisitos tales como: las entrevistas, el brainstorming, casos de uso o el desarrollo conjunto de aplicaciones (JAD).
- Identificar y analizar la información que ha de ser procesada e intercambiada entre los diferentes sitios de la red privada virtual.
- Identificar las aplicaciones que pasará por la red privada virtual. Por ejemplo, servicio de telefonía, servicio de replicación de base de datos, acceso a los sistemas de información.
- Establecer los niveles de seguridad que se implementará en la red privada virtual. Como la autenticación y la privacidad de los datos; así mismo controlar quien puede acceder a cada uno de los sistemas en cada conexión.

Tabla 26. *Identificación de requerimientos*

Requerimiento	Área usuaria	Descripción	Influencia
1. Conectividad a Internet independiente	Red Telemática	La VPN debe estar conectada por una línea conexión a internet de manera independiente	Alta
2. Red VPN segura y de fácil administración	Red Telemática	Red VPN que permita administrar el tráfico de datos y el tráfico de voz	Alta
3. Enviar y compartir información entre las sedes	Área Académica	Red que permita de manera fácil y segura el intercambio de información entre los sitios de la organización	Alta

Fuente: Elaboración propia

Tabla 27. *Identificación de servicios*

Servicio	Usuarios	Descripción	Tráfico
1. Acceso remoto a la VPN	Usuario remotos	Usuarios que desean acceder remotamente de un sitio central o sucursal y viceversa	Medio
2. Servicio de VoIP	Usuarios remotos y móviles	Usuarios de desean hacer uso del servicio de Telefonía IP de la organización	Alto
3. Autenticación e usuarios	Todos	Determinar los tipos de autenticación de usuarios para conectarse a la red	Alto
4. Acceso a los sistemas de información	Usuarios remotos	Usuarios que acceden desde la sucursal a los sistemas de información de la sede central	Alto

Fuente: Elaboración propia

FASE 3: Topología de Red

Para el diseño de la red privada virtual se debe considerar dos diagramas; el diagrama de topología física y el diagrama de topología lógica. El primero describe la ubicación física de los dispositivos, los puertos y la instalación de los cables. El segundo se encarga de identificar los dispositivos, puertos y esquemas de direccionamiento lógico desde el punto de vista de configuración.

a. Acciones

- Diseñar físicamente la red a través de un diagrama de topología física para redes privadas virtuales
- Diseñar lógicamente la red a través de un diagrama de topología lógica para redes privadas virtuales.

Topología física de la red privada virtual

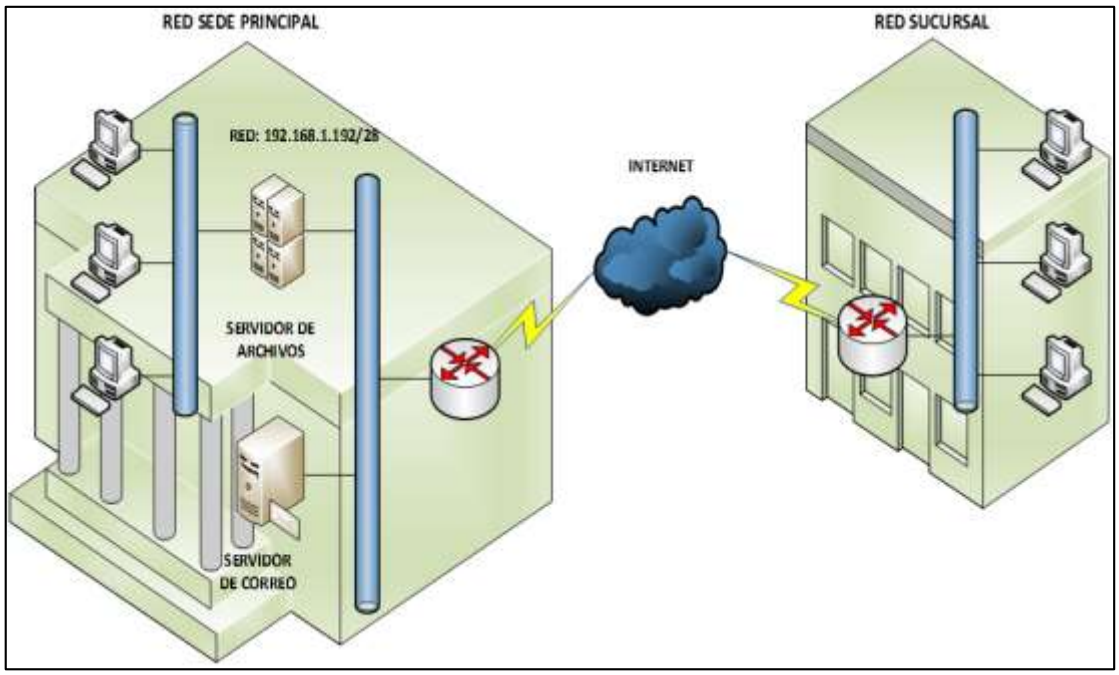


Figura 52. Topología física de la red

Topología lógica de la red privada virtual

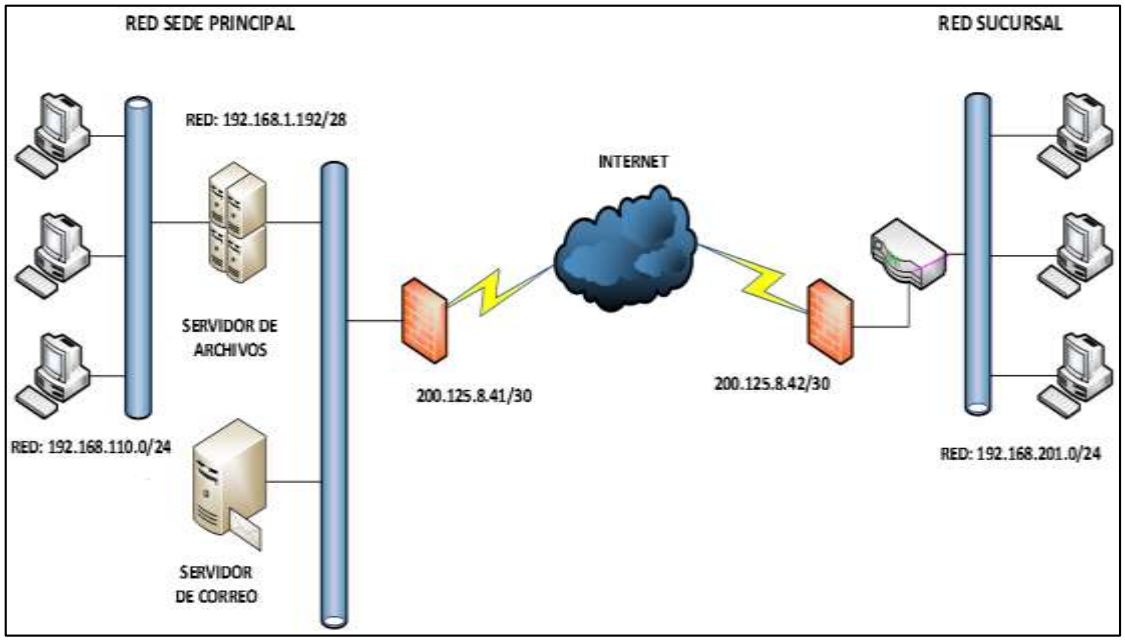


Figura 53. Topología lógica de la red

FASE 4: Infraestructura Tecnológica de la Red Privada

Para nuestra organización e independientemente de la conexión remota que se utiliza para conectarse a las redes de la organización, los usuarios requieren tanto una componentes de oficina doméstica como componentes corporativos (Cisco Networking Academy, 2014).

b. Acciones

- Identificar los componentes de la oficina doméstica, los cuales básicamente son: una computadora portátil o de escritorio o tablet, acceso a internet por banda ancha (ADSL, WIFI o plan de datos) y un software de router o cliente VPN instalado en la computadora, adicionalmente puede necesitarse de un punto de acceso inalámbrico.
- Identificar los componentes corporativos, los cuales están conformados por los routers con capacidad VPN, los concentradores VPN, dispositivos de seguridad multifunción y dispositivos de autenticación y administración central para la agregación y la terminación resistentes de las conexiones VPN (Cisco Networking Academy, 2014).

Tabla 28. *Detalle de equipamiento para la infraestructura tecnológica*

Equipo	Características	Función	Inversión
1. Router	Cisco CISCO1941-SEC/K9 1941 Integrated Services Security Router	Router VPN Sede Central	$ 742.00
2. Firewall	Cisco ASA5506-K9= Network Security Firewall Appliance	Firewall para la VPN sede Central	$276.00

Fuente: Elaboración propia

ETAPA 2: DIMENSIÓN DE LA GESTIÓN DE SEGURIDAD INFORMÁTICA

a. Objetivos Específicos

1. Identificar los riesgos y establecer estrategias para su mitigación antes los posibles daños que estos pueden causar a la red privada virtual.
2. Establecer políticas de seguridad capaces de controlar los accesos, la seguridad física, las copias de seguridad y la seguridad de los sistemas de información, que forman parte de la red privada virtual.
3. Identificar y aplicar los protocolos de seguridad para garantizar la autenticación de usuarios, el cifrado y la integridad de datos asociados a la red privada virtual.

FASE 5: Aceptación y Mitigación de Riesgos

Para mitigar los riesgos es necesario establecer estrategias para evaluar los posibles daños causados en la red privada virtual. Se debe identificar acciones para evitar o minimizar el impacto de los riesgos, los cuales ponen en peligro el correcto funcionamiento de la red VPN.

a. Acciones

Para identificar los riesgos es necesario realizar lo siguiente:

- Enumerar una lista de riesgos que afectarían la red VPN
- Categorizar los riesgos desde la probabilidad que ocurran hasta el impacto que podrían tener.
- Estipular las formas de controlar, evitar o mitigar los posibles riesgos críticos.

- Documentar los riesgos y el grado de ocurrencia de estos.

Como estrategias para mitigar el riesgo podemos indicar:

- Identificar los riesgos que podrían impedir el correcto funcionamiento de la red privada virtual, así mismo se debe categorizar el riesgo en la red de acuerdo a su grado de ocurrencia y a su impacto.
- Identificar alternativas para administrar el riesgo por parte del equipo de TI.

Tabla 29. *Identificación de riesgos*

	Riesgo	Probabilidad	Impacto	Estrategia de mitigación
1.	Falta de disponibilidad de los servicio de internet	Baja	Alto	Ejecutar los SLA (acuerdos de nivel de servicio) para que reponga el servicio
2.	Usuarios no autenticados, con acceso a la VPN	Media	Alto	Establecer una política de autenticación de usuarios

Fuente: Elaboración propia

FASE 6: Implementación de Políticas de Seguridad

La oficina de la Red Telemática de la entidad es la responsable de la elaboración e implementación de políticas de seguridad para ello se deben establecer parámetros como; control de accesos, seguridad física, protección de equipos y copias de seguridad, seguridad de los sistemas, entre otros. Así mismo está oficina será la encargada del cumplimiento de las políticas de seguridad.

a. Acciones

Establecer controles de acceso físico a las áreas protegidas para el procesamiento de información

- Supervisar y proteger a los visitantes de áreas protegidas.
- Controlar y limitar el acceso a la información clasificada exclusivamente a las personas autorizadas.
- Revisar cada cierto tiempo el acceso a las áreas protegidas,

Establecer políticas de mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanente.

- Realizar tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y las especificaciones recomendadas por el proveedor.
- Establecer que solo el personal autorizado para el mantenimiento, sea el indicado para que realice esta labor; así mismo se debe documentar todo el mantenimiento preventivo y correctivo realizado.

Implantar políticas de escritorios y pantallas limpias para proteger documentos en papel y dispositivos de almacenamientos removibles.

- Almacenar bajo llave en gabinetes, cuando corresponda, los documentos en papel y los medios informáticos, cuando no están siendo utilizados.
- Desconectar de la red o sistema las computadoras personales, impresoras asignadas a funciones críticas, cuando no están en uso.
- Bloquear fotocopiadoras fuera de horario normal de trabajo.

Implantar políticas de seguridad para el resguardo de la información y protección contra software malicioso

- Definir un esquema de etiquetado de copias de seguridad que permita administrarlas debidamente.
- Almacenar en una ubicación remota copias de información reciente junto con registros exactos y completos de las mismas.
- Prohibir la instalación y uso de software no autorizado por la organización.
- Redactar procedimientos para evitar riesgos relacionados con la obtención de archivos y software desde o través de redes externas.

Establecer controles que permita garantizar la seguridad de los datos y los servicios conectados a la red.

- Establecer procedimientos para la administración de equipos remotos, incluyendo los equipos de las áreas usuarias.
- Implantar controles para el aseguramiento de la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas.
- Implantar controles para la protección contra ataques al correo electrónico, como por ejemplo virus, interceptación, phising, etc.
- Usar técnicas de encriptación para proteger la confidencialidad e integridad de los mensajes electrónicos.
- Definir los alcances del uso del correo electrónico por parte del personal de la organización.
- Concientizar al personal sobre la toma de las debidas precauciones, como por ejemplo no revelar información sensible

para evitar ser escuchado o interceptado a través de una llamada telefónica, mensajes de correo electrónico o mensajes por redes sociales.

Implantar políticas de seguridad para impedir el acceso no autorizado a los sistemas de información, base de datos y servicios de información.

- Establecer reglas obre la premisa “Todo está permitido a menos que se prohíba expresamente”
- Definir perfiles de acceso de usuarios en función a las tareas a realizar.
- Administrar las contraseñas de usuario de tal manera que estás tengan 8 caracteres como mínimo y que contengan por lo menor una letra, un número y un carácter especial. Así mismo renovar contraseñas cada 90 días, finalmente impedir que las últimas 10 contraseñas puedan volver a ser reutilizadas.

FASE 7: Implementación de Protocolos de Seguridad

La implementación de protocolos de seguridad estará en función de la compatibilidad del sistema operativo, velocidad, autenticación y cifrado e integridad de los datos. Por su parte los protocolos de seguridad VPN determinan exactamente la forma en que los datos se enrutan desde un computador o dispositivo hasta el router o servidor VPN.

a. Acciones

- Elaborar una tabla comparativa (ver Tabla N° 30) que permita elegir el conjunto de protocolos que mejor se adecúan a los requerimientos de la red privada virtual
- Determinar el tipo de protocolo de seguridad VPN de acuerdo a las necesidades del usuario y a los servicios a implementar sobre la plataforma tecnológica (componentes de oficina doméstica o componentes corporativos). También puede consultar la Tabla N° 01 (comparativa de protocolos VPN).

Tabla 30. *Identificación de protocolos de seguridad*

Protocolo	Confidencialidad (cifrado)	Integridad	Autenticación
1. IPSec	- Poco seguros: DES (Encriptación de Datos Estándar), 3DES (Triple DES) - Cifrado simétrico AES (Encriptación avanzada) - Cifrado Simétrico RSA (Rivest, Shamir, Adleman)	- Algoritmo DH (Deffie Hellman) - Algoritmos HASH: MD5 (Algoritmo de Resumen de Mensaje 5), SHA-1 (Algoritmo Hash Seguro)	- PSK (clave previamente compartida) - Firmas RSA, DSA (Algoritmo de Firma Digital).
2. OpenVPN	- AES - OpenSSL - Camellia - Blowfish	- SSL/TLS (Transport Layer Security) - SHA	- RSA - LDAP - RADIUS
3. SSTP	- SSL (Secure Socket Layer)	- SSL/TLS	- EAP – TLS - MS - CHAP
4. IKEv2 (conexión recomendada para dispositivos móviles)	- AES - RSA	- SHA - PFS (Perfect Forward Secrecy)	- PSK

Fuente: Elaboración propia

ETAPA 3: SEGUIMIENTO Y CONTROL

Esta etapa tiene como finalidad la vigilancia de todas las fases de la metodología ya que siguiendo un adecuado control hace posible evitar desviaciones en costos, plazos y riesgos o al menos detectarlos cuanto antes. En esta etapa se debe establecer un conjunto de acciones que se llevarán a cabo para la comprobación de la correcta ejecución de la metodología, según como se muestra en la tabla N° 31.

Tabla 31. *Actividades de seguimiento y control*

Fase	Acciones	Indicador	Escala	
			1 – No logrado	**2 – Por lograr**
			3 – Logrado	**4 - Superado**
1. Identificación Contextual de Usuarios	Identificar los tipos de usuarios (directivo, especialista, operador, generador y consumidor de información) que utilizarán la red privada virtual.	Porcentaje de usuarios identificados por tipo		
	Determinar el nivel de interés de los usuarios, así como sus expectativas, importancia e influencia en el desarrollo de la red privada virtual.	Nivel de interés del usuario (bajo, medio, alto)		
	Describir del nivel de participación de los usuarios identificando sus necesidades y expectativas para lograr su compromiso durante el desarrollo de la red.	Nivel de compromiso del usuario (bajo, medio, alto)		
	Establecer un canal de comunicación claro y directo con los usuarios a fin de balancear sus expectativas con los objetivos del proyecto de red privada virtual.	Número de canales establecidos		
2. Requerimientos y Servicios de Red	Utilizar técnicas para la obtención de los requisitos tales como: las entrevistas, el brainstorming, casos de uso o el desarrollo conjunto de aplicaciones (JAD).	Número de técnicas utilizadas		
	Identificar y analizar la información que ha de ser procesada e intercambiada entre los diferentes sitios de la red privada virtual.	(información identificada / información analizada) x100		

	Identificar las aplicaciones que pasará por la red privada virtual. Por ejemplo, servicio de telefonía, servicio de replicación de base de datos, acceso a los sistemas de información.	Porcentaje de aplicaciones identificadas
	Establecer los niveles de seguridad que se implementará en la red privada virtual. Como la autenticación y la privacidad de los datos; así mismo controlar quien puede acceder a cada uno de los sistemas en cada conexión.	Niveles de seguridad a establecer en la VPN
3. Topología de Red	Diseñar físicamente la red a través de un diagrama de topología física para redes privadas virtuales	Plano físico de la red elaborado
	Diseñar lógicamente la red a través de un diagrama de topología lógica para redes privadas virtuales.	Plano lógico de la red elaborado
4. Infraestructura Tecnológica de la Red Privada	Identificar los componentes de la oficina doméstica, los cuales básicamente son: una computadora portátil o de escritorio o tablet, acceso a internet por banda ancha (ADSL, WIFI o plan de datos) y un software de router o cliente VPN instalado en la computadora, adicionalmente puede necesitarse de un punto de acceso inalámbrico.	Porcentaje de componentes de oficina domestica identificados para la VPN
	Identificar los componentes corporativos, los cuales están conformados por los routers con capacidad VPN, los concentradores VPN, dispositivos de seguridad multifunción y dispositivos de autenticación y administración central para la agregación y la terminación resistentes de las conexiones VPN	Porcentaje de componentes corporativos identificados para la VPN

5. Aceptación y Mitigación de Riesgos	Enumerar una lista de riesgos que afectarían la red VPN	Porcentaje de riesgos enumerados
	Categorizar los riesgos desde la probabilidad que ocurran hasta el impacto que podrían tener.	Probabilidad de ocurrencia del riesgo
	Estipular las formas de controlar, evitar o mitigar los posibles riesgos críticos.	Número de formar para mitigar los riesgos críticos
	Documentar los riesgos y el grado de ocurrencia de estos	Numero de riesgos documentados x probabilidad de ocurrencia
	Identificar alternativas para administrar el riesgo por parte del equipo de TI.	Porcentaje de alternativas de administración de riesgos
6. Implementación de Políticas de Seguridad	Establecer controles de acceso físico a las áreas protegidas para el procesamiento de información.	Porcentaje de controles de acceso físico establecidos
	Establecer políticas de mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanente.	Porcentaje de políticas de mantenimiento de equipamiento establecidas

	Implantar políticas de escritorios y pantallas limpias para proteger documentos en papel y dispositivos de almacenamientos removibles.	Porcentaje de implementación de políticas de escritorios y pantallas limpias
	Implantar políticas de seguridad para el resguardo de la información y protección contra software malicioso	Porcentaje de implementación de políticas de resguardo de información
	Establecer controles que permita garantizar la seguridad de los datos y los servicios conectados a la red.	Porcentaje de controles establecidos de seguridad de los datos y servicios de red
	Implantar políticas de seguridad para impedir el acceso no autorizado a los sistemas de información, base de datos y servicios de información.	Porcentaje de implementación de políticas de seguridad de acceso no autorizado
7. Implementación de Protocolos de Seguridad	Elaborar una tabla comparativa que permita elegir el conjunto de protocolos que mejor se adecuan a los requerimientos de la red privada virtual	Porcentaje de protocolos seleccionados para la red privada virtual
	Determinar el tipo de protocolo de seguridad VPN de acuerdo a las necesidades del usuario y a los servicios a implementar sobre la plataforma tecnológica (componentes de oficina doméstica o componentes corporativos).	Nivel de seguridad VPN

Fuente: Elaboración propia

Conclusiones parciales

- La metodología planteada surge como alternativa guiar a los grupos de interés (directivos, funcionarios, y personal de TI) en la gestión del proceso de seguridad informática para el intercambio de información académica contextualizada en entornos de conexiones públicas, a través de un conjunto y acciones que contribuyan a mejorar este proceso.
- Para el desarrollo de la metodología se ha tenido en cuenta el modelo de seguridad informática, que a su vez permite mediante un planteamiento ordenado y estructurado ofrecer a través de etapas, fases y acciones una guía para la implementación de la red privada virtual que garantice el intercambio de información académica contextualizada en entornos públicos de manera segura y confiable.
- Finalmente se plantea un cuadro de mando para el seguimiento y control de cada una de las fases y las acciones relaciones a estas, permitiendo a través de indicadores la vigilancia y control de los pasos a seguir para la implementación de la metodología.

TERCERA PARTE

VALIDACIÓN DE LOS RESULTADOS

CAPÍTULO 6. VALORACIÓN Y CORROBORACIÓN DE LOS RESULTADOS

Introducción

En este capítulo se describe la valoración cualitativa de la pertinencia del aporte teóricos (modelo de seguridad informática) y el aporte práctico (metodología adaptativa para redes privadas virtuales en entornos de conexiones de redes públicas) en los resultados de la presente investigación, realizada por juicio de expertos, así mismo se plantea la aplicación parcial de la metodología en la Universidad Nacional Pedro Ruiz Gallo.

6.1. Valoración de los resultados

Primeramente, se aplicó una encuesta a cinco posibles expertos para determinar su grado de conocimiento, grado de influencia en cada una de las fuentes de argumentación, para luego obtener los resultados de valoración de la competencia de cada uno de los cinco expertos encuestados.

Tabla 32. *Grado de Conocimiento del Experto*

N°	EXPERTO	1	2	3	4	5	6	7	8	9	10
1	Dr. Luis Alberto Dávila Hurtado								**X**		
2	Dr. Mario Fernando Ramos Moscol									**X**	
3	Dr. Luis Jaime Collantes Santisteban								**X**		
4	Dr. Martin Wilson Lozano Rivera								**X**		
5	Dr. Alberto Enrique Samillan Ayala							**X**			

Fuente: Elaboración propia

Aplicando las formulas, se obtuvo los siguientes coeficientes de conocimiento respectivamente:

Kc1 0.8
Kc2 0.9
Kc3 0.8
Kc4 0.8
Kc5 0.7

Tabla 33. *Grado de Influencia del Experto en relación a las Fuentes de Argumentación*

N°	Fuentes de Argumentación	EXPERTO 1			EXPERTO 2			EXPERTO 3			EXPERTO 4			EXPERTO 5		
		A	M	B	A	M	B	A	M	B	A	M	B	A	M	B
1	Análisis teóricos realizados		X			X		X				X			X	
2	Experiencia como profesional	X			X			X			X				X	
3	Trabajos de autores nacionales		X			X		X			X				X	
4	Trabajos de autores extranjeros		X			X			X			X				X
5	Sus propios conocimientos sobre el estado del problema de investigación		X		X			X				X			X	
6	Su intuición	X			X			X				X			X	

Fuente: Elaboración propia

Aplicando las formulas, se obtuvo los siguientes coeficientes de argumentación, respectivamente:

Ka1	0.2	0.5	0.05	0.05	0.05	0.05	0.9
Ka2	0.2	0.5	0.05	0.05	0.05	0.05	0.9
Ka3	0.3	0.5	0.05	0.05	0.05	0.05	1
Ka4	0.2	0.5	0.05	0.05	0.05	0.05	0.9
Ka5	0.2	0.4	0.05	0.05	0.05	0.05	0.8

Tabla 34. *Resultados de la valoración de la competencia a expertos*

N°	EXPERTO	Kc	Ka	K=1/2(Kc + Ka)	Competencia
1	Dr. Luis Alberto Dávila Hurtado	0.8	0.9	**0.85**	**Alta**
2	Dr. Mario Fernando Ramos Moscol	0.9	0.9	**0.9**	**Alta**
3	Dr. Luis Jaime Collantes Santisteban	0.8	1	**0.9**	**Alta**
4	Dr. Martin Wilson Lozano Rivera	0.8	0.9	**0.85**	**Alta**
5	Dr. Alberto Enrique Samillan Ayala	0.7	0.8	**0.75**	**Media**

Fuente: Elaboración propia

De los resultados de la valoración de la competencia a expertos, se seleccionaron a tres especialistas para con el objetivo de valorar la pertinencia de la *Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas*. En donde se expresa una representación participativa de los especialistas con el investigador, permitiendo un intercambio continuo e enriquecedor con los profesionales seleccionados, desde un enfoque sistémico, que corroboran tanto el constructo teórico como el práctico.

6.2. Ejemplificación de la aplicación del aporte práctico

Para la aplicación del aporte práctico (metodología adaptativa para redes privadas virtuales en entornos de conexiones de redes públicas), se ejecutó de manera parcial la metodología correspondiente a la **Etapa 1** (dimensión de la gestión de la conectividad de la red), **Fase 1** (identificación contextual de usuarios), **Fase 2** (requerimientos y servicios de red) y **Fase 3** (topología de red), teniendo como escenario la Universidad Nacional Pedro Ruiz Gallo.

FASE 1: Identificación Contextual de Usuarios

En esta fase se identificó a los usuarios involucrados con el desarrollo del proyecto para la implementación de la red privada virtual. Entre los usuarios identificados tenemos: Los directivos y líderes de la organización, los especialistas y operadores de la red, los generadores y consumidores de información; así como, los usuarios remotos y usuarios móviles. Tal como se muestra en la tabla 35.

Tabla 35. *Identificación de usuarios de la Organización*

Rol	Expectativa	Influencia	Tipo de Usuario
1. Líder de la Organización	Brindar un servicio seguro y con tecnología de punta	Alta	Líder
2. Directivo Jefe de la Oficina Central de Informática	Implementar la red privada virtual confiable, segura y escalable entres las sedes de la organización	Alta	Especialista
3. Jefe de la Red Telemática	Administra la red privada virtual que responda a la expectativas del usuario	Alta	Especialista
4. Responsable de informática Centro Pre Universitario	Mantener la red privada virtual y que esté disponible para los usuarios	Alta	Operador
5. Empleado Administrativo	Intercambiar información de manera rápida y segura.	Media	Generador y consumidor de información,

Fuente: Elaboración propia

FASE 2: Requerimientos y Servicios de Red

En esta fase se identificó los requerimientos en relación con las expectativas del usuario (ver tabla 36). Así mismo se identificaron los servicios que correrán sobre la red privada virtual (ver tabla 37), que por su naturaleza son aquellos que estarán disponibles para los usuarios de la sede remota, garantizando el acceso a los datos de la organización de manera rápida y oportuna.

Tabla 36. *Identificación de requerimientos de la Organización*

Requerimiento	Área usuaria	Descripción	Influencia
1. Conectividad a Internet independiente	Red Telemática	La red privada virtual debe estar conectada por una línea conexión a internet dedicada de manera independiente	Alta
2. Red privada virtual segura y de fácil administración	Red Telemática	La red privada virtual debe ser de fácil administración tanto local como remota con acceso seguro	Alta
3. Enviar y compartir información entre las sedes	Área Académica	Red VPN que permita de manera fácil y segura el intercambio de información entre los sitios de la organización	Alta
4. Disponibilidad de la información	Red Telemática	El acceso a la información por parte de usuarios autorizados a través de la VPN debe estar disponible en el momento oportuno	Alta
5. Envío de información	Red Telemática	La red privada virtual debe garantizar el envío confiable, rápido y seguro de información (datos, voz y video)	Media

Fuente: Elaboración propia

Tabla 37. *Identificación de servicios de la Organización*

Servicio	Usuarios	Descripción	Tráfico
1. Acceso remoto a la VPN	Usuario remotos	Usuarios que desean acceder remotamente de un sitio central o sucursal y viceversa	Medio
2. Servicio de VoIP	Usuarios remotos y móviles	Usuarios de desean hacer uso del servicio de Telefonía IP de la organización	Alto
3. Servicio de videoconferencia	Usuarios remotos y móviles	Administración del streaming de video de la organización	Alto
4. Autenticación e usuarios	Todos	Determinar los tipos de autenticación de usuarios para conectarse a la red	Medio
5. Acceso a los sistemas de información	Usuarios remotos	Usuarios que acceden desde la sucursal a los sistemas de información de la sede central	Alto
6. Servicio de protección de información	Todos	Sistemas de antivirus, spyware, antiphising, entre otros que protejan la información del usuario	Alto

Fuente: Elaboración propia

FASE 3: Topología de Red

En cuanto al diseño de la red privada virtual se ha tenido en cuenta los dos diagramas; el diagrama de topología física y el diagrama de topología lógico.

Diagrama de topología física

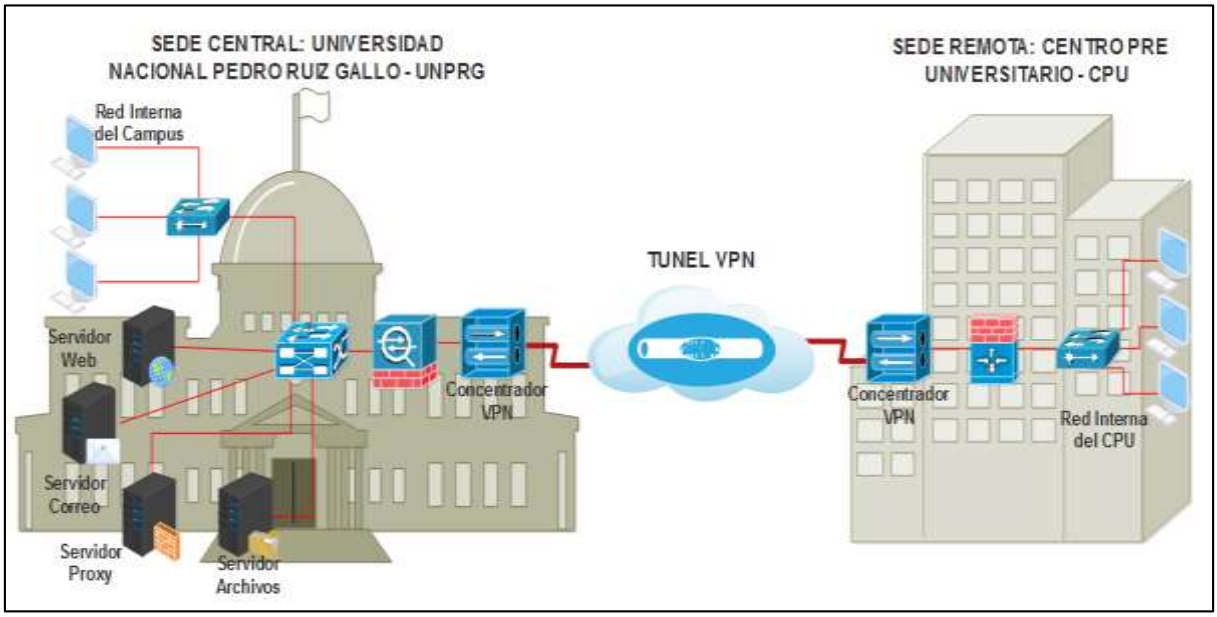


Figura 54. Diagrama de topología física de la red

Diagrama de topología lógica

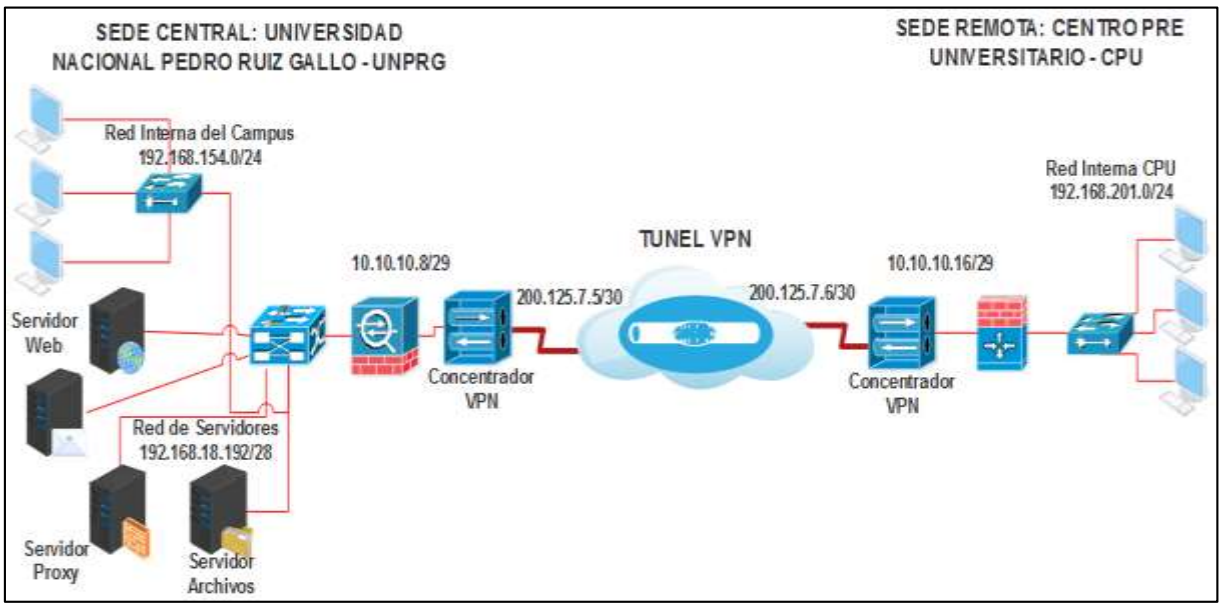


Figura 55. Diagrama de topología lógica de la red

6.3. Corroboración estadística de las transformaciones logradas

Fase	Acciones	Escala	
		1 – No logrado	**2 – Por lograr**
		3 – Logrado	**4 - Superado**
1. Identificación Contextual de Usuarios	Identificar los tipos de usuarios (directivo, especialista, operador, generador y consumidor de información) que utilizarán la red privada virtual.	4	
	Determinar el nivel de interés de los usuarios, así como sus expectativas, importancia e influencia en el desarrollo de la red privada virtual.	3	
	Describir del nivel de participación de los usuarios identificando sus necesidades y expectativas para lograr su compromiso durante el desarrollo de la red.	3	
	Establecer un canal de comunicación claro y directo con los usuarios a fin de balancear sus expectativas con los objetivos del proyecto de red privada virtual.	2	
2. Requerimientos y Servicios de Red	Utilizar técnicas para la obtención de los requisitos tales como: las entrevistas, el brainstorming, casos de uso o el desarrollo conjunto de aplicaciones (JAD).	3	
	Identificar y analizar la información que ha de ser procesada e intercambiada entre los diferentes sitios de la red privada virtual.	4	
	Identificar las aplicaciones que pasará por la red privada virtual. Por ejemplo, servicio de telefonía, servicio de replicación de base de datos, acceso a los sistemas de información.	3	
	Establecer los niveles de seguridad que se implementará en la red privada virtual. Como la autenticación y la privacidad de los datos; así mismo controlar quien puede acceder a cada uno de los sistemas en cada conexión.	3	
3. Topología de Red	Diseñar físicamente la red a través de un diagrama de topología física para redes privadas virtuales	4	
	Diseñar lógicamente la red a través de un diagrama de topología lógica para redes privadas virtuales.	4	

Fuente: Elaboración propia

6.4. Pre y Post Test de la variable dependiente: Intercambio de información académica contextualizada

Dimensión	Indicador	Actual	Proyectado	Diferenciado
Conectividad de la red	Tipo de usuarios	- Directivo - Especialista - Operador - Generador y consumidor de información	- Directivo - Especialista - Operador - Generador y consumidor de información	Los tipos de usuario se mantienen pero estos se tienen que proyectar con diferentes niveles de influencia (alta, media, baja) en el intercambio de información académica.
	Requerimientos y servicios de red	- Conectividad a Internet independiente - Red VPN segura y de fácil administración - Enviar y compartir información entre las sedes - Acceso remoto a la VPN - Servicio de VoIP - Autenticación e usuarios - Acceso a los sistemas de información	- Conectividad a Internet independiente - Red privada virtual segura y de fácil administración - Enviar y compartir información entre las sedes - Disponibilidad de la información - Envío confiable de información (datos, voz y video) - Acceso remoto a la VPN - Servicio de VoIP - Servicio de videoconferencia - Autenticación e usuarios - Acceso a los sistemas de información - Servicio de protección de información	La recolección de requerimientos se ha visto mejorado debido a que se utilizaron técnicas para la obtención de los mismos tales como: las entrevistas, el brainstorming, reuniones, entre otros. Así mismo se identificó y analizo la información que ha de ser procesada e intercambiada entre los diferentes sitios de la red privada virtual. Finalmente se identificó las aplicaciones que pasará por la red privada virtual. Por ejemplo, servicio de telefonía, servicio de replicación de base de datos, acceso a los sistemas de información. la autenticación y la privacidad de los datos.
	Topología de red	- Topología lógica	- Topología lógica - Topología física	El diseño lógico de la VPN se llegó a simular en el software GNS3, en donde se puede corroborar la conexión entre los dos sitios de la red.

Fuente: Elaboración propia

Conclusiones parciales

- Se logró aplicar la encuesta a cinco posibles expertos para determinar su grado de conocimiento, grado de influencia en cada una de las fuentes de argumentación, para luego obtener los resultados de valoración de la competencia, quedando elegidos tres expertos especialistas.
- La metodología adaptativa para redes privadas virtuales en entornos de conexiones de redes públicas se logró aplicar en la Universidad Nacional Pedro Ruiz Gallo de manera parcial para las tres primeras fases de la metodología: identificación de usuarios, requerimientos y servicios de red y topología de red, pudiendo ser corroboradas por el cuadro de mandos de seguimiento y control de la metodología.
- Por su parte el análisis de pre test y post de la variable dependiente (intercambio de información académica contextualizada) revela que los indicadores: tipos de usuarios, requerimientos y servicios de red y topología de red han pasado de un estado actual a un estado proyectado lo que demuestra un cambio favorablemente positivo en la variable en donde los tipos de usuarios se mantienen tal cual, pero con diferentes niveles de influencia; por su parte la recolección de requerimientos obtuvo mejoras debido a que se utilizaron técnicas adecuadas para la obtención de los mismos. Así mismo la topología lógica de la red, se simuló con el del software GNS3, llegando a corroborar la conexión entre los dos sitios de la red privada virtual.

CONCLUSIONES GENERALES

El estudio teórico realizado sobre la caracterización del proceso de seguridad informática en redes privadas virtuales en su evolución histórica, así como los resultados obtenidos de la aplicación parcial de una metodología adaptativa para la implementación de redes privadas virtuales en la Universidad Nacional Pedro Ruiz Gallo, sustentada en un modelo sistémico, sujeto a valoración a través de métodos cuantitativos como parte del cumplimiento de las tareas científicas de la investigación, conlleva a que se aborde a las siguientes **conclusiones**:

1. En la caracterización del proceso de seguridad informática se logró determinar que las organizaciones requieren redes seguras y altamente confiables que permitan proteger la confidencialidad, la integridad y disponibilidad de la información, para lo cual cobra especial importancia y es necesario disponer de estos mecanismos de seguridad informática.
2. Se determinó las tendencias históricas sobre el proceso de seguridad informática en redes privadas virtuales, las cuales no satisfacen las exigencias tecnológicas actuales, como un camino para lograr un mayor nivel en la dinámica de este proceso.
3. El diagnóstico realizado a través de los métodos y técnicas de recolección de datos como la observación de los procedimientos para el intercambio de información, entrevista a los empleados especialista en TI de la Oficina General de Sistemas Informáticos, encuesta a los empleados administrativos de las Oficinas académicas de la Universidad y Centro Pre Universitario, se constata que el intercambio de información entre los usuarios de la red es poco segura, escasa capacitación al personal administrativo en temas de políticas de seguridad, también se evidencia deficiencias para el intercambio de información académica contextualizada entre las

Oficinas académicas de la Universidad y el Área académica del Centro Pre Universitario.

4. El modelo elaborado se sustenta en la concepción sistémica a partir de la teoría general de sistemas, el cual funciona como un todo en donde cada uno de los elementos se interrelacionan mutuamente conllevando a revelar dos dimensiones: dimensión de gestión de conectividad de la red y dimensión de gestión de seguridad de la red.
5. La metodología para la dinámica del proceso de seguridad informática propuesta para la Universidad Nacional Pedro Ruiz Gallo, posibilita la implementación de redes privadas virtuales mediante una guía organizada a través de etapas, fases y acciones; que garantice el intercambio de información académica contextualizada en entornos públicos de manera segura y confiable.
6. La factibilidad, el valor científico y la pertinencia del modelo, así como la metodología, fueron corroborados por tres expertos de reconocida trayectoria académica y profesional de la región, conllevando a reconocer que la propuesta posee potencialidades de contribuir a las organizaciones intercambiar información de manera segura a través de las redes privadas virtuales.
7. La metodología adaptativa basada en un modelo de seguridad informática para redes privadas virtuales, fue aplicada parcialmente en la red Telemática de la Universidad Nacional Pedro Ruiz Gallo y el Centro Pre Universitario de la entidad; la aplicación parcial correspondiente a la Etapa 1: dimensión de la de conectividad de la red y las tres primeras fases (a. Identificación de usuarios, b. Requerimientos y servicios de red y c. Topología de red) de esta etapa.

RECOMENDACIONES

Los resultados de la investigación y su metodología práctica, contribuyen al mejoramiento del proceso de seguridad informática durante el intercambio de información en las redes privadas virtuales en ese sentido se **recomienda**:

1. Revelar los eslabones de la dinámica del proceso de seguridad informática en el intercambio de información en redes privadas virtuales conlleva al entendimiento, a la mejora y puesta en marcha de este proceso.
2. Realizar investigaciones sobre ciberseguridad enfocada en la seguridad interna, seguridad externa y seguridad perimetral, para lograr un enfoque integrador sobre la dinámica del proceso de seguridad informática y la protección en el intercambio de información vital para las empresas.
3. Plantear la aplicación de la metodología en el intercambio de información a través de redes privadas virtuales de manera confiable y segura entre las sedes y sucursales de las organizaciones.

REFERENCIAS BIBLIOGRÁFICAS

Alvarez Marañón, G., & Pérez García, P. P. (2004). *Seguridad informática para empresas y particulares.* Madrid: McGraw-Hill.

Areitio Bertolín, J. (2008). *Seguridad de la Información.* Madrid: Paraninfo.

Baca Urbina, G. (2016). *Introducción a la seguridad informática.* México D.F.: Grupo Editorial Patria.

Bertalanffy, L. V. (1979). *Perspectivas en la Teoría General de Sistemas.* Madrid: Alianza Universidad.

Cisco Networking Acadamy. (2014). *Connecting Networks Companion Guide.* California: Cisco Press.

Cisco Networking Academy. (2014). *Capítulo 6: Soluciones de banda ancha 6.1.1.1 Introducción al trabajo a distancia*. Obtenido de Cisco Networking Academy: https://static-course-assets.s3.amazonaws.com/CN50ES/course/module6/index.html#6.1.1.1

Cisco Networking Academy. (2014). *Capítulo 7: Seguridad de la conectividad Site-to-Site 7.0.1.1 Introducción*. Obtenido de Cisco Networking Academy: https://static-course-assets.s3.amazonaws.com/CN50ES/course/module7/index.html#7.0.1.1

Cisco Networking Academy. (2014). *Capítulo 7: Seguridad de la conectividad Site-to-Site 7.3.1.1 IPsec*. Obtenido de Cisco Networking Academy: https://static-course-assets.s3.amazonaws.com/CN50ES/course/module7/index.html#7.3.1.1

Costas Santos, Jesús. (2014). *Seguridad Informática.* Madrid: RA-MA.

Díaz Orueta, G., Alzórriz Armendáriz, I., & Sancristóbal Ruiz, E. (2014). *Procesos y herramientas para la seguridad de redes.* Madrid: EDITORIAL UNED - Universidad Nacional de Educación a Distancia.

EcuRed. (22 de Mayo de 2018). *Usuario (Informática).* Obtenido de EcuRed: https://www.ecured.cu/Usuario_(Informática)

Expósito Unday, D., & Gonzáles Valero, J. A. (2017). Sistematización de experiencias como método de investigación. *Scielo*, 1-6. Obtenido de http://scielo.sld.cu/pdf/gme/v19n2/GME03217.pdf

Fernández Sánchez, C., & Piattini Velthuis, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO.* Madrid: AENOR.

Giménez Albacete, J. F. (2014). *Seguridad en equipos informáticos.* Madrid: IC Editorial.

Golden Frog. (15 de Junio de 2017). *Comparación de Protocolos de VPN*. Obtenido de Protocolos de VPN: https://www.goldenfrog.com/es/vyprvpn/features/vpn-protocols

Gómez Fernández, L., & Andrés Álvarez, A. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.* España: AENOR - Asociación Española de Normalización y Certificación.

Gómez Fernández, Luis; Fernández Rivero, Pedro Pablo. (2015). *Como implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad.* Madrid: AENOR.

Gómez Vieites, Á. (2014). *Sistemas seguros de acceso y transmisión de datos.* MAdrid: RA-MA.

González Manzano, L., & Fuentes García-Romero de Tejada, J. (2014). *Sistemas seguros de acceso y transmisión de datos.* Madrid: IC Editorial.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). *Metodología de la Investigación* (6ta Edición ed.). México D.F.: Mc Graw Hill Education.

ISO 27000.es. (30 de Julio de 2016). *El portal de ISO 27001 en Español*. Obtenido de ISO 27000.es: http://www.iso27000.es/iso27000.html#home

Jcor. (2013). *Historia de las Redes y la Seguridad Informatica*. Obtenido de Science and Technology timelines: https://www.timetoast.com/timelines/historia-de-las-redes-y-la-seguridad-informatica

Lawas, J. B., Vivero, A., & Sharma, A. (2016). Network Performance Evaluation of VPN Protocols (SSTP and IKEv2). *IEEE Journal*.

LE VPN. (09 de Julio de 2017). *La historia de la VPN*. Obtenido de LE VPN: https://www.le-vpn.com/es/

López, M. Á., García, E., & Ortega, J. (2005). *Una Introducción a la Criptografía.* Castilla - España: Universidad de Castilla - La Mancha.

Lucidchart. (2015). *Qué es un diagrama de red*. Recuperado el 03 de Julio de 2018, de Lucidchart: https://www.lucidchart.com/pages/es/qu%C3%A9-es-un-diagrama-de-red

Masiá, A. J. (20 de Abril de 2015). *Proyectos: Planificación adaptativa*. Obtenido de Cambiando creencias: http://www.cambiandocreencias.com/proyectos-planificacion-adaptativa/

Muhamed, E., & Bujar, R. (2015). Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption. *Science Direct*, 1938-1948.

Narayan, S., Ishrar, S., Kumar, A., Gupta, R., & Khan, Z. (2016). Performance Analysis of 4to6 and 6to4 Transition Mechanisms over Point to Point and IPSec VPN Protocols. *IEEE Juornal*.

Penflip, J. (26 de Junio de 2014). *Implementación VPN*. Obtenido de https://www.penflip.com/Joan/implementacion-vpn/blob/master/chapter1.txt

PMBOOK. (2013). *Guía de los Fundamentos para la dirección de proyectos (Guía del PMBOOK)* (5ta Edición ed.). Pensilvania: Project Management Institute, Inc.

Rodríguez Jiménez, A., & Pérez Jacinto, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista Escuela de Administración de Negocios*, 179-200. doi:https://doi.org/10.21158/01208160.n82.2017.1647

Romero Ternero, M. (2004). *Ingeniería de Protocolos*. Obtenido de Seguridad en Redes y Protocolos Asociados: http://www.dte.us.es/personal/mcromero/docs/ip/tema-seguridad-IP.pdf

Santos Gonzáles, M. (2014). *Sistemas telemáticos.* Madrid: RA-MA.

UNPRG. (2017). *Estatuto UNPRG.* Lambayeque: Universidad Nacional Pedro Ruiz Gallo.

Yadav, S., & Jeyakumar, A. (2016). Design of Traffic Engineered MPLS VPN for Protected Traffic using GNS Simulator. *IEEE Journal*, 405-409.

Zhiyong, L., Guixin, Y., & Hongzhuo, Q. (2014). Research of A VPN Secure Networking Model. *IEEE Journal*, 567-569.

ANEXOS

Anexo 1. Matriz de consistencia

DEFINICIÓN DEL PROBLEMA	OBJETIVOS	TÍTULO	VARIABLES	HIPÓTESIS
Deficiencias e inconvenientes en el acceso seguro, limitan el intercambio de información académica contextualizada entre los sitios de la universidad	**OBJETIVO GENERAL** Elaborar una metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para la Universidad Nacional Pedro Ruiz Gallo que permita mejorar el intercambio de información académica contextualizada en un entorno de conexiones públicas. **OBJETIVOS ESPECÍFICOS** 1. Caracterizar epistemológicamente el proceso de seguridad informática en redes privadas virtuales. 2. Determinar las tendencias históricas del proceso de seguridad informática en redes privadas virtuales. 3. Diagnosticar el estado actual de la dinámica del proceso de seguridad informática de redes privadas virtuales en la Universidad Nacional Pedro Ruiz Gallo. 4. Elaborar un modelo seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en la Universidad Nacional Pedro Ruiz Gallo. 5. Elaborar una metodología adaptiva para la implementación del modelo de seguridad informática para redes privadas virtuales. 6. Corroborar la factibilidad y valor científico de los resultados de la investigación mediante criterios de expertos. 7. Ejemplificar parcialmente la aplicación de la metodología adaptativa del modelo de seguridad informática para redes privadas virtuales.	Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas	**VARIABLE INDEPENDIENTE** Modelo de seguridad informática para redes privadas virtuales y su metodología adaptativa. **VARIABLE DEPENDIENTE** Intercambio de información académica contextualizada.	Si se elabora una metodología adaptativa basada en un modelo de seguridad informática para redes privadas virtuales que tenga en cuenta la lógica de integración del proceso de seguridad informática y la lógica funcional de las políticas de seguridad de la organización, entonces se contribuye al mejoramiento del intercambio de información académica contextualizada en entornos de conexiones públicas

Anexo 2. Operacionalización de variables

Variable dependiente	Dimensión	Indicadores	Subindicadores	Técnicas e Instrumentos	Fuente de verificación
Intercambio de información académica contextualizada	Conectividad de la red	Tipos de usuarios	Directivos Especialistas Generadores y consumidores de información	Encuesta, Observación, Análisis documentario	Jefe de Informática, Personal administrativo, Reporte de aplicación de policías de seguridad, Reporte de funcionalidad de los equipos de informáticos.
		Requerimientos y servicios de red	Requerimientos funcionales Servicios de red		
		Topología de Red	Topología físico Topología lógica		
		Componentes de la infraestructura tecnológica de la red	Componentes móviles y de oficina Componentes corporativos		
	Seguridad informática	Riesgos	Identificación y aceptación de riesgos Mitigación de riesgos		
		Políticas de seguridad	Controles de acceso físico Políticas de mantenimiento de equipamiento Políticas de escritorios y pantallas limpias Políticas de resguardo de información Controles la seguridad de los datos		
		Protocolos de seguridad	Protocolos de cifrado, integridad y Autenticación		

Anexo 3. Encuesta a especialistas en tecnologías de la información de la entidad

Esta encuesta, es dirigida a los especialistas en tecnologías de la información de la Universidad. Con la presente entrevista se pretende diagnosticar el estado actual de la dinámica del proceso de seguridad informática en redes privadas virtuales de la Universidad Nacional Pedro Ruiz Gallo y tiene por finalidad obtener información sobre determinados aspectos relacionados con el compromiso de los directivos en relación a los proyectos de TI, la gestión de la tecnología informática y la implementación de las políticas y protocolos de seguridad en la red telemática, que garanticen el intercambio de información académica contextualizada en la entidad. Por ello le solicito que conteste con mucha claridad a las siguientes preguntas. Finalmente, de antemano le agradezco su valioso aporte que tiene carácter de anónimo.

Instrucciones

Al responder este cuestionario debe tener en cuenta lo siguiente:

- Lea detenidamente cada pregunta, antes de contestarla, así como sus posibles respuestas.
- Encontrará una forma fundamental de responder las preguntas.

Para responder la encuesta, debe utilizar el número correspondiente de la escala que se le ofrece; le ruego analizar con atención cada proposición, cuidando además de la exactitud y veracidad de sus respuestas, marcando con una (X) el número de la escala que te refleje mejor tu opción.

1. Totalmente en desacuerdo (TD)
2. Desacuerdo (D)
3. Ni en acuerdo ni en desacuerdo (I)
4. De acuerdo (DA)
5. Totalmente de acuerdo (TA)

ÍTEMS	**CATEGORÍA**				
	1	2	3	4	5
1. ¿Considera usted, que los directivos o jefes inmediatos se involucran o comprometen en el desarrollo de proyectos relacionados a las TIC?					
2. ¿Cree usted, que los especialistas en TIC de la Universidad, son responsables de sugerir nuevos proyectos en TIC?					
3. ¿Considera importante, realizar un diseño topológico de la red que permita el intercambio de información académica entre la Universidad sede Lambayeque y el Centro Pre Universitario sede Chiclayo?					

4. ¿Considera importante, que para conectarse a una red privada virtual desde el lugar donde se encuentre, es necesario contar con componentes móviles (conexión a internet, computador y software VPN instalado en la PC?					
5. ¿Considera importante, que para conectarse a una red privada virtual desde una sede central o remota, es necesario contar con componentes corporativos (routers VPN, firewall, concentrador VPN?					
6. ¿Considera necesario, la identificación y aceptación de riesgos que se puedan presentar en la red telemática?					
7. ¿Cree usted, que la mitigación de riesgos contribuye a mejorar la seguridad informática en la red telemática?					
8. ¿Considera necesario, establecer controles de acceso físico a los ambientes de procesamiento de información?					
9. ¿Considera necesario, establecer políticas de mantenimiento de equipamiento para los usuarios de la red telemática?					
10. ¿Cree usted necesario, establecer políticas de escritorios y pantallas limpias para los usuarios de la red telemática?					
11. ¿Cree usted necesario implementar políticas de resguardo de información para los usuarios de la red telemática?					
12. ¿Considera necesario, establecer controles de seguridad de los datos entre los usuarios de la red telemática?					

MUCHAS GRACIAS POR SU COLABORACIÓN

Anexo 4. Encuesta a empleados administrativos de la entidad

Esta encuesta, es dirigida a los empleados administrativos de la Universidad. Con la presente entrevista se pretende diagnosticar el estado actual de la dinámica del proceso de seguridad informática en redes privadas virtuales de la Universidad Nacional Pedro Ruiz Gallo y tiene por finalidad obtener información sobre determinados aspectos relacionados con el intercambio seguro y confiable de información académica contextualizada de la entidad. Por ello le solicito que conteste con mucha claridad a las siguientes preguntas. Finalmente, de antemano le agradezco su valioso aporte que tiene carácter de anónimo.

Instrucciones

Al responder este cuestionario debe tener en cuenta lo siguiente:

- Lea detenidamente cada pregunta, antes de contestarla, así como sus posibles respuestas.
- Encontrará una forma fundamental de responder las preguntas.

Para responder la encuesta, debe utilizar el número correspondiente de la escala que se le ofrece; le ruego analizar con atención cada proposición, cuidando además de la exactitud y veracidad de sus respuestas, marcando con una (X) el número de la escala que te refleje mejor tu opción.

1. Totalmente en desacuerdo (TD)
2. Desacuerdo (D)
3. Ni en acuerdo ni en desacuerdo (I)
4. De acuerdo (DA)
5. Totalmente de acuerdo (TA)

ÍTEMS	**CATEGORÍA**				
	1	2	3	4	5
1. ¿Considera importante, que como empleado de la entidad, usted es responsable de generar y consumir información?					
2. ¿Cree usted, que ante la implementación de un nuevo proyecto de red es necesario que como usuario, pueda indicar sus requerimientos para este proyecto?					
3. ¿Considera usted, que los servicios de red (Telefonía IP, acceso a los sistemas de información, autenticación de usuarios) se han definido en función de los requerimientos del usuario?					
4. ¿En la entidad, considera que cada de empleado accede de manera segura para conectarse a la red telemática?					

5.	¿Considera que la información debe viajar encriptada y que no esté sujeta a interceptaciones por parte de usuarios maliciosos?					
6.	¿Se siente seguro al enviar información por la red de la Universidad?					
7.	¿Cree usted, que su información puede ser interceptada por algún otro usuario de la red Telemática?					
8.	¿Se siente preparado para asumir algún tipo de riesgo frente a la perdida, alteración o robo de información?					
9.	¿Ha recibido algún de capacitación por parte de la entidad referente a políticas de seguridad de la información?					
10.	¿Considera necesario, que el intercambio de información entre los usuarios de la red telemática tendría estar normada por protocolos de seguridad?					

MUCHAS GRACIAS POR SU COLABORACIÓN

Anexo 5. Validación del instrumento. Encuesta a especialistas en TI de la entidad

1. ENCUESTA A ESPECIALISTAS EN TI DE LA ENTIDAD

INSTRUMENTO DE VALIDACIÓN NO EXPERIMENTAL POR JUICIO DE EXPERTOS

1. NOMBRE DEL JUEZ		Collantes Santisteban, Luis Jaime
2.	PROFESIÓN	Ingeniero de Sistemas e Informática
	ESPECIALIDAD	Gestión de Tecnologías de la Información
	GRADO ACADÉMICO	Doctor en Ciencias Aplicadas con Mención en Ingeniería Matemática
	EXPERIENCIA PROFESIONAL (AÑOS)	25 años
	CARGO	Catedrático – Universidad Nacional Pedro Ruiz Gallo
Título de la Investigación: Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas.		
3. DATOS DEL TESISTA		
3.1	NOMBRES Y APELLIDOS	Carrión Barco, Gilberto
3.2	PROGRAMA DE POSTGRADO	Doctorado en Ciencias de la Computación y Sistemas
4. INSTRUMENTÓ EVALUADO		Encuesta
5. OBJETIVOS DEL CUESTIONARIO		**GENERAL:** Diagnosticar el estado actual de la dinámica del proceso de seguridad informática en redes privadas virtuales de la Universidad Nacional Pedro Ruiz Gallo.
		ESPECÍFICOS - Diagnosticar el nivel de compromiso de los directivos con los proyectos de TIC de la Universidad Nacional Pedro Ruiz Gallo. - Diagnosticar el nivel de gestión de la tecnología informática en la Universidad Nacional Pedro Ruiz Gallo. - Diagnosticar el grado de implementación de las políticas y protocolos de seguridad en la red telemática de la Universidad Nacional Pedro Ruiz Gallo.

A continuación se le presentan los indicadores en forma de preguntas o propuestas para que Ud. los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS

N°	DETALLE DE LOS ÍTEMS DEL INSTRUMENTO	
01	- ¿Considera usted, que los directivos o jefes inmediatos se involucran o comprometen en el desarrollo de proyectos relacionados a las TIC?	A(X) D( ) SUGERENCIAS:
02	- ¿Cree usted, que los especialistas en TIC de la Universidad, son responsables de sugerir nuevos proyectos en TIC?	A(X) D( ) SUGERENCIAS:
03	- ¿Considera importante, realizar un diseño topológico de la red que permita el intercambio de información académica entre la Universidad sede Lambayeque y el Centro Pre Universitario sede Chiclayo?	A(X) D( ) SUGERENCIAS:
04	- ¿Considera importante, que para conectarse a una red privada virtual desde el lugar donde se encuentre, es necesario contar con componentes móviles (conexión a internet, computador y software VPN instalado en la PC?	A(X) D( ) SUGERENCIAS:
05	- ¿Considera importante, que para conectarse a una red privada virtual desde una sede central o remota, es necesario contar con componentes corporativos (routers VPN, firewall, concentrador VPN?	A(X) D( ) SUGERENCIAS:
06	- ¿Considera necesario, la identificación y aceptación de riesgos que se puedan presentar en la red telemática?	A(X) D( ) SUGERENCIAS:
07	- ¿Cree usted, que la mitigación de riesgos contribuye a mejorar la seguridad informática en la red telemática?	A(X) D( ) SUGERENCIAS:
08	- ¿Considera necesario, establecer controles de acceso físico a los ambientes de procesamiento de información?	A(X) D( ) SUGERENCIAS:
09	- ¿Considera necesario, establecer políticas de mantenimiento de equipamiento para los usuarios de la red telemática?	A(X) D( ) SUGERENCIAS:
10	- ¿Cree usted necesario, establecer políticas de escritorios y pantallas limpias para los usuarios de la red telemática?	A(X) D( ) SUGERENCIAS:
11	- ¿Cree usted necesario implementar políticas de resguardo de información para los usuarios de la red telemática?	A(X) D( ) SUGERENCIAS:
12	- ¿Considera necesario, establecer controles de seguridad de los datos entre los usuarios de la red telemática?	A(X) D( ) SUGERENCIAS:
	PROMEDIO OBTENIDO:	A(X) D( )

6. COMENTARIOS GENERALES

Instrumento bien elaborado

7. OBSERVACIONES

Dr. Collantes Santisteban, Luis Jaime
Juez Experto
Colegiatura CIP N° 184933

Anexo 6. Validación del instrumento. Encuesta a empleados administrativos de la entidad

2. ENCUESTA A EMPLEADOS ADMINISTRATIVOS DE LA ENTIDAD

INSTRUMENTO DE VALIDACIÓN NO EXPERIMENTAL POR JUICIO DE EXPERTOS

1. NOMBRE DEL JUEZ		Collantes Santisteban, Luis Jaime
2.	PROFESIÓN	Ingeniero de Sistemas e Informática
	ESPECIALIDAD	Gestión de Tecnologías de la Información
	GRADO ACADÉMICO	Doctor en Ciencias Aplicadas con Mención en Ingeniería Matemática
	EXPERIENCIA PROFESIONAL (AÑOS)	25 años
	CARGO	Catedrático – Universidad Nacional Pedro Ruiz Gallo
Título de la Investigación: Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas.		
3. DATOS DEL TESISTA		
3.1	NOMBRES Y APELLIDOS	Carrión Barco, Gilberto
3.2	PROGRAMA DE POSTGRADO	Doctorado en Ciencias de la Computación y Sistemas
4. INSTRUMENTÓ EVALUADO		Encuesta
5. OBJETIVOS DEL CUESTIONARIO	GENERAL:	Diagnosticar el estado actual de la dinámica del proceso de seguridad informática en redes privadas virtuales de la Universidad Nacional Pedro Ruiz Gallo.
	ESPECÍFICOS	- Diagnosticar el nivel de compromiso en cuanto a la aplicación de las políticas de seguridad en la red de la Universidad Nacional Pedro Ruiz Gallo, - Diagnosticar el nivel de conocimiento de la tecnología informática en la Universidad Nacional Pedro Ruiz Gallo.

A continuación se le presentan los indicadores en forma de preguntas o propuestas para que Ud. los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS

N°	DETALLE DE LOS ÍTEMS DEL INSTRUMENTO	
01	- ¿Considera importante, que como empleado de la entidad, usted es responsable de generar y consumir información?	A(X) D( ) **SUGERENCIAS:**
02	- ¿Cree usted, que ante la implementación de un nuevo proyecto de red es necesario que como usuario, pueda indicar sus requerimientos para este proyecto?	A(X) D( ) **SUGERENCIAS:**
03	- ¿Considera usted, que los servicios de red (Telefonía IP, acceso a los sistemas de información, autenticación de usuarios) se han definido en función de los requerimientos del usuario?	A(X) D( ) **SUGERENCIAS:**
04	- ¿En la entidad, considera que cada de empleado accede de manera segura para conectarse a la red telemática?	A(X) D( ) **SUGERENCIAS:**
05	- ¿Considera que la información debe viajar encriptada y que no esté sujeta a interceptaciones por parte de usuarios maliciosos?	A(X) D( ) **SUGERENCIAS:**
06	- ¿Se siente seguro al enviar información por la red de la Universidad?	A(X) D( ) **SUGERENCIAS:**
07	- ¿Cree usted, que su información puede ser interceptada por algún otro usuario de la red Telemática?	A(X) D( ) **SUGERENCIAS:**
08	- ¿Se siente preparado para asumir algún tipo de riesgo frente a la pérdida, alteración o robo de información?	A(X) D( ) **SUGERENCIAS:**
09	- ¿Ha recibido algún de capacitación por parte de la entidad referente a políticas de seguridad de la información?	A(X) D( ) **SUGERENCIAS:**
10	- ¿Considera necesario, que el intercambio de información entre los usuarios de la red telemática tendría estar normada por protocolos de seguridad?	A(X) D( ) **SUGERENCIAS:**
	PROMEDIO OBTENIDO:	A( ) D( )

6. COMENTARIOS GENERALES

Instrumento bien elaborado

7. OBSERVACIONES

Dr. Collantes Santisteban, Luis Jaime
Juez Experto
Colegiatura CIP N° 134937

Anexo 7. Validación del instrumento. Guía de observación

3. GUÍA DE OBSERVACIÓN ADMINISTRATIVOS DE LA ENTIDAD

INSTRUMENTO DE VALIDACIÓN NO EXPERIMENTAL POR JUICIO DE EXPERTOS

1.	NOMBRE DEL JUEZ	Collantes Santisteban, Luis Jaime
2.	PROFESIÓN	Ingeniero de Sistemas e Informática
	ESPECIALIDAD	Gestión de Tecnologías de la Información
	GRADO ACADÉMICO	Doctor en Ciencias Aplicadas con Mención en Ingeniería Matemática
	EXPERIENCIA PROFESIONAL (AÑOS)	25 años
	CARGO	Catedrático – Universidad Nacional Pedro Ruiz Gallo
	Título de la investigación: Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas.	
3.	DATOS DEL TESISTA	
3.1	NOMBRES Y APELLIDOS	Carrión Barco, Gilberto
3.2	PROGRAMA DE POSTGRADO	Doctorado en Ciencias de la Computación y Sistemas
4.	INSTRUMENTO EVALUADO	Guía de observación
5.	OBJETIVOS DEL CUESTIONARIO	**GENERAL:** Diagnosticar el estado actual de la dinámica del proceso de seguridad informática en redes privadas virtuales de la Universidad Nacional Pedro Ruiz Gallo.
		ESPECÍFICOS - Diagnosticar el tipo de información enviada y compartida entre los usuarios de la red de la Universidad Nacional Pedro Ruiz Gallo. - Diagnosticar el cumplimiento de las políticas de seguridad que la institución ejerce sobre el acceso y envío de información.

A continuación se le presentan los indicadores en forma de preguntas o propuestas para que Ud. los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS

N°	DETALLE DE LOS ÍTEMS DEL INSTRUMENTO	
01	- Se han establecido procedimientos y políticas para garantizar el envío seguro de información en la Universidad.	A(X) D( ) **SUGERENCIAS:**
02	- Las contraseñas utilizadas por el personal administrativo son seguras.	A(X) D( ) **SUGERENCIAS:**
03	- Las contraseñas son cambiadas con frecuencia.	A(X) D( ) **SUGERENCIAS:**
04	- El personal administrativo identifica el tipo de información según su uso: pública, privada, interna y externa.	A(X) D( ) **SUGERENCIAS:**
05	- El personal administrativo clasifica la información según su acceso: confidencial, privada y sensitiva.	A(X) D( ) **SUGERENCIAS:**
06	- El personal administrativo conoce sobre los riegos a los que está expuesta la información.	A(X) D( ) **SUGERENCIAS:**
07	- Se brinda capacitación o talleres de socialización relacionados con seguridad informática.	A(X) D( ) **SUGERENCIAS:**
08	- Se documentan las evidencias de las vulnerabilidades de la información.	A(X) D( ) **SUGERENCIAS:**
09	- La institución cuenta con una o área responsable de la seguridad informática.	A(X) D( ) **SUGERENCIAS:**
10	- Se han establecido perfiles de usuarios de acuerdo a los niveles de acceso, roles, responsabilidades, privilegios, etc.	A(X) D( ) **SUGERENCIAS:**
11	- La institución cuenta con medidas de seguridad frente a posibles ataques.	A(X) D( ) **SUGERENCIAS:**
12	- La institución cuenta con un plan de contingencia frente a incidentes graves o desastres naturales.	A(X) D( ) **SUGERENCIAS:**
13	- El personal del área de sistemas tiene asesoramiento especializado en materia de seguridad informática.	A(X) D( ) **SUGERENCIAS:**
	PROMEDIO OBTENIDO:	A( ) D( )

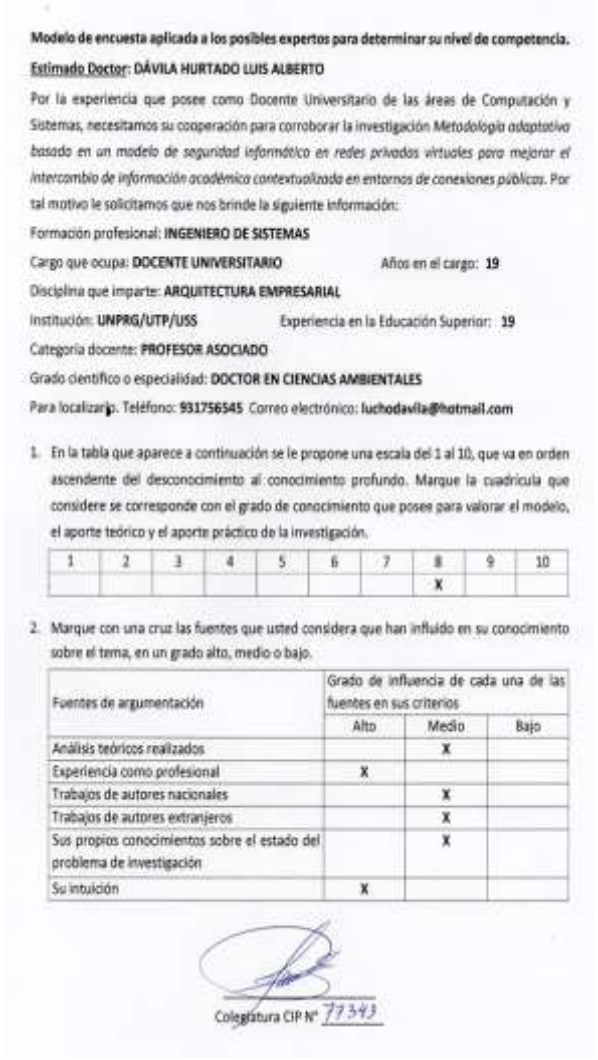
6. COMENTARIOS GENERALES

Instrumento bien elaborado

7. OBSERVACIONES

Dr. Collantes Santisteban, Luis Jaime
Juez Experto
Colegiatura CIP N° 184937

Anexo 8. Modelo de encuesta aplicada a posibles expertos para determinar su nivel de competencia



Modelo de encuesta aplicada a los posibles expertos para determinar su nivel de competencia.

Estimado Doctor: DÁVILA HURTADO LUIS ALBERTO

Por la experiencia que posee como Docente Universitario de las áreas de Computación y Sistemas, necesitamos su cooperación para corroborar la investigación *Metodología adaptativa basada en un modelo de seguridad informático en redes privadas virtuales para mejorar el intercambio de información académico contextualizada en entornos de conexiones públicas*. Por tal motivo le solicitamos que nos brinde la siguiente información:

Formación profesional: **INGENIERO DE SISTEMAS**

Cargo que ocupa: **DOCENTE UNIVERSITARIO** Años en el cargo: **19**

Disciplina que imparte: **ARQUITECTURA EMPRESARIAL**

Institución: **UNPRG/UTP/USS** Experiencia en la Educación Superior: **19**

Categoría docente: **PROFESOR ASOCIADO**

Grado científico o especialidad: **DOCTOR EN CIENCIAS AMBIENTALES**

Para localizarlo. Teléfono: **931756545** Correo electrónico: **luchodavila@hotmail.com**

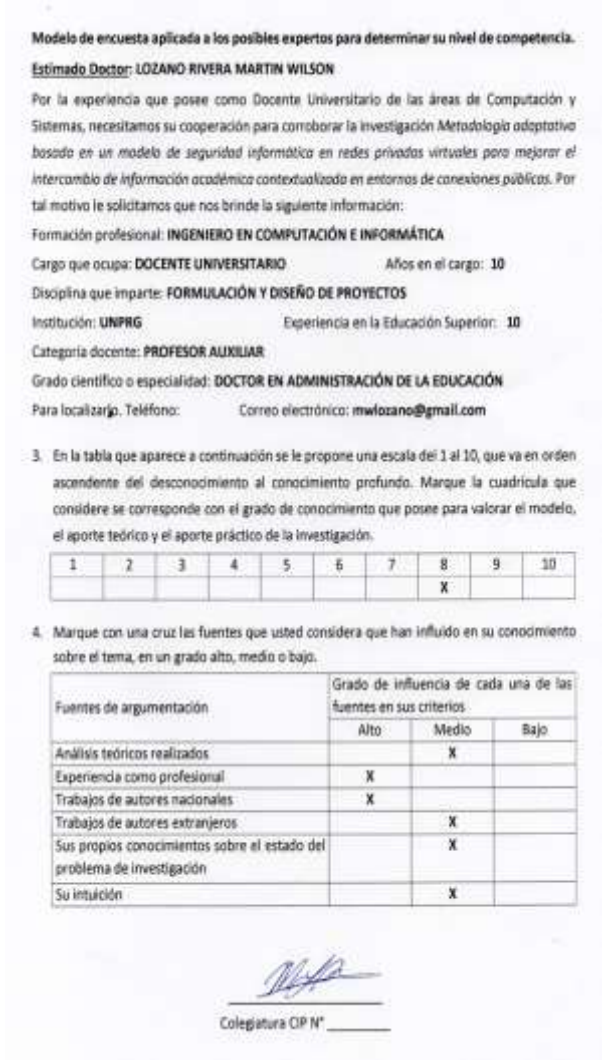
1. En la tabla que aparece a continuación se le propone una escala del 1 al 10, que va en orden ascendente del desconocimiento al conocimiento profundo. Marque la cuadrícula que considere se corresponde con el grado de conocimiento que posee para valorar el modelo, el aporte teórico y el aporte práctico de la investigación.

1	2	3	4	5	6	7	8	9	10
							X		

2. Marque con una cruz las fuentes que usted considera que han influido en su conocimiento sobre el tema, en un grado alto, medio o bajo.

Fuentes de argumentación	Grado de influencia de cada una de las fuentes en sus criterios		
	Alto	Medio	Bajo
Análisis teóricos realizados		X	
Experiencia como profesional	X		
Trabajos de autores nacionales		X	
Trabajos de autores extranjeros		X	
Sus propios conocimientos sobre el estado del problema de investigación		X	
Su intuición	X		

Colegiatura CIP N° 77343



Modelo de encuesta aplicada a los posibles expertos para determinar su nivel de competencia.

Estimado Doctor: LOZANO RIVERA MARTIN WILSON

Por la experiencia que posee como Docente Universitario de las áreas de Computación y Sistemas, necesitamos su cooperación para corroborar la investigación *Metodología adaptativa basada en un modelo de seguridad informático en redes privadas virtuales para mejorar el intercambio de información académico contextualizada en entornos de conexiones públicas*. Por tal motivo le solicitamos que nos brinde la siguiente información:

Formación profesional: **INGENIERO EN COMPUTACIÓN E INFORMÁTICA**

Cargo que ocupa: **DOCENTE UNIVERSITARIO** Años en el cargo: **10**

Disciplina que imparte: **FORMULACIÓN Y DISEÑO DE PROYECTOS**

Institución: **UNPRG** Experiencia en la Educación Superior: **10**

Categoría docente: **PROFESOR AUXILIAR**

Grado científico o especialidad: **DOCTOR EN ADMINISTRACIÓN DE LA EDUCACIÓN**

Para localizarlo. Teléfono: Correo electrónico: **mwlozano@gmail.com**

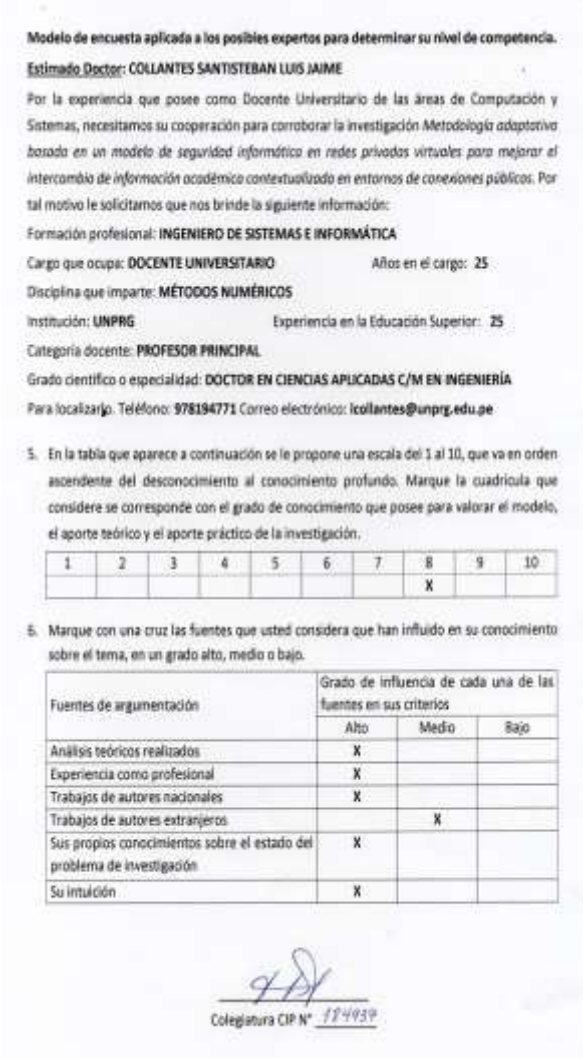
3. En la tabla que aparece a continuación se le propone una escala del 1 al 10, que va en orden ascendente del desconocimiento al conocimiento profundo. Marque la cuadrícula que considere se corresponde con el grado de conocimiento que posee para valorar el modelo, el aporte teórico y el aporte práctico de la investigación.

1	2	3	4	5	6	7	8	9	10
							X		

4. Marque con una cruz las fuentes que usted considera que han influido en su conocimiento sobre el tema, en un grado alto, medio o bajo.

Fuentes de argumentación	Grado de influencia de cada una de las fuentes en sus criterios		
	Alto	Medio	Bajo
Análisis teóricos realizados		X	
Experiencia como profesional	X		
Trabajos de autores nacionales	X		
Trabajos de autores extranjeros		X	
Sus propios conocimientos sobre el estado del problema de investigación		X	
Su intuición		X	

Colegiatura CIP N° _____



Modelo de encuesta aplicada a los posibles expertos para determinar su nivel de competencia.

Estimado Doctor: COLLANTES SANTISTEBAN LUIS JAIME

Por la experiencia que posee como Docente Universitario de las áreas de Computación y Sistemas, necesitamos su cooperación para corroborar la investigación *Metodología adaptativa basada en un modelo de seguridad informático en redes privadas virtuales para mejorar el intercambio de información académico contextualizada en entornos de conexiones públicas*. Por tal motivo le solicitamos que nos brinde la siguiente información:

Formación profesional: **INGENIERO DE SISTEMAS E INFORMÁTICA**

Cargo que ocupa: **DOCENTE UNIVERSITARIO** Años en el cargo: **25**

Disciplina que imparte: **MÉTODOS NUMÉRICOS**

Institución: **UNPRG** Experiencia en la Educación Superior: **25**

Categoría docente: **PROFESOR PRINCIPAL**

Grado científico o especialidad: **DOCTOR EN CIENCIAS APLICADAS C/M EN INGENIERÍA**

Para localizarlo. Teléfono: **978194771** Correo electrónico: **lcollantes@unprg.edu.pe**

5. En la tabla que aparece a continuación se le propone una escala del 1 al 10, que va en orden ascendente del desconocimiento al conocimiento profundo. Marque la cuadrícula que considere se corresponde con el grado de conocimiento que posee para valorar el modelo, el aporte teórico y el aporte práctico de la investigación.

1	2	3	4	5	6	7	8	9	10
							X		

6. Marque con una cruz las fuentes que usted considera que han influido en su conocimiento sobre el tema, en un grado alto, medio o bajo.

Fuentes de argumentación	Grado de influencia de cada una de las fuentes en sus criterios		
	Alto	Medio	Bajo
Análisis teóricos realizados	X		
Experiencia como profesional	X		
Trabajos de autores nacionales	X		
Trabajos de autores extranjeros		X	
Sus propios conocimientos sobre el estado del problema de investigación	X		
Su intuición	X		

Colegiatura CIP N° 114939

Modelo de encuesta aplicada a los posibles expertos para determinar su nivel de competencia.

Estimado Doctor: RAMOS MOSCOL MARIO FERNANDO

Por la experiencia que posee como Docente Universitario de las áreas de Computación y Sistemas, necesitamos su cooperación para corroborar la investigación *Metodología adaptativa basado en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas*. Por tal motivo le solicitamos que nos brinde la siguiente información:

Formación profesional: **INGENIERO INDUSTRIAL**

Cargo que ocupa: **DOCENTE UNIVERSITARIO** Años en el cargo: **40**

Disciplina que imparte: **REDES Y COMUNICACIONES DE DATOS**

Institución: **UNP/USS/USP** Experiencia en la Educación Superior: **40**

Categoría docente: **PROFESOR PRINCIPAL**

Grado científico o especialidad: **MAGISTER EN INFORMÁTICA / DOCTOR EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES**

Para localizarlo. Teléfono: **950859098** Correo electrónico: **mframosm@yahoo.com.ar**

7. En la tabla que aparece a continuación se le propone una escala del 1 al 10, que va en orden ascendente del desconocimiento al conocimiento profundo. Marque la cuadrícula que considere se corresponde con el grado de conocimiento que posee para valorar el modelo, el aporte teórico y el aporte práctico de la investigación.

1	2	3	4	5	6	7	8	9	10
								X	

8. Marque con una cruz las fuentes que usted considera que han influido en su conocimiento sobre el tema, en un grado alto, medio o bajo.

Fuentes de argumentación	Grado de influencia de cada una de las fuentes en sus criterios		
	Alto	Medio	Bajo
Análisis teóricos realizados		X	
Experiencia como profesional	X		
Trabajos de autores nacionales		X	
Trabajos de autores extranjeros		X	
Sus propios conocimientos sobre el estado del problema de investigación	X		
Su intuición	X		

Colegiatura CIP N° 30517

Modelo de encuesta aplicada a los posibles expertos para determinar su nivel de competencia.

Estimado Doctor: SAMILLAN AYALA ALBERTO ENRIQUE

Por la experiencia que posee como Docente Universitario de las áreas de Computación y Sistemas, necesitamos su cooperación para corroborar la investigación *Metodología adaptativa basado en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas*. Por tal motivo le solicitamos que nos brinde la siguiente información:

Formación profesional: **INGENIERO DE COMPUTACIÓN Y SISTEMAS**

Cargo que ocupa: **DOCENTE UNIVERSITARIO** Años en el cargo: **20**

Disciplina que imparte: **GESTIÓN DE PROYECTOS INFORMÁTICOS**

Institución: **UNP/USS/USP** Experiencia en la Educación Superior: **40**

Categoría docente: **PROFESOR PRINCIPAL**

Grado científico o especialidad: **MAGISTER EN INFORMÁTICA / DOCTOR EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES**

Para localizarlo. Teléfono: **950859098** Correo electrónico: **mframosm@yahoo.com.ar**

9. En la tabla que aparece a continuación se le propone una escala del 1 al 10, que va en orden ascendente del desconocimiento al conocimiento profundo. Marque la cuadrícula que considere se corresponde con el grado de conocimiento que posee para valorar el modelo, el aporte teórico y el aporte práctico de la investigación.

1	2	3	4	5	6	7	8	9	10
						X			

10. Marque con una cruz las fuentes que usted considera que han influido en su conocimiento sobre el tema, en un grado alto, medio o bajo.

Fuentes de argumentación	Grado de influencia de cada una de las fuentes en sus criterios		
	Alto	Medio	Bajo
Análisis teóricos realizados		X	
Experiencia como profesional		X	
Trabajos de autores nacionales		X	
Trabajos de autores extranjeros			X
Sus propios conocimientos sobre el estado del problema de investigación		X	
Su intuición		X	

Colegiatura CIP N° 57150

Anexo 9. Validación de los aportes de la investigación a través de la selección de expertos

ENCUESTA A EXPERTOS

Estimado Doctor: LUIS ALBERTO DÁVILA HURTADO

Ha sido seleccionado en calidad de experto con el objetivo de valorar la pertinencia de la *Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas*. Las interrogantes están en función de evaluar la pertinencia científico-metodológica de la aplicación de los aportes teórico y práctico.

Datos del experto:

Profesión	Ingeniero de Sistemas
Grado Científico	Doctor en Ciencias Ambientales
Años de Experiencia	19
Entidad donde labora	Universidad Nacional Pedro Ruíz Gallo
Cargo	Catedrático

Datos de la investigación:

Titulo	Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas
Línea	Redes y Sistemas Distribuidos
Aporte Teórico	Modelo de seguridad informática en redes privadas virtuales
Aporte Práctico	Metodología adaptativa para la implementación del modelo de seguridad informática en redes privadas virtuales

1. Novedad científica del modelo de seguridad informática en redes privadas virtuales.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

2. Pertinencia de los fundamentos teóricos del modelo de seguridad informática en redes privadas virtuales.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

3. Nivel de argumentación de las relaciones fundamentales aportadas en el modelo de seguridad informática.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

4. Nivel de correspondencia entre el aporte teórico (modelo de seguridad informática) y el aporte práctico (metodología para redes privadas virtuales) de la investigación.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

5. Claridad en la finalidad de cada una de las acciones de la metodología para redes privadas virtuales propuesta.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

6. Posibilidades de aplicación de Metodología adaptativa para la implementación del modelo de seguridad informática en redes privadas virtuales propuesto.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

7. Concepción general de la metodología según sus acciones para la mejora en el intercambio de información académica contextualizada.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

8. Significación práctica de la metodología en el intercambio de información académica contextualizada.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Observaciones generales: ----------

Colegiatura CIP N° 77343

ENCUESTA A EXPERTOS

Estimado Doctor: MARIO FERNANDO RAMOS MOSCOL

Ha sido seleccionado en calidad de experto con el objetivo de valorar la pertinencia de la *Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas*. Las interrogantes están en función de evaluar la pertinencia científico-metodológica de la aplicación de los aportes teórico y práctico.

Datos del experto:

Profesión	Ingeniero Industrial
Grado Científico	Magister en Informática / Doctor en Tecnologías de la Información y Comunicaciones
Años de Experiencia	40
Entidad donde labora	Universidad Nacional de Piura
Cargo	Catedrático

Datos de la investigación:

Titulo	Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas
Línea	Redes y Sistemas Distribuidos
Aporte Teórico	Modelo de seguridad informática en redes privadas virtuales
Aporte Práctico	Metodología adaptativa para la implementación del modelo de seguridad informática en redes privadas virtuales

1. Novedad científica del modelo de seguridad informática en redes privadas virtuales.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

2. Pertinencia de los fundamentos teóricos del modelo de seguridad informática en redes privadas virtuales.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

3. Nivel de argumentación de las relaciones fundamentales aportadas en el modelo de seguridad informática.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

4. Nivel de correspondencia entre el aporte teórico (modelo de seguridad informática) y el aporte práctico (metodología para redes privadas virtuales) de la investigación.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

5. Claridad en la finalidad de cada una de las acciones de la metodología para redes privadas virtuales propuesta.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

6. Posibilidades de aplicación de Metodología adaptativa para la implementación del modelo de seguridad informática en redes privadas virtuales propuesto.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

7. Concepción general de la metodología según sus acciones para la mejora en el intercambio de información académica contextualizada.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

8. Significación práctica de la metodología en el intercambio de información académica contextualizada.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Observaciones generales: ----------

Colegiatura CIP N° 30517

ENCUESTA A EXPERTOS

Estimado Doctor: LUIS JAIME COLLANTES SANTISTEBAN

Ha sido seleccionado en calidad de experto con el objetivo de valorar la pertinencia de la *Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas*. Las interrogantes están en función de evaluar la pertinencia científico-metodológica de la aplicación de los aportes teórico y práctico.

Datos del experto:

Profesión	Ingeniero de Sistemas e Informático
Grado Científico	Doctor en Ciencias Aplicadas con mención en Ingeniería
Años de Experiencia	28
Entidad donde labora	Universidad Nacional Pedro Ruíz Gallo
Cargo	Catedrático

Datos de la investigación:

Titulo	Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas
Línea	Redes y Sistemas Distribuidos
Aporte Teórico	Modelo de seguridad informática en redes privadas virtuales
Aporte Práctico	Metodología adaptativa para la implementación del modelo de seguridad informática en redes privadas virtuales

1. Novedad científica del modelo de seguridad informática en redes privadas virtuales.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

2. Pertinencia de los fundamentos teóricos del modelo de seguridad informática en redes privadas virtuales.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

3. Nivel de argumentación de las relaciones fundamentales aportadas en el modelo de seguridad informática.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

4. Nivel de correspondencia entre el aporte teórico (modelo de seguridad informática) y el aporte práctico (metodología para redes privadas virtuales) de la investigación.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

5. Claridad en la finalidad de cada una de las acciones de la metodología para redes privadas virtuales propuesta.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

6. Posibilidades de aplicación de Metodología adaptativa para la implementación del modelo de seguridad informática en redes privadas virtuales propuesto.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

7. Concepción general de la metodología según sus acciones para la mejora en el intercambio de información académica contextualizada.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

8. Significación práctica de la metodología en el intercambio de información académica contextualizada.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Observaciones generales: ----------

Colegiatura CIP N° 184937

Anexo 10. Identificación de usuarios

Anexo 11. Servicios de red