UNIVERSIDAD SANTO TOMAS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA

NUEVO PROXY PARA BANCO SCOTIABANK COLPATRIA

RODRIGO MENDOZA MESA

Mayo 2020

UNIVERSIDAD SANTO TOMAS

ESPECIALIZACION EN GESTION DE REDES DE DATOS

Proyecto Dirigido II

UNIVERSIDAD SANTO TOMAS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA

.

TABLA DE CONTENIDO

Tabla de contenido

INTRODUCCIÓN

El banco Scotiabank Colpatria tiene como visión convertirse en los próximos años en un banco digital y uno de los más grandes de la región, es por eso que la compra de un segmento del funcionamiento del banco City impulsó nuevos retos dentro del área de tecnología y seguridad de la información, de allí que la seguridad ha sido la principal premisa a tratar cuando la organización desea brindar el servicio de Internet a los nuevos empleados que llegan a formar parte del banco.

Los administradores de red y áreas de seguridad informática ven la necesidad de incrementar todo lo concerniente a la integridad de los sistemas y eficiencia en el tráfico de red de los mismos, debido a que se expone la información privada de los datos, así como la infraestructura de su red a posibles atacantes. Para superar estos planteamientos y proveer el nivel de protección requerida, se necesita seguir una política de seguridad a través del proxy para prevenir el acceso no autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la fuga de información sensible y privada.

En lo que respecta al tráfico de red, la mejora del proxy permitirá afrontar los retos que se generan y nacen de la integración, dando un gran servicio al funcionario interno que se verá reflejado en una buena atención al cliente externo y satisfacción general de sus aplicaciones y productos que se ofrecen.

Y por supuesto no podría faltar una razón importante que permite asegurar la red interna y permitir restringir el uso de internet solo al personal autorizado y a las páginas web autorizadas por el banco, teniendo un control eficaz y benéfico para todos

1. JUSTIFICACIÓN

De acuerdo con las metas estratégicas de la organización y su deseo de crecer y expandirse en el mercado bancario colombiano, Colpatria del grupo Scotiabank realiza la compra del segmento pyme y personas del banco City. Dicho cambio genera un gran impacto en la operación interna del banco tanto para los temas operativos y de oficinas como para el área de tecnología, ya que se requiere robustecer toda su infraestructura para soportar los nuevos clientes y los procesos internos del banco. Con base a lo anterior, uno de los retos que se presenta es soportar el tráfico de internet que generará los nuevos funcionarios, ya que muchas funciones dependen bastante de este servicio, pero ejerciendo un control en la navegación con políticas de seguridad que garanticen un buen uso del internet así como la mejora en la productividad laboral, porque los usuarios tendrán acceso a los sitios que se requieren por sus funciones, pero también se denegará aquellos sitios que no requieren en su labor, tales como redes sociales, juegos, deportes, etc.

Los cargos de entidades financieras que tengan un contacto directo con el cliente externo, es decir las áreas de caja, asesoría y personal de cobranza no pueden tener navegación a sitios públicos para prevenir la fuga de información y más aún la protección de los datos de sus clientes, de allí la importancia del proxy y control de contenido de la navegación en el banco. Como se puede ver en muchos escritos y regulaciones que resaltan la importancia de la protección y la seguridad de la información:

> Por otro lado, desde el punto de vista de la seguridad, es bien sabido que el acceso a internet es un vector de ataque utilizado por distintos software de tipo malicioso. Los usuarios acceden a páginas web de poca confianza y pueden infectar sus equipos. (*Mendoza & Panadero, 2019, p.9)*

El proxy no es solo brindar servicio de navegación sino que cumple un papel importante en la seguridad, ya que por allí se puede controlar el tráfico tanto hacia afuera, como el tráfico entrante que viene de internet y así prevenir ataques o fugas de información que pueden afectar notoriamente la reputación de la entidad, por lo que el control de contenido en la navegación es un hito importante en el proyecto de fusión planteado entre los 2 dominios del banco.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 SITUACION ACTUAL

El banco Colpatria cuenta con un dispositivo marca Fortinet modelo 3240C, el cuál cumple la función principal de proxy de navegación y control de contenido para todos los funcionarios actuales del banco, (aproximadamente 6 mil empleados), presentándose picos de consumo de memoria que alcanzan el 80% de la memoria actual del dispositivo en referencia.

Debido al anuncio de hace varios meses de la compra por parte de banco Colpatria del segmento pymes y Banca Personas del banco Citibank, la organización y su área de tecnología de seguridad se ve forzada a ampliar la capacidad de la mayoría de sus dispositivos. Es por eso que surge la necesidad de garantizar que los 2700 nuevos empleados que vienen del Citibank también tengan acceso a internet para el desarrollo de sus funciones y en vista que el actual dispositivo no tiene la capacidad para soportar los nuevos funcionarios, se requiere un nuevo equipo o solución que supla dicha tarea a cabalidad.

El nuevo dispositivo debe estar disponible en los próximos 4 meses, soportar el servicio de proxy y control de navegación para un total aproximado de 8700 empleados, asegurando y aplicando políticas respectivas que permitan la navegación solo a los sitios permitidos de acuerdo a la labor o función que cumplan dentro del banco. Adicionalmente el dispositivo debe tener la capacidad de permitir inspección profunda del tráfico https, así como control de DLP (Data Loss Prevention), Antivirus e IPS (Sistema de Prevención de Intrusos). Por lo tanto, debe ser un equipo robusto y que se ajuste a la arquitectura actual, pero que también pueda aplicar el control a 2 dominios de red diferentes, el actual Colpatria.com y el nuevo dominio Scotiabank.com.co.

Los controladores de dominio de ambas redes ya se encuentran en el mismo Forest y con la respectiva relación de confianza para que se puedan integrar.

De acuerdo a lo planteado y la problemática expuesta anteriormente, se plantea la siguiente pregunta:

¿El diseño de un nuevo sistema de proxy web permitirá garantizar la navegación a todos los funcionarios actuales y nuevos para la fusión Colpatria y Citibank?

3. GESTION

3.1 OBJETIVOS

3.1.1 Objetivo General

Diseñar un nuevo sistema de proxy web para dar navegación a los empleados actuales y los nuevos empleados de Scotiabank Colpatria.

3.1.2 Objetivos Específicos

- Integrar de manera eficiente la navegación de los 2 dominios de red del banco
- Establecer lineamientos de navegación para restringir sitios no autorizados a todos los funcionarios del banco.
- Diseñar políticas de control adicionales de DLP, IPS e inspección profunda para el tráfico de Internet en el proxy.

4. REQUERIMIENTOS

4.1 MARCO TEORICO

4.1.1 ANTECEDENTES

Dentro del desarrollo del presente proyecto, se ha encontrado la siguiente información que ayuda a definir como otros proyectos similares fueron implementados y dan una idea de cómo tramitar y gestionar dichas soluciones para beneficio de este.

1	**SISTEMA PROXY-WEB con FILTRADO y CONTROL DE ACCESO** Autor: MENDOZA FLOREZ Manuel Jesús y PANADERO MARTINEZ Javier Fecha de publicación: 09 jun 2019 http://openaccess.uoc.edu/webapps/o2/bitstream/10609/94506/6/ihocesmoralTFG0619memoria.pdf
	En este escrito los autores aportan el detalle técnico para diseñar e implementar una solución de Proxy y Filtrado Web, dando claridad sobre los componentes y dispositivos que trae la solución, como trabajan e interactúan para cumplir con el objetivo planteado de la navegación y su correcta gestión. Un gran aporte importante es la especificación de la arquitectura a utilizar y como se realiza el filtrado, analizando el tráfico y con implementación de balanceo de carga entre dispositivos, y se plantea como las diferentes marcas de equipos pueden soportar lo que se requiere para el proyecto con la mejor eficiencia y los mejores resultados.
2	**IMPLEMENTACIÓN DE UN SISTEMA PROXY DE NAVEGACION SEGURA EN EL GET DE CIENFUEGOS** AUTOR: Castellanos Hernández Juan Manuel y López Pérez Frank Manuel

	Fecha de publicación: 10 de marzo de 2018 Disponible en: http://revistas.unipamplona.edu.co/ojs_viceinves/index.php/RCTA/article/view/3332/1969
	Los ingenieros de hoy se enfrentan a nuevos retos y desarrollos en tecnología de punta, y si se requiere obtener navegación en internet en una entidad de manera segura y controlada, este artículo plasma como dar solución a través de un servidor proxy, el cual permitirá la conexión entre la red privada (interna) con el tráfico público (internet), para este proyecto por medio de herramientas libres que disminuyen su costo de implementación y licenciamiento, permitiendo eficiencia en la red, ya que contribuye a un mejor desempeño y seguridad de acceso ya que es realmente el proxy en que tiene la conexión a Internet y es la puerta principal para el tráfico entre la intranet y la extranet. Y de gran ayuda para ubicaciones pequeñas que no tienen gran cantidad de usuarios o peticiones para navegación.
3	**IMPLEMENTACION DE UN PROXY FIREWALL EN UNA RED CONSIDERANDO POLITICAS DE SEGURIDAD** Autor: NADER Mauricio José Fecha de publicación: 2011 Disponible en: https://www.academia.edu/25170216/implementacion_de_un_proxy_firewall_en_una_red_considerando_politicas_de_seguridad
	Importante para el proyecto que se desarrolla ya que se plasma como el autor presenta las ventajas y desventajas al implementar un proxy y como la variedad de políticas implementadas permite realizar un filtrado dinámico y eficiente.

	Un segundo punto a resaltar es como logra explicar el funcionamiento del firewall en la solución del proyecto, mejorando el comportamiento del ancho de banda y el uso adecuado del Internet.
4	**PROXY HTTP PARA VISUALIZACIÓN DE TRÁFICO WEB EN TRÁNSITO** Autor: Fondo Ferreiro, P. Fecha de publicación: (2017). Disponible en: http://castor.det.uvigo.es:8080/xmlui/bitstream/handle/123456789/52/TFG_PabloFondo.pdf?sequence=1
	Es un artículo de gran valor para la elaboración de nuestro proyecto, ya que usa definiciones y conceptos que aportan y dan una visión de los múltiples beneficios de usar un servidor proxy. Allí resalta que el proxy es un agente que actúa como intermediario entre un cliente y un servidor. La mayor parte de los proxy existentes son proxy web, cuya función es la de gestionar el acceso a recursos disponibles en la Web. En la parte final determina los usos de los servidores proxy, destacando el filtro de contenido, el monitoreo de la navegación y la mejora del rendimiento ya que almacena en cache las url ya visitadas. Importante ya que usa otro enfoque realizando un ataque llamado "man in the middle" para capturar el tráfico y re direccionarlo para que sea analizado en otro dispositivo y así determinar la categoría y confiabilidad de la página visitada, asegurando la navegación.
5	**Implementación de un servidor firewall-proxy bajo la plataforma de GNU/LINUX para la Facultad de Ingeniería en Ciencias Aplicadas, a fin de liberar procesamiento de los equipos del data center de la Universidad Técnica del Norte.** Autor: Espinosa Padilla, G. I. Fecha de publicación: jul-2017 Disponible en: http://repositorio.utn.edu.ec/bitstream/123456789/6233/2/ARTICULO.pdf

	El Proyecto se desarrolla en un entorno universitario y busca la implementación de un firewall que permita manejar de manera optima el tráfico, evitando la congestion en la red y los cuellos de botella que se pueden generar al no tener dispositivos que permitan el control de los datos. Por ello el objetivo que ellos plantean es utilizar mecanismos que permitan liberar procesamiento de los equipos de comunicación, por medio de la implementación de un firewall y un proxy, bajo la plataforma de GNU/Linux, que ayude a controlar el contenido de la información que atraviesa cada segmento de la red.
6	**Internet based parenting control application on teenagers** Autor: LÍDICE Haz ; GUARDA Teresa; ZAMBRANO Isaac; SÁNCHEZ Carlos Fecha de publicación: jul-2017 Disponible en: https://ieeexplore.ieee.org/abstract/document/7975739/authors
	El artículo aporta tips para realizar el filtrado web y como aplicarlo, adicional muestra la importancia del control del Internet en la crianza de los jóvenes, impidiendo el acceso a sitios de internet no autorizados, sitios de contenidos para adultos, sitios web con software malicioso, asegurando así riesgos de seguridad tanto para las estaciones de trabajo, computadores personales, dispositivos móviles como para los usuarios que los manipulan. De gran ventaja para los padres preocupados por el bienestar y el buen desarrollo académico de los hijos, ya que asegura un Internet adecuado para las edades de los niños y jóvenes en el hogar familiar.
7	**Prototipo de un sistema de protección perimetral y navegación segura para entornos domésticos** Autor: CUEVA ANCHAPAXI Carlos Andrés Fecha de publicación: 11-jul-2016

	Disponible en: http://bibdigital.epn.edu.ec/handle/15000/16481 Proyecto previo a la obtención de título de Ingeniero Electrónico y Redes de Información
	El artículo digital presenta un sistema de protección perimetral y navegación segura para entornos domésticos mediante el uso de herramientas open source "free". En donde se presentan diferentes dispositivos para ser implementados de manera local en un servidor local y así poder tener seguridad y control de contenidos de Internet en el hogar, incluso con horarios y cantidad de tiempo del uso del internet. Además el bloqueo por categorías de navegación, como redes sociales, contenido para adultos, sitios maliciosos, etc. y permitiendo ejecutar estadísticas de navegación, como los sitios web más visitados, o sitios que se denegaron en la navegación por no estar permitidos, dando una idea al administrado sobre la eficacia de la solución.
8	**Diseño e implementación de un clúster homogéneo para procesar los registros de navegación del proxy de la UCI** Autor: DESPAIGNE REYES Husseyn, HERNÁNDEZ PÉREZ Julio y ORDOÑEZ LEYVA Yoanni Fecha de publicación: 20-may-2014 Disponible en: https://www.researchgate.net/figure/Distribucion-de-los-nodos-de-procesamiento_fig1_233426527

	En el funcionamiento y gestión de un proxy, se debe tener un control y logs de navegación, para monitorear y tener un trazado de los sitios a los que navegan los empleados dentro de una organización, pero la cantidad de logs que llegan son millones de registros, por lo que el artículo plantea una solución en clúster para mejorar el rendimiento tanto en el almacenamiento como en la generación de informes y reportes de la navegación, ayudando a una buena administración del proxy. De otro lado, se plasma como realizar el tratamiento de los logs, su clasificación y posterior uso, logrando un buen desempeño para el objetivo del análisis en tiempo real del consumo de ancho de banda, url que más visitan los usuarios y el tiempo que duran conectados en la internet, para luego ser presentados en informes gerenciales o comités directivos en donde se toman acciones dependiendo del uso adecuado o no de la navegación.
9	**DISEÑO E IMPLEMENTACIÓN DE UN PROXY PARA LA ELIMINACIÓN DE CONTENIDO ESTEGANOGRÁFICO** Autor: FERNÁNDEZ ESCOLAR Carlos Fecha de publicación: 2009 Disponible en: https://core.ac.uk/download/pdf/30043027.pdf
	Importante resaltar lo que el autor aporta con el texto, en el filtrado que se puede realizar también a nivel de archivos, para este caso puntual el control a las imágenes que se descargan de internet, realizando un análisis exhaustivo de los archivos con contenido jpg, gif, bmp, etc. y así poder detectar que no tengan contenido estenográfico, para evitar ataques, virus, u ocultamiento de virus en dichos archivos, mejorando así la seguridad de la información y la red interna de la entidad donde se implemente.

10	**Implementación de un proxy en plataforma Linux para el control de transferencia de archivos con FTP, E-mail y Firewall para el laboratorio de software** Autor: NAVARRO Jorge Anibal Fecha de publicación: Junio 2009 Disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/1821/1/CD-2408.pdf
	Se resalta del artículo como se logra aplicar un filtro en la navegación, ya que los estudiantes podían navegar ilimitadamente, lo que hacía muy lenta la navegación y problemas de seguridad porque no había bloqueos de los archivos descargados, ni se examinaba el tráfico proveniente de internet. Importante recalcar también, como por medio de herramientas Linux se puede aplicar una solución de proxy efectiva, no solo para tráfico web, sino también de inspección en los correos y transferencia de archivos FTP.
11	**Sistema multiagente para el filtrado de pornografía mediante la evaluación del contenido multimedia de las páginas web** Revista en Telecomunicaciones e Informática, Vol 3 Medellín - Colombia. Enero - Junio de 2013, ISSN 2215-8200 Disponible en: https://revistas.upb.edu.co/index.php/telecomunicaciones/article/view/3311/2912
	Con el desbordado crecimiento de las tecnologías de la información y de la mano de esta el contenido malicioso en internet, en el artículo en mención se trata de realizar un filtrado del contenido web para detectar tráfico que no tiene que ver con los temas laborales, especialmente los contenidos de pornografías. Por eso el autor plantea procesos de filtrado y métodos de clasificación de contenidos Web para poder aplicar controles y bloquear dicho

	tráfico, para contribuir con la productividad laboral en las empresas. Adicional a lo anterior, el énfasis en el contenido de multimedia y su respectivo análisis permite realizar un control efectivo en el control de contenido que hacen los proxys, mejorando el rendimiento de la red y brindando seguridad a la red de la empresa.
12	**Implementación de un sistema proxy con seguridad para la navegación de médicos y pacientes en el Hospital Santa Inés** Autor: CRESPO Esteban, NARVÁEZ María Salomé y TENESACA Romel Leuvís Fecha de publicación: 2012 Disponible en: http://dspace.uazuay.edu.ec/bitstream/datos/2689/1/09225.PDF
	Dos aportes importantes a resaltar de este enlace es la idea que desarrolla y como a medida que el Internet se fue apoderando del tiempo de los usuarios, las entidades en general se han preocupado por brindar el servicio de navegación no solo para sus empleados o clientes internos, sino también para el cliente externo, logrando así agregar satisfacción y mejora en la evaluación o resultados que se buscan alcanzar. Por eso para contribuir con el buen uso del ancho de banda y tráfico hacia las redes públicas, los autores plantean el uso de uno proxy, que permite añadir seguridad, por medio de soluciones como autenticación, políticas de seguridad, control de acceso, perfilamiento y mejora en la administración y control de la navegación para el Hospital Santa Inés.

4.1.2 TERMINOLOGÍA

A continuación se relacionan conceptos que buscan clarificar su significado, para que el lector comprenda correctamente el uso y desarrollo dentro del proyecto.

ANCHO DE BANDA: Es la capacidad máxima que contiene un canal para transmitir información a través de él por un periodo de tiempo específico.

CIFRAR: Es la manera de transformar los datos en claro o legible a un archivo ilegible o representado por medio de códigos, que solo puede ser entendido o descifrado por quién contenga la llave privada para descifrarla.

CONFIDENCIALIDAD: Forma de garantizar y prevenir la divulgación de la información a personas o sistemas que no se encuentran autorizados.

CONTROL DE ACCESO: Es un sistema o política que controla y verifica si un usuario tiene los privilegios suficientes para acceder a la información o aplicación, por medio de autenticación o credenciales correctas.

CONTROL DE CONTENIDO WEB: Es una herramienta o solución diseñada principalmente para permitir, filtrar o bloquear el contenido en cuanto a la navegación, que por medio de formularios y categorías de los sitios URL, definir si un usuario o grupos de usuarios pueden consultar dicha categoría o sitios.

CONTROLADOR DE DOMINIO: Es un servidor que almacena una réplica de la cuenta y de la información de seguridad de un dominio y define los límites del mismo. Los controladores de dominio tienen una serie de responsabilidades, y una de ellas es la autenticación, que es el proceso de garantizar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red, a través del uso de una contraseña. Esto permite validar a los usuarios de una red para

ser partes de la plataforma de clientes que recibirán los servicios de información. En un dominio Windows, cuando un cliente no autorizado solicita un acceso a los recursos compartidos de un servidor, el servidor actúa y pregunta al controlador de dominio si ese usuario está autentificado. Si lo está, el servidor establecerá una conexión de sesión con los derechos de acceso correspondientes para ese servicio y usuario. Si no lo está, la conexión es denegada.

DISPONIBILIDAD: Asegurar que la información puede ser consultada en cualquier momento que el usuario la necesite de manera segura y con privilegios de acceso.

DIRECTORIO ACTIVO: Es un servicio de directorio, propietario de Microsoft para su uso en redes de dominio de Windows. Cuenta con funciones de autenticación y autorización y proporciona un framework para otros servicios similares. Básicamente, el directorio consiste en una base de datos LDAP que contiene objetos en red. Active Directory corre y ejecuta bajo el sistema operativo Windows Server. Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

DOMINIO: En el ámbito informático un dominio se define como un grupo de computadoras, dispositivos y equipos de computación que comparten el mismo nombre de dominio, es decir se encuentran en un mismo grupo de red. Ejemplo: "*Colpatria.com"*

EXTRANET: Es una red privada para compartir información de manera segura, pero que suele tener un acceso semiprivado, es decir que no solo los empleados internos la consulten sino también los proveedores, socios y clientes.

FIREWALL: Es un sistema, dispositivo o servidor, ya sea por hardware o software, que permite proteger a un equipo de computación o a una red de computadoras, de las intrusiones que provienen de una tercera red. El firewall es un sistema que permite filtrar los paquetes de datos que andan por la red y filtra el tráfico entre la red interna y externa.

FOREST: En Active Directory el bosque (forest) es una colección de uno o más dominios que comparten una misma estructura lógica, catálogo global, esquema y configuración. Todos los dominios del bosque cuentan con relaciones de confianza automáticas de 2 vías y transitivas. El bosque representa una instancia completa del directorio y una frontera de seguridad.

FSSO: Es un concentrador o recolector de logs de inicio de sesión que los almacena y a su vez alimenta al servidor proxy para el control de navegación para saber qué política de seguridad aplicar y así saber si un usuario o grupo de directorio activo está autorizado para consultar una página web o sitio.

HTTPS: Es el principal protocolo seguro para intercambio de información que usa internet basado en SSL y TLS.

INSPECCION PROFUNDA: Método de análisis de paquetes y escaneo de tráfico, el cual permite inspeccionar a fondo los datos, si vienen cifrados los descifra, valida su contenido y verifica que sean seguros, importante para la navegación https.

INTEGRIDAD: En seguridad de la información la integridad se refiere a cómo los datos se deben mantener intactos libre de modificaciones o alteraciones por terceros, cuando se modifica

algo en la información, sea por accidente o intencionado se pierde la integridad y falla el proceso. Por este motivo se debe proteger la información para que sólo sea modificada por la misma persona, evitando así que se pierda la integridad.

INTERNET: Se puede definir como la red más grande que existe, o comúnmente conocida como la red de redes interconectadas a nivel mundial para compartir información o servicios por medios de sitios web o software especializado y basado en el protocolo TCP/IP.

Existen diferentes tipos de conexión a internet, es decir, distintos medios por los cuales uno puede obtener conexión a la red de redes. El primero de ellos fue la conexión por dial-up, es decir, tomando la conectividad de una línea telefónica a través de un cable. Luego surgieron otros tipos más modernos como ser el ADSL, la fibra óptica, y la conectividad 3G y 4G (LTE) para dispositivos móviles.

INTRANET: Principalmente es una red privada e interna que se basa o utiliza tecnología de Internet pero que no se tiene acceso libre o público.

KEY o LLAVE: Para el presente proyecto una llave es una cadena de caracteres que actúa como un password o código para permitir descifrar un archivo o acceder a un sistema informático.

NAVEGADOR: Se conoce también como navegador de Internet, explorador web o simplemente *browser*. Y sirve para recuperar, consultar y visualizar la información que contiene un sitio web desde servidores localizados en cualquier parte del planeta.

OPEN SOURCE: Es un modelo de software libre que se puede modificar de manera personalizada de acuerdo a su objetivo, conocido también como código abierto.

POLITICAS DE SEGURIDAD: Son definiciones o normas de seguridad que se deben seguir para asegurar principalmente la información y los dispositivos que interactúan con esta.

PROCESO MAN-IN-THE-MIDDLE: Encargado de realizar el ataque man-in-the-middle mediante envenenamiento de la caché ARP, logrando atraer el tráfico del usuario a otra máquina.

PROTOCOLO DE RED: Es un conjunto de normas y estándares que establecen como se comunican los componentes o dispositivos de una red, independiente de la marca o equipo que se comunique, como es un estándar este se debe cumplir para que decirlo de alguna manera hablen el mismo idioma.

PROXY: El proxy en un equipo de cómputo, servicio o dispositivo que sirve como intermediario para atender solicitudes o peticiones de otras estaciones, como para el presente proyecto atiende las peticiones de navegación que hacen las estaciones cliente y reenvía el paquete al destino o url que el usuario solicitó, tanto para la entrada como para la salida de tráfico.

RED INFORMATICA: Se entiende como el conjunto de computadores o equipos que comparten un mismo enlace de comunicación, para compartir servicios, recursos y aplicaciones para un fin común.

SERVIDOR: Es un ordenador físico o virtual que brinda un servicio a otros clientes o dispositivos informáticos, el servidor es capaz de atender solicitudes de sus clientes y dar una respuesta a dichas solicitudes de manera efectiva. Hay muchos ejemplos de servidores pero los más famosos son: Servidores web, servidores de impresión, servidores de almacenamiento, etc.

SSL/TLS: Protocolo de seguridad que actúa en la capa de transporte para proporcionar seguridad, cifrado e integridad en una comunicación de red, para asegurar dicha comunicación mediante cifrado simétrico o asimétrico.

4.2 MARCO LEGAL

Dentro del desarrollo del proyecto se ha tenido en cuenta la actual regulación que existe para los temas que tienen que ver con Internet, tanto las leyes nacionales, como los lineamientos internos del banco que hablan sobre el buen uso del Internet y de la protección de la información.

Es importante tener en cuenta la ley 1582 de 2012, que habla de la "protección de los datos" en Colombia, ya que en ella involucra el tratamiento, uso, control y seguridad que se debe tener con la información personal de los clientes, ya que toda persona tiene derecho a saber si sus datos se encuentran en las bases de datos de las entidades y como esta controla y da buen uso de las mismas. De allí el compromiso del banco para el control de la información y prevenir la fuga de información a través del servicio de Internet.

Otra regulación de soporte y lineamiento para el desarrollo del presente proyecto es el proyecto de ley No. 179 de 2018 "Sobre regulación del buen uso y funcionamiento de redes sociales y sitios web" en donde plantean principalmente dar condiciones básicas para garantizar la protección de la honra y el buen nombre de los ciudadanos, tanto para las redes sociales como

sitios Web, preocupándose por la integridad y veracidad de la información, haciendo énfasis en el buen uso del servicio de Internet, aunque para unos sectores lo vean como una afectación al derecho a la libre expresión.

No hay que pasar por alto las leyes y regulaciones que se tienen por promover y poseer material de pornografía infantil, por ello el proxy y el control de contenido ayuda en el bloqueo de los sitios que contienen dicho material, asegurando la red interna y la reputación de la entidad.

Al interior del banco también se tienen lineamientos y códigos de conducta que los empleados deben seguir para hacer buen uso de la navegación, en donde detalla el alcance de la política que todos sus empleados deben comprometerse a cumplir para no exponer al banco a sanciones o multas por falta a la protección de la información.

En el párrafo III del *código interno de conducta para el uso del Internet y del correo electrónico*" se puntualiza en este tema que es vital para el proyecto y allí detalla: "El derecho del Grupo Scotiabank a supervisar, restringir el acceso y establecer políticas de acceso a Internet, y por lo general no restringe el acceso a la mayoría de los sitios Web. Sin embargo, se reserva el derecho de restringir el acceso a Internet, al correo electrónico y a los sistemas de información internos por cualquier motivo, en cualquier momento, y sin notificación.

Además, con la finalidad de proteger a Scotiabank y a sus empleados, algunas áreas de internas emplean tecnología para bloquear el acceso a sitios Web con contenidos prohibidos.

El uso de la tecnología y de los servicios de información del banco puede supervisarse en cualquier momento para identificar o tomar medidas según las actividades sospechosas, inadecuadas o inusuales que puedan indicar una violación de las Pautas, las leyes aplicables u otras políticas del Grupo Scotiabank.

5. PROPUESTA DE SOLUCIÓN

Dentro de los requisitos iniciales y objetivos del proyecto, se requiere que la nueva solución, en lo posible no afecte la arquitectura actual y requiera el mínimo de ajustes posibles para no afectar a los funcionarios actuales, es por ello que luego de estudiar alternativas lo más beneficioso para cumplir con el objetivo del proyecto es robustecer el proxy actual con un nuevo equipo de mayor capacidad, procesamiento y rendimiento, que permita cumplir todas las características nuevas solicitadas como inspección profunda en tráfico SSL e IPS.

La función principal de la solución y el primer elemento del sistema y pieza fundamental del mismo es el servicio de proxy-web. Este sistema es el intermediario entre los usuarios de una red y el acceso a internet. De manera general, estos sistemas funcionan según el siguiente proceso:

•El cliente solicita una página web al servidor proxy.

•El servidor proxy recibe la petición y consulta si la información solicitada la tiene guardada en su memoria cache.

•Si dispone de ella verifica si está actualizada, si es así se la ofrece al cliente

•Si no es así, actualiza la información y se la ofrece al cliente.

•En caso de no disponerla en la memoria cache, la solicita, la almacena y se la ofrece al cliente.

La solución consiste en reemplazar el equipo actual por un equipo de la misma marca pero un modelo más actualizado que tenga mejores características y por ende mejor rendimiento, para recibir todo el tráfico de navegación generado por los 2700 nuevos empleados más los actuales.

Después de validación y estudio de dispositivos, se propone un equipo Fortinet 3000D, este proxy hace parte de la tecnología Next-Generation Firewall de tecnología avanzada, protegen la red y el tráfico contra APTs (ataques personalizados) con la mejor protección contra amenazas de la industria y el mejor rendimiento por precio. Las series de tecnología avanzada de FortiGate ofrecen innovación en el procesador de seguridad especialmente diseñado para brindar una seguridad y rendimiento sin compromiso con una inspección SSL y un rendimiento de NGFW superiores para el borde, el centro de datos y los segmentos internos. Debido a las más recientes innovaciones de procesadores de seguridad, FortiGate de la serie 3000 ofrece una protección

contra amenazas de hasta 30 Gbps y el rendimiento de inspección de SSL más alto de la industria en un appliance compacto.

La adquisición total será de dos equipos del modelo relacionado previamente, para tener alta disponibilidad y poder armar un clúster que garantice que en caso de alguna falla del equipo master o principal, el segundo equipo podrá soportar el servicio de navegación en el banco, cubriendo así la necesidad y objetivos planteados de poder actuar ante un desastre o falla en el centro de cómputo principal del banco, asegurando así el servicio de navegación de los funcionarios.

EQUIPOS NECESARIOS

CANTIDAD	EQUIPO	MODELO
2	Fortigate NGFW	3000D
1	Servidor virtual (agente colector login)FSSO	Windows Server 2016
2	Cableado centro de cómputo alterno	Fibra óptica
6	Conectores Transceiver	N/A

Tabla 1: Equipos necesarios

5.1 PLANEACIÓN METODOLOGICA

Dentro de dicha planeación se han identificado las siguientes fases:

FASE DE PREPARACION: En esta fase abarca todo el proceso de levantamiento de la información, estudio de factibilidad, validación y elección de la solución o soluciones planteadas.

FASE DE APROBACION Y VALIDACION DE LAS TAREAS A DESARROLLAR:

El proyecto será sometido a aprobación del área de PPM, se documentará todos los procesos y se identificará los involucrados y fases para llevar a cabo la ejecución del proyecto. Se realizará el análisis de riesgo, evaluación de costos y apertura de tareas para cada área involucrada.

5.2 **DESARROLLO TECNOLOGICO**

FASE DE ALISTAMIENTO: En esta fase también se podría llamar como la fase de adquisición y ajustes de prerrequisitos para implementar la solución. Se ejecutará todo el procedimiento de la compra de los equipos, desde su cotización, trámite de autorización de compra en el comité respectivo y toda la logística para recibir los nuevos equipos en las instalaciones del data center principal del banco. Ultimar detalles del cableado y adquisición y aprovisionamiento del nuevo servidor Windows 2016 con el área de arquitectura y virtualización del banco.

Diagrama FISICO de red planteado

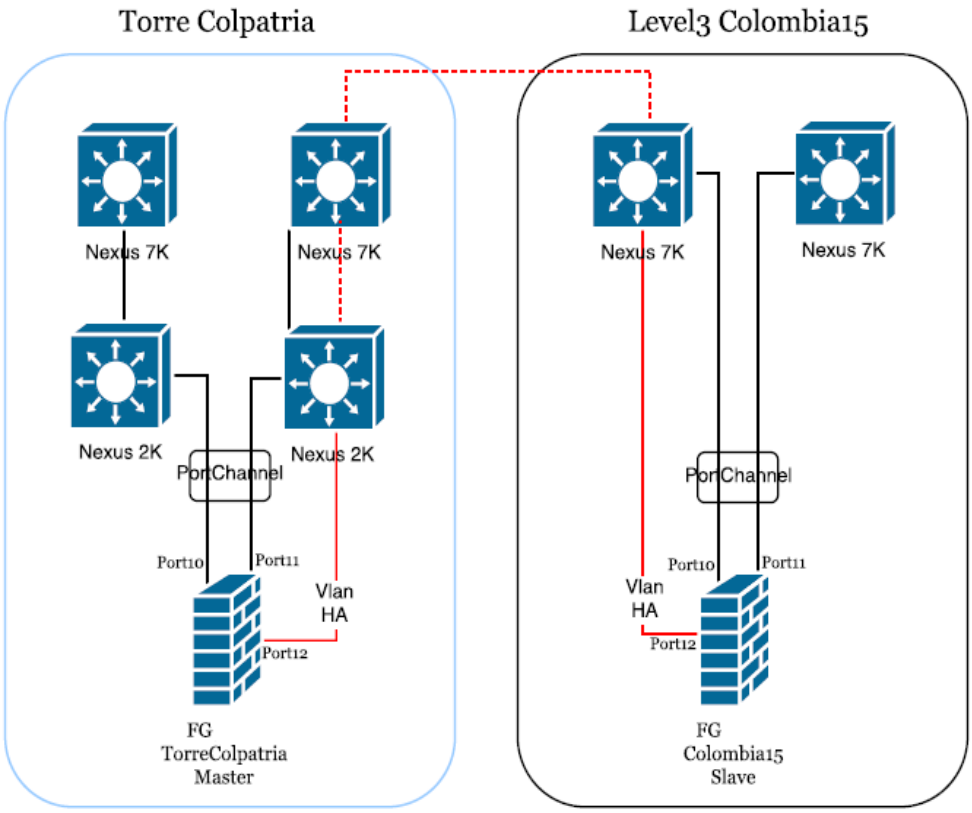

Imagen 1: Arquitectura física

DISEÑO LÓGICO

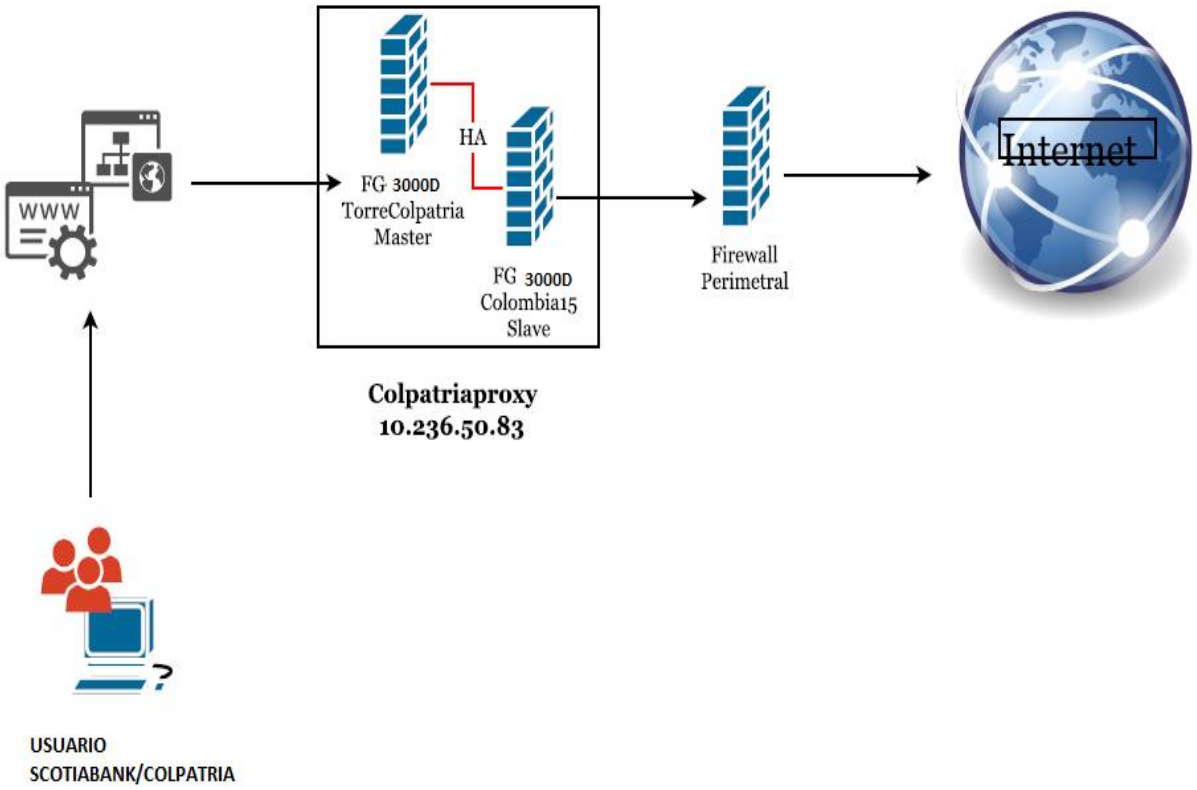

Imagen 2: Arquitectura lógica

Como se detalló en el planteamiento del problema, los nuevos "Controladores de Dominio" de Scotiabank.co, deben tener relación de confianza con los actuales controladores de dominio de Colpatria, a través del mismo Forest, permitiendo la integración de los dos dominios.

En los nuevos controladores de dominio se debe instalar el programa DCAgent de Fortinet que se encargará de recolectar los logs o alertas de cuando un usuario se loguea en una estación de trabajo, para poder enviarlos al servidor FSSO que se integra con el proxy 3000D, y con base en las políticas de directorio activo y políticas del proxy, definirá que permisos tiene autorizados el usuario, que categorías o sitios de navegación puede o no consultar.

El nuevo proxy deberá manejar y aplicar las políticas actuales de navegación, en donde lee el grupo de directorio activo al que pertenece el usuario de red y le aplica el perfil de navegación correspondiente, que definirá si el usuario puede o no consultar o no las siguientes categorías:

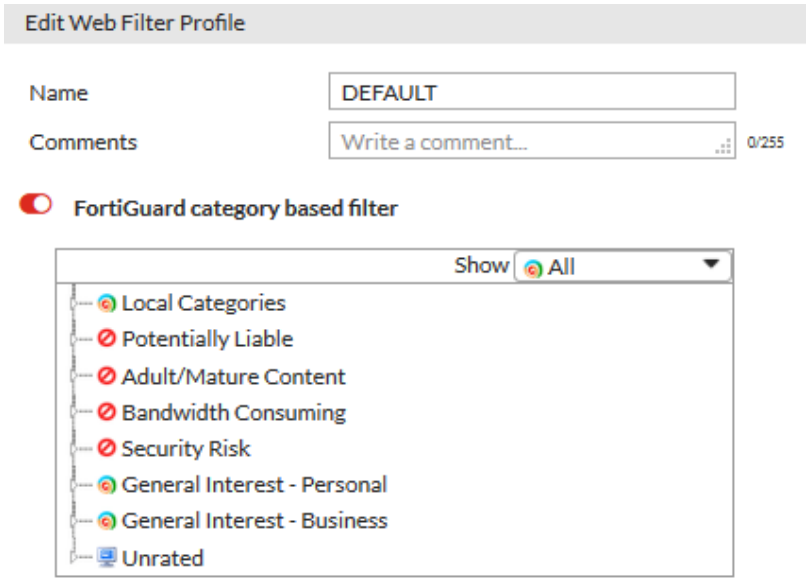

Imagen 3: Categorías de navegación

Las categorías definidas permiten una administración más aplicable y controlable, ya que permite una mejor gestión para el equipo de seguridad y el establecimiento de las políticas seguras acorde al perfil, obteniendo así la implementación correcta y funcionamiento del nuevo proxy.

FASE DE IMPLEMENTACIÓN: Esta fase es la más crítica ya que involucra toda la fase de ejecución, instalación y aseguramiento de la nueva plataforma fortinet, y allí se detallan las siguientes tareas a realizar:

a. Crear cambio en la herramienta de cambios, para ser sustentado en el comité de cambios, con toda la información y documentación requerida, así como el análisis de riesgos del cambio en mención
b. Realizar backup del actual equipo que brinda el servicio de proxy. Dicho backup de la configuración será editado y personalizado para que pueda ser instalado en los nuevos Fortigate adquiridos.
c. Preconfiguración de los nuevos equipos. Validar que el backup editado pueda ser cargado en los nuevos equipos y realizar validaciones previas del equipo, así como la ubicación física de los equipos en el mismo rack que se encuentran los equipos a reemplazar. En paralelo en área de control de acceso estará creando los nuevos usuarios de red en el

nuevo dominio y en el grupo de directorio activo respectivo para la aplicación del perfil de navegación.

d. Ventana del cambio. Una vez en el comité de cambios se haya aprobado la fecha para la ventana del cambio en horario no productivo, se planeará la logística para contar con personal del área de seguridad informática del banco y personal del proveedor con quién se adquirió el producto, tanto en el data center principal como en el data center alterno.
e. Ejecución del cambio. El día fijado el proveedor en compañía del coordinador del proyecto realizarán el cambio del equipo, desconectando los cables del equipo anterior al nuevo equipo y validarán que el servicio quede disponible nuevamente. Paralelamente se realizará la configuración del FSSO en el servidor Windows 2016 y la instalación del agente Colector en los controladores de domino nuevos.

FASE POST-INSTALACIÓN: En esta fase se ejecutará toda la parte de monitoreo, validación y pruebas de la funcionalidad de los nuevos equipos. Se debe revisar todos los logs de la máquina y ejecutar reportes donde se evidencie que la navegación funciona correctamente así como la aplicación del control de contenido correcta de acuerdo al perfil en que se encuentre. Pruebas con usuarios finales donde se evidencie el bloqueo a categorías no autorizadas de acuerdo a su perfil y también la navegación a las url permitidas, así como el funcionamiento del correo Office 365 que también va por internet.

FASE DE CIERRE: Se evaluará la efectividad del nuevo dispositivo y se realizará el cierre de las tareas de cambio gestionadas, así como el proceso de facturación con el área encargada y documentación de las tareas aprendidas con el proyecto.

INNOVACIÓN

El proyecto cuenta con varios elementos de innovación, y el principal es que se implementa en medio de 2 dominios de red diferentes, integrándolos como si fuera uno solo. Adicional la importancia que tiene el implementar en el filtrado Web, controles adicionales como inspección profunda SSL, Data Leak Prevention e IPS, lo que agrega una capa de seguridad más fortalecida en la navegación de los usuarios del banco.

6. CONCLUSIONES

- La solución elegida logra ser la de menor impacto y más rápida de implementar para cumplir con el poco tiempo para la ejecución del proyecto, pero ante todo dando un buen servicio y continuando con las políticas de seguridad que aseguran el control de contenido en la navegación y se restringe los accesos a las páginas que estén prohibidas, o sitios que puedan perjudicar la red interna del banco.

- Se define la arquitectura física y lógica que tendrá la nueva solución proxy con el clúster en alta disponibilidad para temas de contingencia y redundancia del servicio de Internet.

- Se logra identificar mejoras en las políticas de navegación y el buen uso de las categorías de navegación para un mejor filtrado del tráfico web.

- Con el desarrollo del proyecto se identifica el marco legal que rige la navegación tanto a nivel global como a nivel interno con las políticas internas que dispuso la entidad.

RECOMENDACIONES

Se recomienda a futuro implementar un Fortiautenticator en la arquitectura actual, ya que facilita el tiempo de autenticación de los usuarios, debido a que las políticas entre controladores de dominio a veces no tienen el tiempo prudente para replicación y con la solución aconsejada se podría disminuir este tiempo, aunque implicaría un costo adicional por el precio del nuevo dispositivo.

7. REFERENCIAS

DESPAIGNE REYES Husseyn, HERNÁNDEZ PÉREZ Julio y ORDOÑEZ LEYVA Yoanni. 20-may-2014. **DISEÑO E IMPLEMENTACIÓN DE UN CLÚSTER HOMOGÉNEO PARA PROCESAR LOS REGISTROS DE NAVEGACIÓN DEL PROXY DE LA UCI.**

https://www.researchgate.net/figure/Distribucion-de-los-nodos-de-procesamiento_fig1_233426527

FERNÁNDEZ ESCOLAR Carlos. 2009. **DISEÑO E IMPLEMENTACIÓN DE UN PROXY PARA LA ELIMINACIÓN DE CONTENIDO ESTEGANOGRÁFICO.**

Web: https://core.ac.uk/download/pdf/30043027.pdf

NAVARRO Jorge Anibal. 2009. **IMPLEMENTACIÓN DE UN PROXY EN PLATAFORMA LINUX PARA EL CONTROL DE TRANSFERENCIA DE ARCHIVOS CON FTP, E-MAIL Y FIREWALL PARA EL LABORATORIO DE SOFTWARE.**

Web: https://bibdigital.epn.edu.ec/bitstream/15000/1821/1/CD-2408.pdf

CRESPO Esteban, NARVÁEZ Salomé y TENESACA Romel. 2012. **IMPLEMENTACIÓN DE UN SISTEMA PROXY CON SEGURIDAD PARA LA NAVEGACIÓN DE MÉDICOS Y PACIENTES EN EL HOSPITAL SANTA INÉS.**

Web: http://dspace.uazuay.edu.ec/bitstream/datos/2689/1/09225.PDF

CASTELLANOS HERNÁNDEZ Juan Manuel y LÓPEZ PÉREZ Manuel. 10 de marzo de 2018. **IMPLEMENTACIÓN DE UN SISTEMA PROXY DE NAVEGACION SEGURA EN EL GET DE CIENFUEGOS.**

Web: http://revistas.unipamplona.edu.co/ojs_viceinves/index.php/RCTA/article/view/3332/1969

NADER Mauricio Jose. 2011. **IMPLEMENTACION DE UN PROXY FIREWALL EN UNA RED CONSIDERANDO POLITICAS DE SEGURIDAD.**

https://www.academia.edu/25170216/implementacion_de_un_proxy_firewall_en_una_red_considerando_politicas_de_seguridad

LÍDICE Haz; GUARDA Teresa; ZAMBRANO Isaac; SÁNCHEZ Carlos. Jul-2017. **INTERNET BASED PARENTING CONTROL APPLICATION ON TEENAGERS**

Web: https://ieeexplore.ieee.org/abstract/document/7975739/authors

CUEVA ANCHAPAXI Carlos Andrés. 11-jul-2016.**PROTOTIPO DE UN SISTEMA DE PROTECCIÓN PERIMETRAL Y NAVEGACIÓN SEGURA PARA ENTORNOS DOMÉSTICOS.** Web: http://bibdigital.epn.edu.ec/handle/15000/16481

Oviedo Isabel, Manco Andrea, Guerra Juan Esteban**.** Junio 2013. **SISTEMA MULTIAGENTE PARA EL FILTRADO DE PORNOGRAFÍA MEDIANTE LA EVALUACIÓN DEL CONTENIDO MULTIMEDIA DE LAS PÁGINAS WEB.**

Web: https://revistas.upb.edu.co/index.php/telecomunicaciones/article/view/3311/2912

MENDOZA Jesús y PANADERO Javier. (9 junio 2019). **SISTEMA PROXY-WEB CON FILTRADO Y CONTROL DE ACCESO**. Universidad de Catalunya Sitio web: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/94506/6/ihocesmoralTFG0619memoria.pdf p.9

FONDO FERREIRO, P. (2017). **PROXY HTTP PARA VISUALIZACIÓN DE TRÁFICO WEB EN TRÁNSITO.** Sitio Web

http://castor.det.uvigo.es:8080/xmlui/bitstream/handle/123456789/52/TFG_PabloFondo.pdf?sequence=1

Espinosa Padilla, G. I. (jul-2017) **IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL-PROXY BAJO LA PLATAFORMA DE GNU/LINUX PARA LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, A FIN DE LIBERAR PROCESAMIENTO DE LOS EQUIPOS DEL DATA CENTER DE LA UNIVERSIDAD TÉCNICA DEL NORTE.**

Disponible en: http://repositorio.utn.edu.ec/bitstream/123456789/6233/2/ARTICULO.pdf