UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

INFORME CIENTÍFICO

TEMA:

"SISTEMA DE GESTIÓN DE SEGURIDAD PERIMETRAL PARA LA RED DE DISTRIBUCIÓN Y ACCESO DE LA COOPERATIVA DE AHORRO Y CRÉDITO ESCENCIA INDÍGENA LTDA. IBARRA, BASADO EN LA NORMA ISO 27002:2013"

AUTOR: KARINA ESTEFANÍA QUILCA BURGOS

DIRECTOR: ING. DIEGO TREJO

IBARRA, ECUADOR

2016

“Sistema de gestión de seguridad perimetral para la red de distribución y acceso de la Cooperativa de Ahorro y Crédito Escencia Indígena Ltda. Ibarra, basado en la norma ISO 27002:2013” (Abril 2016)

Autor: Quilca, K. karo keqb2890@hotmail.com
Director: Mgs. Trejo D. djtrejo@utn.edu.ec

Resumen— *Este proyecto presenta un sistema de gestión de seguridad perimetral para la red de distribución y acceso de la Cooperativa de Ahorro y Crédito Escencia Indígena Ltda. Ibarra, basado en la norma ISO 27002:2013.El mismo que se compone de un manual de políticas y buenas prácticas de seguridad dirigido a todos los funcionarios de la empresa, la implementación de un firewall, IDS/IPS y una zona desmilitarizada (DMZ), lo cual se logró gracias a la implementación y configuración de un equipo de tecnología UTM gateprotect GPA 500 con lo cual la empresa adquirirá un mejor desempeño en sus actividades de negocio.*

Índice de Términos—DMZ, IDS/IPS, UTM

I. INTRODUCCIÓN

La Cooperativa de ahorro y crédito Escencia Indígena es una empresa financiera de carácter privada creada por un grupo de personas emprendedoras de la provincia de Imbabura y Tungurahua el 19 de mayo del 2007. Dispone de un grupo de servidores (base de datos, ventanilla móvil, facilito, APP ventanillas, intranet, etc. Ubicados en la agencia Ibarra la cual se desempeña como matriz y desde allí se distribuyen y controlan los servicios y aplicaciones al resto de agencias ubicadas en las distintas ciudades del país. (Castañeda, 2013b)

II. ANÁLISIS DE LA SITUACIÓN ACTUAL

En la actualidad existen diferentes metodologías para el análisis de riesgos de la seguridad de la información de una entidad pública o privada. En vista de que en la ISO/IEC 27002:2013 no se especifica ninguna metodología; para este estudio se seleccionó la metodología OSSTMM (Manual de la metodología abierta de testeo de seguridad) debido a las ventajas que esta ofrece.

Esta metodología abarca toda la seguridad operativa basada en diferentes áreas o canales como lo describe el manual, y se muestra en la Figura 1:

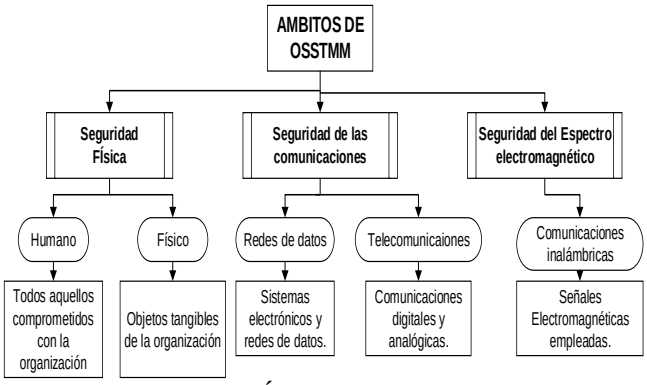

Figura 1: Ámbitos de OSSTMM
Fuente: (Valdez Alvarado, 2013)

La forma más simple para hacer RAVs es usar las hojas de cálculo creadas específicamente para calcular el área de ataque y varias métricas requeridas a partir de los datos de prueba. Esta hoja de cálculo se encuentra disponible en el sitio web de ISECOM. El analista sólo necesita introducir los valores en las cajas blancas vacías, y el resto de los cálculos se manejará de forma automática (Herzog, 2003).

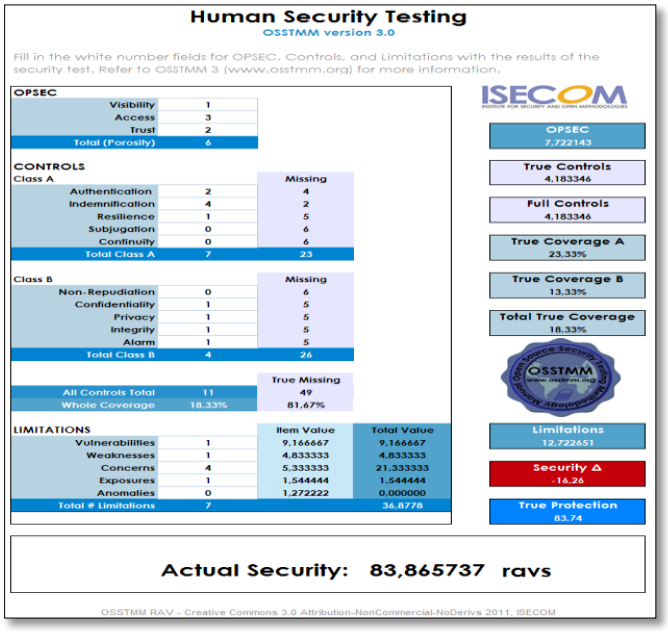

Figura 2: Cálculo del RAVS en Canal Humano.
Fuente: Obtenida de Calculadora de RAVs OSSTMM 3.0

A. Canal Humano

El análisis de seguridad en este canal, se realizó a nivel de acceso y confianza que éste entrega a la seguridad de la información. Para lo cual se realizó pruebas de observación directa y de ingeniería social, con lo que se obtuvo información muy valiosa la cual compromete la seguridad de la información de la empresa.

El resultado obtenido refleja acorde a los parámetros de la metodología que la seguridad operacional es considerablemente baja, reflejada en la falta de manuales de normas y buenas prácticas del correcto uso de la información actualmente implementadas por la administración.

Se tiene un grado de prioridad alto en cuanto a la indemnización del personal, más no así en otros controles que son totalmente nulos como la Subyugación y la Continuidad.

B. Canal Físico

La evaluación de seguridad en el canal físico, fue enfocada al nivel de acceso al cuarto de equipos, a la disponibilidad de los dispositivos, y sobre todo a la respuesta ante eventualidades del mismo.

Al realizar el test de seguridad física y analizar los controles existentes se determinó que lamentablemente no se tiene implementados algunos controles de seguridad física los mismos que resultan un blanco perfecto para los atacantes informáticos.

C. Canal de Telecomunicaciones

La evaluación de seguridad en este canal, se realizó un escaneo de puertos, con la ayuda del software Zenmap, dejando en evidencia el nivel de acceso que se tiene a las aplicaciones.

Los resultados obtenidos se reflejan acorde a los parámetros de la metodología y de determinó que se tienen únicamente controles de Indemnización, autenticación y privacidad; los demás controles son nulos; abriendo una brecha para la inseguridad de la información.

Las limitaciones se valoran individualmente pero están relacionadas con algunos controles y seguridad operacional, debido a que los valores en seguridad operacional son altos, el cálculo de las limitaciones también lo es. Por lo tanto resaltan limitaciones como las Vulnerabilidades, debilidades y exposiciones las mismas que reflejan una administración no adecuada que expone a la red a ciertas amenazas informáticas.

D. Canal de Datos

Tiene como objetivo monitorear los datos de entrada y salida de la red de comunicaciones a través de web, mensajería instantánea, chat, foros de discusión basados en la Web, o por e-mail, con la finalidad de verificar si consigo traen códigos maliciosos, conductas inapropiadas.

Los resultados obtenidos se reflejan acorde a los parámetros de la metodología y de determinó que La seguridad operacional es muy alta, principalmente en el aspecto de confianza, en el que se ha considerado todos los puertos que están abiertos. Esto refleja la importancia que se le ha dado a la seguridad de las telecomunicaciones

De acuerdo al test realizado, se constató que se tienen únicamente controles de Indemnización, autenticación y privacidad; mientras tanto los demás controles son nulos; dando lugar a la inseguridad de la información.

III. DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD PERIMETRAL

Se diseñó el sistema de seguridad tanto a nivel de acceso como a nivel de distribución. A nivel de acceso se concientizó a los usuarios y

administradores de los activos informáticos de la empresa mediante la creación de un manual de políticas de seguridad basado en los controles de la norma ISO/IEC 27002. A nivel de distribución se implementó un equipo gateprotect GPA 500 que cumple las funciones de Firewall, IDS/IPS además permitió la configuración de una zona desmilitarizada.

A. Políticas de Seguridad

Una vez identificados los riegos de seguridad, se seleccionaron controles que garanticen su reducción hasta un nivel aceptable; tomando en consideración que ningún conjunto de controles puede lograr la seguridad completa. Se propone crear una guía de políticas y buenas prácticas con el objetivo mejorar la gestión de la seguridad de la información, así como también concientizar a los funcionarios y administradores de los activos de información en el buen uso de los mismos.

El manual de políticas y buenas práctica de seguridad se realizó en base a la Norma NTE INEN-ISO/IEC 27002:3013; la misma que establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información.

Los dominios seleccionados fueron:

1. Políticas de la seguridad
2. Aspectos organizativos de la seguridad de la información.
3. Seguridad ligada a los recursos humanos.
4. Gestión de activos
5. Control del acceso
6. Cifrado
7. Seguridad física y ambiental
8. Seguridad en la operative
9. Seguridad en las telecomunicaciones
10. Adquisición, desarrollo y mantenimiento de los sistemas de información
11. Relaciones con suministradores
12. Gestión de incidentes en la seguridad de la información
13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
14. Cumplimiento

B. Topología

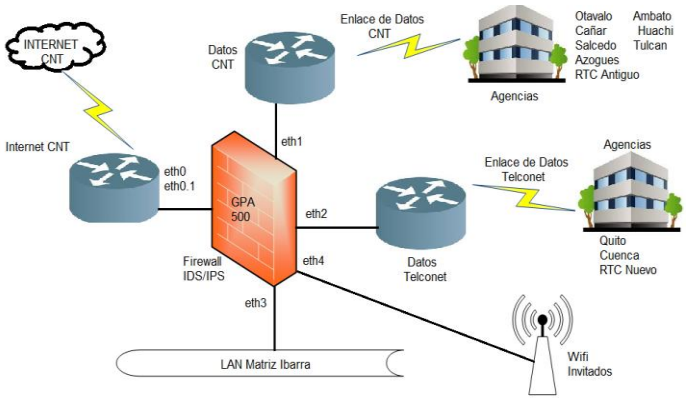

Figura 3: Diseño de seguridad perimetral.
Fuente: Desarrollo del proyecto

Las Amenazas de Seguridad son cada día más complejas y peligrosas, además, causan pérdidas y altos costos a las empresas. Los productos que integran soluciones efectivas contra esas amenazas son sistemas cuyo funcionamiento es difícil de entender y administrar y requiere demasiada atención y tiempo por parte de los encargados de TI, lo cual se vuelve un problema ante el incremento constante de las labores de ese departamento. Esto inevitablemente aumenta la posibilidad y el riesgo de errores por parte de los usuarios, errores de configuración y funcionamiento en los sistemas, errores que actualmente representan más del 90% de las vulnerabilidades y brechas en la seguridad perimetral en las empresas.

No se consideró optar por una solución por software libre debido a la carga laboral que dispone el área de sistemas. Debido a que una solución por software libre no brinda la integración de servicios y su administración, monitoreo y mantenimiento es más complicado ya que en la mayoría de los casos se tiene que realizar vía consola y utilizar procesos más complicados y que implican más tiempo hasta poder determinar fallas y errores en el sistema.

TABLA 1
COMPARACIÓN DE SOLUCIONES

Característica	Gateprotect GPA 500	Software Libre
Puertos GbE	Dispone de 6 puertos	Necesita al menos 3 tarjetas de red
Prestaciones	Firewall, DMZ, IDP/IPS, Filtro de virus, filtrado web, detección de spam, IPSec/SSL, VLANs, VPN, QoS, Balanceo de carga.	Requiere configurar servidores por separado
Rendimiento de Firewall (MBit/s)	2100	Dependiente del sistema operativo
Exposición a vulnerabilidades	Muy reducidas	Propias del sistema operativo y de configuraciones incorrectas.
Costos	Por licenciamiento con soporte incluido.	Costo de aprendizaje, de instalación, de migración, de interoperabilidad.
Modo de operación	Amigable con el usuario o administrador	Complejo

Fuente: Desarrollo de proyecto

C. Solución Perimetral

Como primer paso a realizar es la instalación del firmware del equipo firewall para poder acceder a todas las bondades que este equipo ofrece.

Posteriormente se ingresa todos los objetos que conforman la red de la empresa con sus respectivas configuraciones y se obtiene una topología como se muestra en la Figura 4. Esta está dividida en dos áreas:

La primera (izquierda) permite el acceso a redes de agencias y proveedores de servicios como: servidor de base de datos conectado mediante una VPN al servidor Fitbank, también está la VPN entre la red LAN (Ibarra) y el servidor Conecta y la conexión wifi conectado con la otra área.

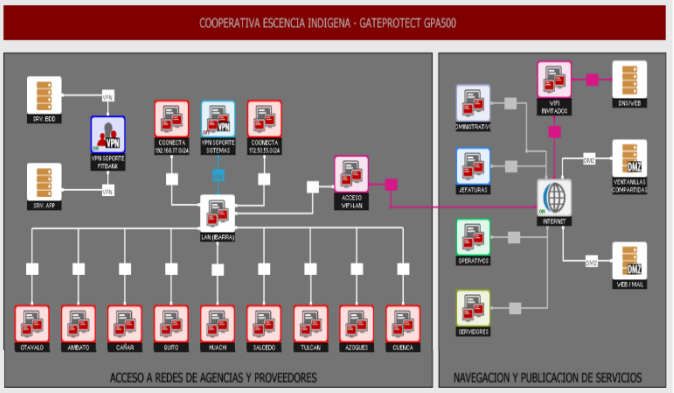

Figura 4: Diagrama de red de la empresa.
Fuente: Obtenido de administrador GPA500

La segunda área permite la navegación y publicación de servicios. Esta área contiene los siguientes objetos: servidores (propios de la empresa), jefaturas, operarios, DMZ, Wifi invitados.

Para la DMZ se han considerado los servidores web, correo electrónico y servidor de ventanillas.

Para configurar el IDS/IPS el Firewall gateprotect usa perfiles. Cada perfil puede ser ajustado y asignado a una interface de red. Las reglas de un perfil pueden ser ajustadas a distintos estados.

El IPS ofrece 5 estados diferentes, DISABLE, LOG, DROP, DROP_LOG y REJECT para configurar reglas individualmente, el IDS tiene dos estados diferentes, LOG y DISABLE. Los estados definen el tráfico que se apareja con las reglas

El IDS/IPS solo produce reportes de alarma si se registran ataques en las direcciones de IP de un grupo determinado de computadores.

El Sistema de detección de intrusos monitorea sistemas de computación especiales o redes, ej. un servidor de red, un servidor de correo o un DMZ en particular.

IV. PRUEBAS DE FUNCIONAMIENTO

1. Estadística de bloqueos

En la barra de herramientas Se puede usar la barra de herramientas en las Estadísticas de Cliente para:

Imprimir las estadísticas, Cambiar el idioma de Estadísticas de Cliente para menú y uso, Obtener información sobre Estadísticas de cliente, Finalizar Estadísticas de Cliente.

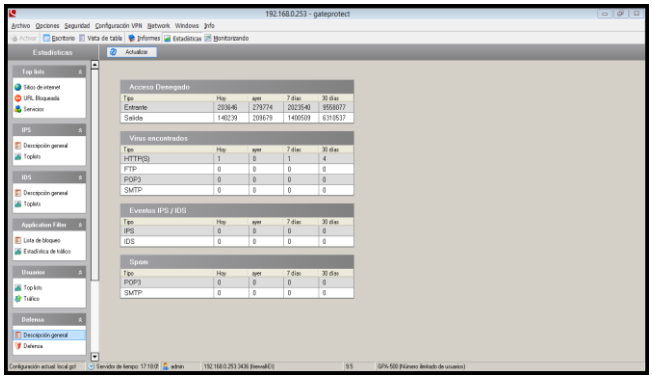

Figura 5: Estadísticas de bloqueos.
Fuente: Obtenido de administrador GPA500

Se pueden filtrar los resultados exhibidos dependiendo de la información de estadísticas preparada en la parte superior de la ventana de estadísticas:

Escritorio: red completa, usuarios o computadores

Período: 6, 12 o 24 horas, 7 o 14 días, 1, 3 o 12 meses

Período de auto-definición con fecha y hora para inicio y término

Ventana de tiempo: cualquier hora del día con inicio y fin

Acceso bloqueado: ingreso o salida

2. Intento de acceso a página bloqueada, acceso denegado correctamente.

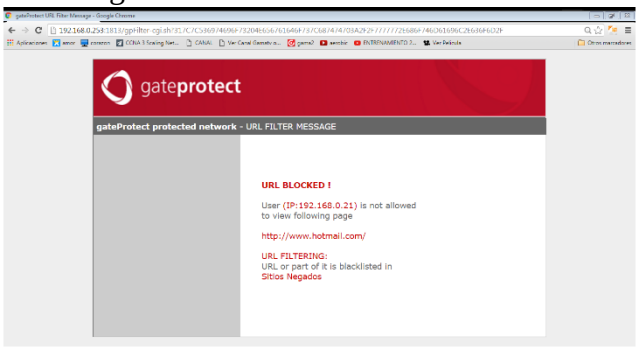

Figura 6: Acceso denegado.
Fuente: Obtenido de administrador GPA500

V. ANÁLISIS DE COSTOS

A. Costos de equipamiento

En este punto se detalla el valor de los equipos necesarios para la implementación de este diseño descritos en la Tabla 2. El análisis se basó, en los equipos disponibles en el mercado nacional, las marcas más utilizadas y los precios referenciales de las mismas.

TABLA 2
COSTO DE EQUIPOS

COSTOS EQUIPAMIENTO			
EQUIPAMIENTO	CANTIDAD	PRECIO	
		COSTO UNITARIO	SUBTOTAL
GATEPROTECT GPA 500	1	$ 4.032,00	$ 4.032,00
PC CLIENTE	1	$ 300.00	$ 300,00
TOTAL			**$ 4.332,00**

Fuente: Proforma empresa SMART HELP SOLUCIONES

B. Costos de Ingeniería

En los costos de ingeniería se considera el costo del servicio de instalación y configuración del equipo mostrados en la Tabla 3.

TABLA 3
COSTO INGENIERIA

COSTOS INGENIERIA			
EQUIPAMIENTO	CANTIDAD	PRECIO	
		COSTO UNITARIO	SUBTOTAL
Diseño del sistema de seguridad	1	$ 400,00	$ 400,00
Instalación y configuración	1	$ 100,00	$ 100,00
TOTAL			**$ 500,00**

Fuente: Proforma empresa SMART HELP SOLUCIONES

C. Costo total del sistema de seguridad

TABLA 4
COSTO TOTAL

COSTOS TOTALES DE SEGURIDAD			
DESCRIPCIÓN	UNIDAD	CANT	TOTAL
EQUIPAMIENTO	u	1	$4.332,00
INGENIERIA	u	1	$ 500,00
TOTAL			**$4.832,00**

Fuente: Desarrollo del proyecto

La implementación de este proyecto tiene un valor

4032 dólares debido a que la pc para la administración ya contaba la empresa y el valor de ingeniería fue parte del desarrollo del proyecto.

El beneficio que obtiene la empresa además de los ya mencionados es que al adquirir esta solución es que al no optar por esta solución y haber optado por servidores independientes sean estos de software libre era necesario contratar una persona encargada de los servidores de seguridad perimetral ya que la carga para el departamento de sistemas es demasiada. Con esto al contratar un empleado con un sueldo mínimo de 600 dólares en los 12 meses que dura la licencia del equipo se tendría una inversión de 7200 dólares exponiéndose a fallos ya que los sistemas no resultan tan robustos como lo es la solución de gateprotect. Con la solución planteada se tiene segura la infraestructura tecnológica de la empresa y aumenta su productividad basado en tres puntos clave: reducción de tiempo, reducción de errores y reducción de costos.

VI. Conclusiones

Conocer la infraestructura tecnológica de la empresa y las entrevistas con el administrador de la infraestructura tecnológica de la empresa fue el primer paso para desarrollar el proyecto ya que esto permitió conocer los riesgos y debilidades.

La norma ISO IEC/27002:2013 no establece una metodología de análisis y gestión de riesgos informáticos, pero recomienda elegir una metodología que más se relacione con las necesidades y características de la entidad a analizar.

El análisis de riegos se realizó en base a los canales y parámetros descritos en el manual de la metodología abierta de testeo de seguridad (OSSTMM), mediante la cual se determinó el nivel de riegos al que estaba expuesta la empresa.

El análisis de riesgos realizado en la COAC “Escencia Indígena” permitió mitigar, eliminar o transferir el riesgo de las fallas que afectaban el rendimiento de la red; entre las cuales se pudo destacar la inseguridad y mal estado de su cuarto de equipos.

El manual de políticas de seguridad de la información es el documento más importante en el que se basa la toma de decisiones y acciones a emprender en temas de seguridad, ninguna normativa interna o procedimiento está sobre la política y cualquier violación a la misma deberá ser sancionada conforme al reglamento interno considerando el análisis que si el daño es muy grave se debe adoptar medidas severas.

Se ubicaron los servidores web y mail en una zona desmilitarizada DMZ con el fin de permitir las conexiones tanto desde la red interna como de la externa, mientras que las conexiones que parten de la DMZ solo sean posibles con la red local.

El equipo gateProtect 500 integra varios servicios de seguridad como es: firewall, DMZ, IDS/IPS además de control de spam, antivirus, proxy y otros lo cual le convierte en una solución integral al momento de proteger una red.

Mediante el análisis de costos realizado se determinó que utilizar el equipo gateprotect GPA 500 es lo más conveniente para garantizar la estabilidad y continuidad del negocio; ya que este equipo proporciona las mejores características en cuanto aseguramiento de redes perimetrales.

Después de realizar la comparación entre una solución con software libre y la del equipo GPA 500 se observó que se tiene un mayor ahorro de costos en lo referente a la capacitación, instalación y administración que requiere la solución por software libre.

Al implementar esta solución la empresa tendrá mayor estabilidad y control de su red; es decir ya no existirá tanta congestión y perdidas de conexión por lo que la atención a sus clientes o socios será más rápida y eficiente que anteriormente lo cual representa un aumento en su productividad y desarrollo empresarial.

REFERENCIAS

[1] DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA. (2015*). DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA. Obtenido de Definición de Fuerza bruta:* *http://www.alegsa.com.ar/Dic/fuerza%20bruta.php*.

[2] Castañeda, D. (2013). *Escencia Indígena*

[3] Erb, M. (2009). *Gestión de Riesgo en la Seguridad Informática. Obtenido de https://protejete.wordpress.com/gdr_principal/definicion_si/.*

[4] García, A., Hurtado, C., & Alegre, M. (2011). *Seguridad Informática. Madrid, España: Paraninfo*.

[5] Guijarro, Á. P. (2012). *Seguridad Perimetral. Obtenido de https://alvaroprimoguijarro.files.wordpress.com/2012/01/ud03_sad_alvaroprimoguijarro.pdf.*

[6] Herzog, P. (2003). *OSSTMM 2.1*.

[7] Herzog, P. (2003). *OSSTMM 3.0*.

[8] NTE INEN-ISO/IEC 27002. (2009). *Tecnología de la Información- Técnicas de la Seguridad - Código de Práctica para la Gestión de la Seguridad de la Información. Quito.*

[9] Superintendencia de Economía Popular y Solidaria. (2012). *REGLAMENTO A LA LEY ORGÁNICA DE LA ECONOMIA POPULAR Y SOLIDARIA.*

[10] Toth, G., & Sznek, J. (2014). Inplementación de la guía NIST SP800-30 mediante la utilizacion de OSSTMM. Neuquén.

[11] Valdez Alvarado, A. (2013). OSSTMM3. Analisis y Diseño de Sistemas de Información.

Bibliografía

Karina Estefanía Quilca Burgos

Nació en Ibarra el 28 de Mayo de 1990. Realizó sus estudios secundarios en el Colegio Técnico “Víctor Manuel Guzmán”, donde obtuvo el bachillerato en Informática.
En el 2008 ingresó a la Universidad Técnica del Norte como estudiante de pre-grado en la Carrera de Ingeniería Electrónica y Redes de Comunicación.