Servicios de integración seguridad de la información

José Andres Buila Ortiz, Jonathan Rincón González, Andres Leonardo Gordillo Bautista, Daniel Esteban Diaz Guerra, Jhon Eduardo González Fonseca

Seguridad Informática, Fundación Universitaria Compensar

Proyecto fin de grado

Carlos Alberto Cañón Romero

18 de noviembre de 2022



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

Servicios de integración seguridad de la información

José Andrés Buila Ortiz
Jonathan Rincón González
Andrés Leonardo Gordillo Bautista
Daniel Esteban Diaz Guerra
Jhon Eduardo González Fonseca

Trabajo de grado presentado como requisito parcial para optar al título de:

Especialista en Seguridad Informática

Director (a):

M.Sc., Ingeniero Jairo Cesar Gómez Acero

Línea de Investigación:

Consultoría

Fundación Universitaria Unipanamericana – Compensar
Facultad de Ingeniería, Ingeniería de Especialización en Seguridad Informática
Bogotá, Colombia
2022

Resumen

Proteger los datos es una de las tareas más importantes en la actualidad, cuándo se utilizan servicios públicos como internet se está más vulnerable a cualquier ataque cibernético por lo cual se requieren mecanismos sofisticados de seguridad.

El presente trabajo de investigación consiste en la descripción y análisis de las condiciones actuales de asegurar la información o datos basados en las infraestructuras seguras expuestas por organizaciones para proteger la información.

El problema de investigación fue analizar los aspectos que conllevan a la planeación de una empresa para poder asegurar los datos en geolocalizaciones distintas y brindar en todo momento el cifrado. Seguidamente se analizan técnicamente los métodos de asegurar la información con protocolos, certificados y métodos avanzados para demostrar la baja probabilidad de vulneraciones.

Se necesita implementar el protocolo seguro IPsec el cual se conforma por algoritmos seguros que se adaptan al diseño de red de la empresa Baracoff.

Palabras clave: (IPsec, Protocolo, Cifrado, Certificados, Datos).

Abstract

Protecting data is one of the most important tasks today, when public services such as the Internet are used, they are more vulnerable to any cyber-attack, for which sophisticated security mechanisms are required.

This research work consists of the description and analysis of the current conditions of securing information or data based on secure infrastructures exposed by organizations to protect information.

The research problem was to analyze the aspects that lead to the planning of a company to be able to secure the data in different geolocations and provide encryption at all times. Next, the methods of securing the information with protocols, certificates and advanced methods are technically analyzed to demonstrate the low probability of violations.

It is necessary to implement the secure protocol IPsec which is made up of secure algorithms that adapt to the network design of the Baracoff company.

Keywords: (IPsec,Protocolo,Cifrado,Certificados,Datos).

Contenido

PÁG.

Introducción 6
Antecedentes y Justificación 7
Formulación del Problema 8
Objetivo General 9
Objetivos Específicos 9
Alcances y Limitaciones 9
Riesgos 10
Cronograma 15
Marco teórico 16
Diseño Metodológico 43
Resultados 45
Discusión 46
Conclusiones y recomendaciones 46
Bibliografía 47

Ilustraciones

Ilustración 1 Riesgo Actual 11
Ilustración 2 Control para el riesgo 12
Ilustración 3 implementación de controles a los riesgos 13
Ilustración 4 Riesgo Residual 14
Ilustración 5 Cronograma Primer Momento 15
Ilustración 6 Cronograma Segundo Momento 16
Ilustración 7 Diseño LAN Sucursal Principal 18
Ilustración 8 Diseño LAN Sucursales 19
Ilustración 9 Backbone MPLS (Ecorp, 2015) 20
Ilustración 10 Equipos (JavaTPoint, 2018) 26
Ilustración 11 IPsec Tunnel (CISCO, 2017) 33
Ilustración 12 Triada de seguridad (ServiTux, 2018) 35
Ilustración 13 Ciclo 38
Ilustración 14 Topología Actual 41
Ilustración 15 Diagrama topológico - Integración Sede A y Sede B 42

Ilustración 16 Diagrama topológico con protocolo IPsec..... 42

Introducción

El presente informe se basará en la competencia constante y critica de la seguridad informática que es un punto importante para tratar, fortalecer y tener segura la información, viendo la necesidad de la compañía Baracoff se ha diseñado un conjunto de estrategias para centralizar y controlar de manera segura la información que transmitirá las sucursales nuevas que va a implementar Baracoff.

Considerando las necesidades de Baracoff de integrar las dos (2) sucursales adicionales con la actual, la importancia de este proyecto es que la data de contabilidad e inventario de la compañía siga centralizada, se está teniendo en cuenta los conceptos generales que se aplican para garantizar que los datos que se enviaran de extremo a extremo este protegido por algoritmos que permita viajar de manera segura por un canal dedicado toda la información que maneje la compañía tales como reporte, contabilidad e inventario, entre otros.

Se ha tenido en cuenta las expectativas descritas en las reuniones de entendimiento y verificación de infraestructura, por lo que el diseño que se evaluó y se presenta basado en las siguientes expectativas:

- Se espera un máximo de 10 personas que transmitan, actualicen en tiempo real la contabilidad y reportes mensuales de ventas de la empresa.
- Se presentará unas políticas de seguridad informática, establecidas con los estándares y directrices de la compañía.
- El cliente usara este canal seguro para que su información tenga un monitoreo constante y no se pierda los datos.
- En caso de que se requiera, se evaluara las condiciones de los equipos de cómputo de los operarios de la empresa y así garantizar que manejen herramientas básicas de seguridad tales como antivirus.

Antecedentes y Justificación

Baracoff, es una empresa que se instaló en la ciudad de Bogotá a principios del año 2021. El mismo es un Bar, dirigido a personas mayores de 18 años, de ambos sexos que eligen pasar un momento divertido y placentero. Una propuesta innovadora y diferente, en la que se destacan la ambientación, un original sistema de servicio al cliente y toda la tecnología de vanguardia necesaria para lograr el objetivo antes enunciado. Cuenta con una amplia experiencia y trayectoria en la actividad del entretenimiento, consumo y preparación de bebidas alcohólicas. A futuro se implementarán dos (2) sucursales en las cuales se deberá acondicionar un canal seguro en la parte tecnológica para el envío de la información entre estas tres.

Esta consultoría está basada en la importancia de mantener segura la información en cualquier compañía y la manera correcta para ser dirigida desde los diferentes puntos aportando conocimientos adquiridos por cada autor. Conectar la tecnología con los clientes es un elemento clave en cualquier negocio de la actualidad, lograr demostrar esa necesidad

sobre las facilidades que brinda la tecnología para realizar diferentes acciones de nuestra vida diaria es parte clave de este negocio.

Una parte fundamental en la implementación de tecnologías de administración que permitan conectar la información de las sedes generara un incremento en el control y manejo de las sedes, lo que permitirá una conexión más rápida de la información sobre hechos que ocurran en tiempo real.

Según datos de la Cámara de Comercio Colombiana, actualmente en Colombia existen más de 1.300.000 empresas, y más del 60% de estas son declaradas Pymes o Mini Pymes. Esto abre la puerta a una clara necesidad ya que en muchas empresas cuyo establecimiento la tecnología en seguridad y manejo de la información no siempre hace parte entre los principales activos que deben tener implementados o contratados.

Formulación del Problema

¿Cómo hacer que Baracoff posea una infraestructura segura de red?

Para Baracoff la cual carece de una infraestructura segura para el manejo de la información y esto afecta la triada de seguridad en la empresa, por esto se hace necesario realizar una conexión con un protocolo a implementar para garantizar la seguridad en el envío y recibido de datos.

Objetivo General

Establecer las condiciones para que Baracoff establezca la conectividad con sus sucursales de manera segura usando mecanismos tecnológicos que garanticen la seguridad de los datos.

Objetivos Específicos

- Comprender la dinámica del envío y recepción de la información desde las diferentes sucursales.
- Diseñar a detalle el proceso, subprocesos, protocolos e instructivos de mejora seleccionada, utilizando un canal seguro.
- Establecer un diseño de baja escala para entender el funcionamiento del cifrado de información de extremo a extremo.
- Implementar el protocolo IPsec sobre los canales dedicados en su centro de datos principal.

Alcances y Limitaciones

El objetivo final de esta consultoría es aportar recomendaciones y un diseño a la empresa sobre el envío y recepción de la información por medio del protocolo adecuado entre diferentes sucursales, para el respectivo despliegue en las instalaciones de la organización.

La implementación de la red será por medio del proveedor de servicios el cual lo asumirá el cliente y a continuación, se presentará la propuesta económica de los elementos

propuestos de acuerdo con el diseño a implementar en la compañía en un término de 2 meses a partir de la apertura de las nuevas sucursales.

Ítem	Descripción	Cantidad	Valor
1.	Router Cisco	3	$17’000.000
2.	Switch Cisco	3	$ 3.000.000
2.	Licencias Soporte	3	$60’000.000
3.	Servicio de Implementación	1	$35´000.000

Riesgos

En riesgos es posible observar que la empresa posee una infraestructura de red básica y débil para el manejo adecuado de la información de las sucursales validando con la compañía indican que no poseen un sistema de seguridad correcto para la oferta que se implementará se indican los diferentes controles para que se mitigue el riesgo actual en esta se evidencia en el siguiente mapa de riesgos:

Nº	Categoría Activo / Activo	Tipo / Clasificación del Riesgo	Riesgo	Causas / Vulnerabilidades	Probabilidad	Impacto	Riesgo inherente
R1	Información	Seguridad de la Información	PÉRDIDA O DETRIMENTO DE INFORMACIÓN POR:	Robo de información en los datos de las sucursales	Probable	Mayor	EXTREMO
R2	Activos Físicos	Operativo	DAÑO EN LOS ACTIVOS POR:	Manipulación indebida de los elementos de red	Probable	Mayor	EXTREMO
R3	Activos Físicos	Operativo	DEFICIENCIAS O DETERIORO DEL SERVICIO AL CLIENTE POR:	Perdida de la información almacenada por daño en disco duro.	Posible	Mayor	ALTO
R4	Infraestructura y comunicaciones	Seguridad Física	DAÑO EN LOS ACTIVOS POR:	Fallas de envío y recibido de la información de las demas sucursales	Posible	Mayor	ALTO
R5	Personas	Operativo	DEMORAS EN LOS SERVICIOS PRESTADOS Y EJECUCIÓN DE LOS PROCESOS POR:	falta de información sobre inventario en sucursales	Probable	Alto	EXTREMO
R6	Infraestructura y comunicaciones	Seguridad de la Información	INTERRUPCIÓN DE LOS SISTEMAS / PROCESOS POR:	fallas de seguridad en las estaciones de servicio de red	Casi seguro	Alto	EXTREMO
R7	Activos Físicos	Operativo	PÉRDIDAS ECONÓMICAS POR:	Mal calculo de caja	Probable	Mayor	EXTREMO

Ilustración 1 Riesgo Actual

Se indica a la empresa que se generará un control para mitigar estos riesgos ya que al observa la falla de seguridad en la arquitectura actual, implementando un protocolo adecuado para el manejo de esta información.

		DISEÑO							Evaluación Diseño
Control	Descripción	Tipo	Naturaleza	Frecuencia	Registro de Ejecución	Evidencia	Responsable Ejecución	Reponsable Supervisión	
C1	Canal Seguro para el envio y recibio de la información de las sucursales	Correctivo	Semi-automatica	Semanal	Si	Estadisticas	Analista en Seguridad	Representante Legal	ADECUADO
C2	Capacitación personal encargado de Datacenter	Correctivo	Manual	Diario	Si	Planilla ingreso y salida	Ingeniero Telecomunicaciones	Representante Legal	ADECUADO
C3	Cambio de Almacenamiento a la Nube	Correctivo	Automática	Semanal	Si	Logs	Servicio Cloud	Representante Legal	ADECUADO
C4	Manejo de información por protocolo Ipsec	Correctivo	Automática	Semanal	Si	Logs	Ingeniero Telecomunicaciones	Representante Legal	ADECUADO
C5	Actualización de datos en tiempo real	Preventivo	Manual	Diario	Si	Logs	Personal de Caja	Representante Legal	ADECUADO
C6	Actualizaciones al día de los servicios de red	Detectivo	Automática	Semanal	Si	Logs	Ingeniero Telecomunicaciones	Representante Legal	ADECUADO
C7	Capacitación personal encargado de la caja	Preventivo	Manual	Diario	si	Planilla de dinero	Personal de Caja	Representante Legal	ADECUADO

Ilustración 2 Control para el riesgo

Se implementará el control en cada riesgo evidenciado en la empresa para realizar la estructura y correcto manejo de los protocolos de seguridad en cada sucursal y así dar una correcta capacitación sobre los servicios y usos de estos:

			Control 1	Control 2	Control 3	Control 4	Control 5	Control 6	Control 7
			Canal Seguro para el envio y recibio de la información de las sucursales	Capacitación personal encargado de Datacenter	Cambio de Almacenamiento a la Nube	Manejo de información por protocolo Ipsec	Actualización de datos en tiempo real	Actualizaciones al día de los servicios de red	Capacitación personal encargado de la caja
Nº	Riesgo	Causas / Vulnerabilidades							
R1	PÉRDIDA O DETRIMENTO DE INFORMACIÓN POR:	Robo de información en los datos de las sucursales	X	x	x	x		x	
R2	DAÑO EN LOS ACTIVOS POR:	Manipulación indebida de los elementos de red		X					
R3	DEFICIENCIAS O DETERIORO DEL SERVICIO AL CLIENTE POR:	Perdida de la información almacenada por daño en disco duro.		x	x		X		
R4	DAÑO EN LOS ACTIVOS POR:	Fallas de envío y recibido de la información de las demas sucursales		x	x	x	x		
R5	DEMORAS EN LOS SERVICIOS PRESTADOS Y EJECUCIÓN DE LOS PROCESOS POR:	falta de información sobre inventario en sucursales			x		x		x
R6	INTERRUPCIÓN DE LOS SISTEMAS / PROCESOS POR:	fallas de seguridad en las estaciones de servicio de red	x			x	x	x	
R7	PÉRDIDAS ECONÓMICAS POR:	Mal calculo de caja			x		x		x

Ilustración 3 implementación de controles a los riesgos

Nº	Riesgo	Riesgo inherente	Efecto del control en las vulnerabilidades	Probabilidad	Impacto	Riesgo Residual	Opción de Tratamiento	Plan de tratamiento
R1	PÉRDIDA O DETRIMENTO DE INFORMACIÓN POR:	EXTREMO	Robo de información en los datos de las sucursales	Improbable	Mayor	MEDIO		
R2	DAÑO EN LOS ACTIVOS POR:	EXTREMO	Manipulación indebida de los elementos de red	Improbable	Mayor	MEDIO		
R3	DEFICIENCIAS O DETERIORO DEL SERVICIO AL CLIENTE POR:	ALTO	Perdida de la información almacenada por daño en disco duro.	Improbable	Mayor	MEDIO		
R4	DAÑO EN LOS ACTIVOS POR:	ALTO	Fallas de envio y recibido de la información de las demas sucursales	Improbable	Mayor	MEDIO		
R5	DEMORAS EN LOS SERVICIOS PRESTADOS Y EJECUCIÓN DE LOS PROCESOS POR:	EXTREMO	falta de información sobre inventario en sucursales	Posible	Moderado	BAJO		
R6	INTERRUPCIÓN DE LOS SISTEMAS / PROCESOS POR:	EXTREMO	fallas de seguridad en las estaciones de servicio de red	Improbable	Mayor	MEDIO		
R7	PÉRDIDAS ECONÓMICAS POR:	EXTREMO	Mal calculo de caja	Improbable	Mayor	MEDIO		

Ilustración 4 Riesgo Residual

Al implementar correctamente los controles para mitigar el riesgo se evidencia que el riesgo residual baja considerablemente beneficiando a la empresa para el buen manejo de la información.

Cronograma

En el cronograma diseñado junto con el Representante legal sobre los tiempos para implementar el proyecto de consultoría dividiéndolo en dos momentos en el cual el primero es la presentación a la empresa los costos y beneficios de estas para el proyecto sobre los Servicios de integración seguridad de la información en las sucursales y el siguiente momento es cuando el cliente ya tenga las sucursales para la implementación de los modelos y protocolos presentados en el informe.

Cronograma propuesta

Escala de tiempo Gantt

Presentacion y ejecucion de una propuesta seguridad informatica en la ampliación de la infraestructura de la organización Baracoff

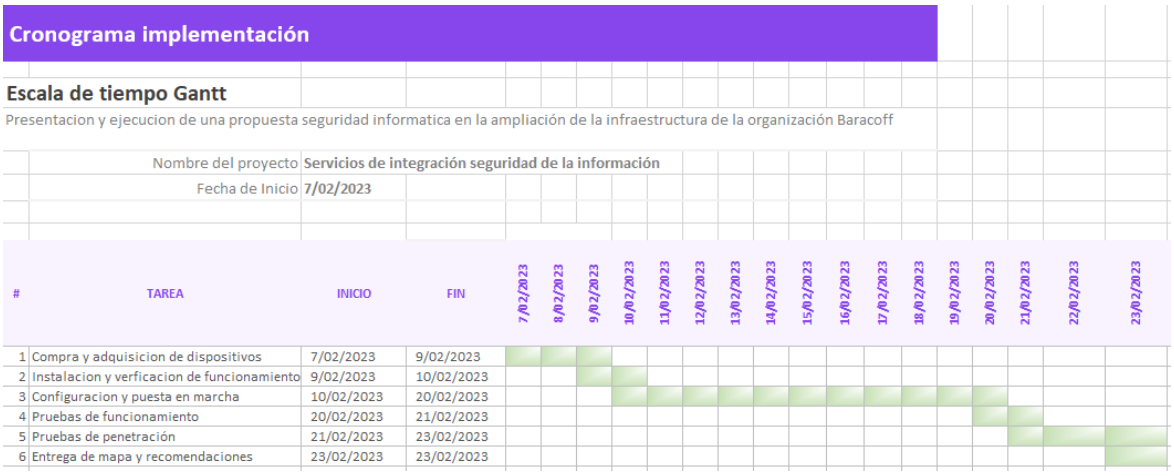
Nombre del proyecto **Servicios de integración seguridad de la información**

Fecha de Inicio **30/10/2022**

#	TAREA	INICIO	FIN
1	Presentacion de propuesta	30/10/2022	30/10/2022
2	Aceptacion de la propuesta	30/10/2022	30/10/2022
3	Reunion socios del proyecto	31/10/2022	31/10/2022
4	Relización de lista de prioridades	1/11/2022	2/11/2022
5	Recolección de datos	2/11/2022	2/11/2022
6	Procesamiento de información	3/11/2022	4/11/2022
7	Desarrollo del modelo a implementar	4/11/2022	5/11/2022
8	Análisis de resultados	5/11/2022	7/11/2022
9	Realización de documento final	7/11/2022	21/11/2022
10	Revision por parte de jurados	22/11/2022	22/11/2022
11	Correcion y presentacion de correciones	22/11/2022	22/11/2022

30/10/2022 31/10/2022 1/11/2022 2/11/2022 3/11/2022 4/11/2022 5/11/2022 6/11/2022 7/11/2022 8/11/2022 9/11/2022 10/11/2022 11/11/2022 12/11/2022 13/11/2022 14/11/2022 15/11/2022 16/11/2022 17/11/2022 18/11/2022 19/11/2022 20/11/2022 21/11/2022 22/11/2022

Ilustración 5 Cronograma Primer Momento



Cronograma implementación

Escala de tiempo Gantt

Presentacion y ejecucion de una propuesta seguridad informatica en la ampliación de la infraestructura de la organización Baracoff

Nombre del proyecto: **Servicios de integración seguridad de la información**

Fecha de Inicio: **7/02/2023**

#	TAREA	INICIO	FIN
1	Compra y adquisicion de dispositivos	7/02/2023	9/02/2023
2	Instalacion y verficacion de funcionamiento	9/02/2023	10/02/2023
3	Configuracion y puesta en marcha	10/02/2023	20/02/2023
4	Pruebas de funcionamiento	20/02/2023	21/02/2023
5	Pruebas de penetración	21/02/2023	23/02/2023
6	Entrega de mapa y recomendaciones	23/02/2023	23/02/2023

Ilustración 6 Cronograma Segundo Momento

Marco teórico

1.1 Diseño solución de seguridad unificada.

El presente diseño se basa en varias etapas de implementación de acuerdo con todo el análisis recopilado durante las visitas y reuniones técnicas con el personal encargado de la empresa, El primer paso es garantizar que la estructura tecnológica y políticas de seguridad estén alineadas con la solución a recomendar. A continuación, mencionara

Considerando lo anterior, se sugiere la implementación de MPLS que garantice la comunicación centralizada de las dos (2) sedes adicionales, con unas políticas de seguridad que permitirán que tanto internamente como externamente la información viaje de manera segura por la red.

Para el fortalecimiento de las pagina web de inventario de productos y servicios contables, se ha llegado a la conclusión que parametrizaremos los servicios por medio de métodos de seguridad interna en las plataformas, esto se modificara en paralelo con la implementación de políticas y segmentación de seguridad. Es importante aumentar la seguridad del Hosting CPanel, se podría realizar de dos (2) maneras.

- Fortalecer los servicios actuales con el proveedor del Hosting aumentando su paquete a premium, que blindará nuevos servicios como rendimiento en su CPU y RAM, además habilitará campos de seguridad que permitirá proteger la información alojada en estos servicios.

- Rendimiento de recursos optimizar con este dónde actualmente se alojan los servicios de página principal de la compañía, sistema contable e inventarios, se debe fortalecer esto adquiriendo el paquete premium que brinda mejor CPU y RAM en los procesos internos, además tendrán a disposición opciones adicionales de seguridad básica dentro del panel de administración de hosting de la compañía.

- Este diseño anterior lo hemos basado en la norma ISO 27001 que habla de la protección de la información que es nuestro principal foco de este desarrollo de mejoramiento e integración de seguridad.

1.2. Diseño de tecnologías de red

Es necesario tener claro en la empresa Baracoff su modo de conectividad y la importancia en que la información se pueda transmitir segura, cabe resaltar que en esta consultoría se dará a conocer a la empresa cual es la mejor manera para tener una forma de que esta información sea trasmitida correctamente, a continuación, se presentaran las redes. Servicios y protocolos adecuados para que funcione correctamente este tema.

1.1.2 Redes de LAN

Las redes LAN son tipos de redes pequeñas, redes de áreas locales que se encuentran en las empresas, oficinas, hogares, conectados generalmente por cables o Access Point. tanto si se trata de un edificio completo o de un local. Permite conectar ordenadores, impresoras, escáneres, fotocopiadoras y otros muchos periféricos entre sí para el intercambio de datos y órdenes desde los diferentes nodos de la oficina. Las redes LAN pueden abarcar desde los 200 metros hasta 1 kilómetro de cobertura.

1.1.2.1 Diseño LAN de las sucursales.

El diseño para las tres sucursales es el mismo, en donde se conectan PCs, impresoras y en la sede principal se cuenta con el servidor donde se almacenan los datos.

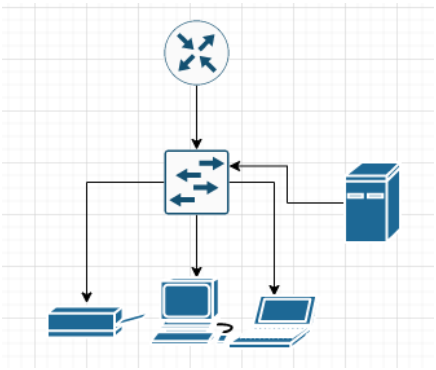


Ilustración 7 Diseño LAN Sucursal Principal

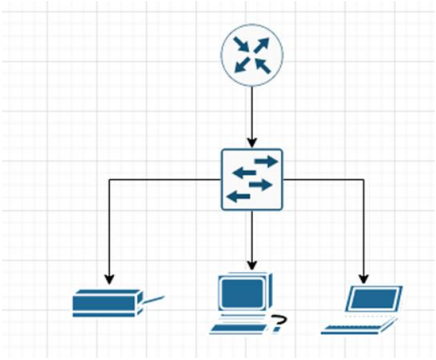


Ilustración 8 Diseño LAN Sucursales

1.1.3 Red WAN – MPLS

"Permite a la mayoría de los paquetes ser enviados en la capa OSI 2(Nivel de enlace) de forma preferente a que suban al nivel 3 (Nivel de Red). Cada paquete es etiquetado a la entrada de la red del proveedor de servicios por el router de ingreso. Todos los conmutadores de ruta subsiguientes ponen en marcha el reenvío de paquetes basándose en estas etiquetas (no miran la cabecera IP). Finalmente, el router de salida elimina las etiquetas y envía el paquete IP original hasta su destino final." (PATIÑO, 2019)

Ventajas:

MPLS ofrece un mecanismo sencillo para establecer túneles IPSEC donde se permite cifrar los datos por medio de los canales, este proceso garantiza la seguridad.

"Mejora del rendimiento, ya que al ser su naturaleza "muchos-a-muchos", los diseñadores de red pueden reducir el número de saltos entre puntos, permitiendo a su vez mejorar los tiempos de respuesta y rendimiento de las aplicaciones" (CISCO, 2005)

Desventaja:

Su aparente flexibilidad no es completa del todo, ya que ciertas características o su forma de implementación en el protocolo no han sido estandarizadas, dejándose al arbitrio de cada fabricante de red

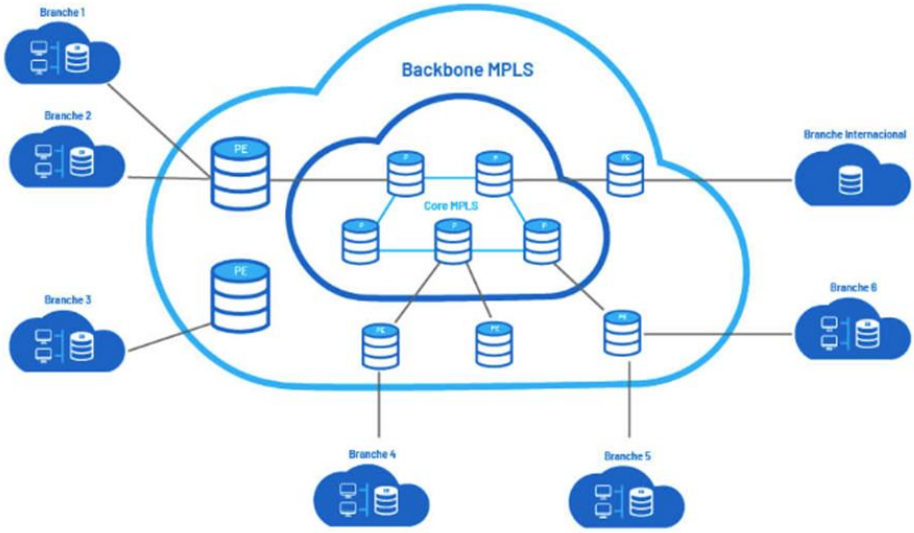


Ilustración 9 Backbone MPLS (Ecorp, 2015)

1.1.4 Servicios LAN

El servicio LAN se dispondrá correctamente en las sucursales cuando estas ya estén en funcionamiento dando a entender que la “Calidad de servicio de LAN en la capa de enlace de datos (capa 2 del modelo OSI). Incluye características para la priorización de

tráfico y la gestión de ancho de banda, con el propósito de minimizar la demora de la red mediante la clasificación, la señalización, la programación y el control del Costo de servicio (CoS).” (CISCO, 2022)

1.1.4.1 Mejoramientos tecnológicos

Se actualizará la infraestructura de la compañía en base a nuevas tecnologías para la conectividad entre las tres sucursales corrigiendo la escasez de equipos funcionales en la sede principal teniendo en cuenta la manera correcta de obtener un mejor desempeño en cuanto al manejo de los datos en la empresa.

1.1.4.2 Parámetros de seguridad

La infraestructura de una red de datos es la parte más importante de la empresa Baracoff ya que en ella se extraerá la información de las demás sucursales en tiempo real y al observar que la seguridad de esta red es débil es posible que no sea confiable para un manejo adecuado de esta.

Actualmente toda empresa necesita seguridad de la información ya que por el avance tecnológico es posible que se vea vulnerable ante intrusos o usuarios mal intencionado que intentan vulnerar la seguridad, donde se dará la solución con un robusto protocolo para evitar cualquier intento de vulnerabilidad hacia la triada de seguridad.

1.1.5 Equipos tecnológicos y cableado estructurado

1.1.5.1. Cableado Estructurado

Un sistema de cableado estructurado constituye un modelo global por el cual es posible transmitir voz, datos e imágenes, estos brindan necesidades integrales sobre servicios de transmisión fiable de la información., además proporciona un modelo de conexión física en medio de todas las zonas de trabajo de una estructura y se instala la necesidad de tener en cuenta el tipo de comunicación el cual se requiere conectar, esto con el fin de tener la capacidad de acoplarse a futuros cambios en los requerimientos que lleguen a ser necesitados conforme se presentan.

Existen diferentes tipos de cableado estructurado los cuales se han ido moldeando a las necesidades que sean requeridas por cada compañía dependiendo de sus propias circunstancias específicas. Cabe recalcar que un buen modelo supone una instalación de red que llegaría a ser muy útil para el funcionamiento de los equipos de una compañía, hablamos de la mejor vía por la que es posible la transmisión de datos y de igual forma ofrecer los mejores medios y herramientas a los trabajadores para su ejecución de funciones.

El resultado final que buscamos con un buen ecosistema de cableado estructurado es obtener el mayor beneficio en base a funcionamiento de una red local, no podemos olvidar que esto incluye como intuitivamente se esperara, cableado, conectores, canalizaciones, y básicamente cualquier dispositivo que conforme un sistema de telecomunicaciones, bajo estrictas reglas y estándares de calidad.

Gozar de un buen sistema de cableado estructurado nos permite acceder a diferentes beneficios a corto y largo plazo como lo pueden llegar a ser:

- La gran facilidad que conlleva el mantenimiento de uno de estos sistemas cabe aclarar que todo se basa en la organización inicial de este.

- El rendimiento y vida útil de una arquitectura de cableado estructurado es sinónimo de ahorro en costos y velocidades de procesamientos.

- La versatilidad es fundamental en los procesos de mejora a largo plazo ya que no nos veremos detenidos en ningún momento al acceder a mejorar de nuevas tecnologías.

- Precisamente ser un sistema nuevo, cuenta con medidas de seguridad las cuales son muy fiables, con componentes testeados para garantizar la tranquilidad de cualquier que los manipule.

- Transmitir datos rápidamente es sinónimo de ahorro en tiempos y por consiguiente, de ingresos.

- El orden es clave en cualquier compañía, si hablamos de armonía estética siempre contaremos con una apariencia limpia y ordenada de nuestros equipos.

1.1.5.2. ISO 27001

Muchas empresas tienen varios mecanismos para protegerse contra el software que puede afectar la continuidad del negocio, evitar que los empleados accedan a sitios web maliciosos o cifrar la información cuando se envía o recibe por correo electrónico. La forma más fácil de controlar todo esto es implementar un sistema de gestión de seguridad de la información basado en el estándar internacional ISO 27001. Sin embargo, muchas veces hay empresas que descuidan la protección física de los dispositivos, quizás porque muchas organizaciones piensan que, comprando un buen programa antivirus o alguna otra buena solución de software, se resolverán los problemas de seguridad de la información.

En cuanto a la protección física de los equipos, se debe distinguir entre dos tipos de medidas: las que afectan al equipo y las que afectan al equipo indirectamente. Se proporcionarán algunas recomendaciones y mejores prácticas para las medidas de seguridad informática para ayudar a su empresa a estar más segura mientras protege la seguridad de la información de su organización. Para brindar dicho asesoramiento, se utiliza el Anexo A de la norma ISO 27001 2013, que se enfoca en la seguridad física de los equipos al implementar un sistema de gestión de seguridad de la información.

Parece obvio que el equipo debe enchufarse y, en muchos casos, un UPS o un generador proporcionarán energía en caso de un corte de energía. A menudo se encuentran empresas que nunca han probado su producción de energía alternativa y no saben cuánto

tiempo pueden trabajar con esta energía alternativa. Por lo tanto, no solo es importante crear una alternativa, sino también definir un plan de mantenimiento y definir las tareas a realizar. Se recomienda encarecidamente un informe sobre todos los resultados. También hay empresas que trabajan en un centro común y tienen un generador que es gestionado por un tercero. Esto no debería ser un problema, ya que puede solicitar mantenimiento y pruebas a su proveedor de servicios.

1.1.5.3. Seguridad de cableado

En este caso, parece claro que las tecnologías actuales no son posibles sin cables y es muy común que nadie se moleste en organizar el cableado de forma estructurada. Sin embargo, para evitar errores, los cables no deben estar sueltos ni sin marcar, sino que deben recogerse y enrutarse de acuerdo con las rutas de cable preparadas. gabinetes, tableros eléctricos u otros materiales que protejan y guíen cables que deban ser utilizados y bloqueados.

En general, todos los usuarios modernos saben y saben que no deben escribir su contraseña en papel adhesivo y pegarla en la pantalla del equipo de cómputo o en el escritorio. Sin embargo, este problema no se puede ignorar, ni los usuarios deben asumir que saben qué acciones deben realizar en el escritorio de su computador. Por ello, es necesario establecer un conjunto de políticas que recuerden a los usuarios no dejar información sensible en ningún lugar, tal y como define el sistema de gestión de seguridad de la información ISO 27001. “Estamos seguros de que sabes que el software no es la solución a todo lo relacionado con la seguridad de los datos de tu negocio, por lo que

debes tener implementado un sistema de gestión de seguridad que cumpla con la norma ISO 27001 para proteger a tu equipo de ataques maliciosos por parte de hackers. diferentes caminos. La otra cara de la moneda es que existen muchas amenazas de seguridad física y los atacantes saben que los dispositivos son un punto débil en muchas organizaciones." (Arévalo Ascanio, Bayona Trillos, & Rico Bautista, 2015)

1.1.5.4. Equipos Tecnológicos

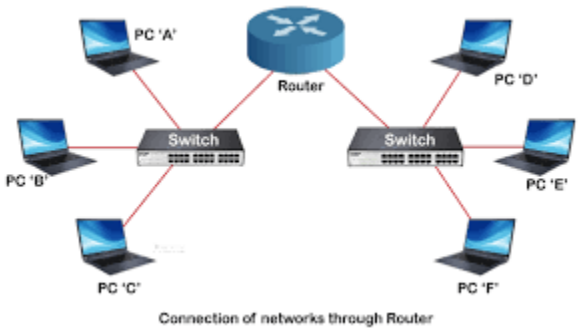


Ilustración 10 Equipos (JavaTPoint, 2018)

Switch (Conmutador)

Los switches son los bloques de construcción centrales de cualquier red. Conectan varios dispositivos como computadores, puntos de acceso inalámbrico, impresoras y servidores; en la misma red en un edificio o campus. Con la ayuda de un conmutador, los dispositivos conectados pueden compartir datos y comunicarse entre sí.

Conmutadores administrados

Le brindan una mejor protección, más funciones y flexibilidad cuando los configura para que coincidan con su red. Con esta mejor administración, puede proteger mejor su red y mejorar la calidad del servicio para los usuarios de la red.

Conmutador de red no administrado

Está diseñado para que pueda enchufarlo y usarlo sin configuración. Los conmutadores no administrados se utilizan normalmente para conexiones básicas. Por lo general, los verá en redes domésticas o en cualquier otro lugar donde se necesiten más puertos, como un escritorio, un laboratorio o una sala de conferencias.

Concentradores y conmutadores de red

Un concentrador de red es un punto de conexión centralizado para dispositivos en una LAN o LAN. Sin embargo, la cantidad de ancho de banda que los usuarios pueden compartir en una red basada en concentrador es limitada. Cuantos más dispositivos se agreguen al concentrador de red, más tiempo tardarán en llegar los datos. Un conmutador evita estas y otras limitaciones de los concentradores de red. Una red grande puede contener varios conmutadores que conectan diferentes grupos de sistemas informáticos. Por lo general, estos conmutadores están conectados a un enrutador que permite que los dispositivos conectados accedan a Internet.

Permiten que diferentes dispositivos en una red se comuniquen, mientras que los enrutadores permiten la comunicación entre diferentes redes. Un enrutador puede conectar computadores a una red que enruta paquetes de datos entre redes de estos. Un enrutador puede conectar computadores en red a Internet para que varios usuarios puedan compartir la conexión. Los enrutadores permiten conectar redes dentro de una organización o redes de varias sucursales. Y el enrutador actúa como distribuidor. Administra el tráfico de datos y elige la mejor ruta para los datos a través de la red para entregarlos de la manera más eficiente posible.

Router

Dirigen y controlan los datos de la red a través de paquetes que contienen diferentes tipos de datos, como archivos, mensajes y transmisiones simples, como interacciones de red. Los paquetes de datos tienen varias capas o partes; uno de ellos contiene información de identificación como el remitente, el tipo de datos, el tamaño y, lo más importante, la dirección de Protocolo de Internet IP del destino. El enrutador lee esta capa, prioriza la información y elige la mejor ruta para cada transmisión.

¿Cómo ayudan los enrutadores a su negocio?

Una herramienta común en la informática de red moderna, los enrutadores conectan a los trabajadores a la red de área local e Internet, donde ocurren casi todas las funciones comerciales importantes. Sin enrutadores, no podríamos usar Internet para colaborar, comunicarnos o recopilar información y aprender. Los enrutadores también pueden proporcionar protección. El software de firewall y filtrado de contenido integrado brinda protección adicional contra contenido no deseado y sitios web maliciosos sin comprometer su experiencia en línea. Pero un router no solo se utiliza para la transmisión de datos o para establecer conexiones a Internet. La mayoría de los enrutadores le permiten conectar discos duros y usarlos como servidores o impresoras para compartir archivos que pueden usar todos los usuarios de la red.

Los enrutadores principales proporcionan el máximo ancho de banda para conectar enrutadores o conmutadores adicionales. La mayoría de las empresas no necesitan enrutadores centrales. Sin embargo, las empresas muy grandes con varios empleados en varios edificios o ubicaciones pueden usar enrutadores centrales como parte de su arquitectura de red.

El enrutador perimetral, también llamado enrutador de puerta de enlace o "puerta de enlace" para abreviar, es el punto de conexión más externo de una red a redes externas, incluida Internet. Los enrutadores Edge están optimizados para ancho de banda y diseñados para conectarse a otros enrutadores para compartir datos con los usuarios finales. Los enrutadores perimetrales generalmente no ofrecen Wi-Fi ni la capacidad de

administrar todas las redes de área local. Por lo general, solo tienen puertos Ethernet; entrada para conectarse a Internet y varias salidas para conectar otros Router.

Los enrutadores inalámbricos o puertas de enlace domésticas combinan las funciones de los enrutadores de anillo y los enrutadores de distribución. Estos enrutadores son comunes en redes domésticas y conexiones a Internet. La mayoría de los proveedores de servicios ofrecen enrutadores inalámbricos con todas las funciones como equipo estándar. Si bien puede usar un enrutador inalámbrico ISP para su pequeña empresa, es posible que prefiera usar un enrutador empresarial para beneficiarse de un mejor rendimiento inalámbrico, una mejor administración de la conexión y seguridad.

Un Router Virtual es un software que le permite virtualizar una serie de enrutadores en la nube para proporcionarlos como un servicio. Estos enrutadores son ideales para grandes empresas con necesidades de redes complejas. Ofrecen flexibilidad, fácil escalabilidad y costos de acceso más bajos. Otra ventaja de los enrutadores virtuales es reducir la carga de administrar el hardware de la red local.

Un ancho de banda suficiente es importante para la experiencia del usuario. Garantiza el máximo rendimiento para múltiples usuarios: cuantos más usuarios, más ancho de banda se requiere. Puede expandir la red de su empresa agregando enrutadores o concentradores según sea necesario, pero el ancho de banda insuficiente en algunas partes de la red puede crear cuellos de botella. La mayoría de los enrutadores tienen una interfaz

basada en web que se conecta directamente al enrutador para la configuración y administración. Sin embargo, muchos fabricantes ahora ofrecen aplicaciones móviles diseñadas específicamente para dispositivos que ofrecen una interfaz más intuitiva y una configuración más sencilla. El enrutador debe proporcionar al menos protección de contraseña WPA o WPA 2. Algunos enrutadores también tienen un software de firewall que verifica constantemente los datos entrantes en busca de posibles programas malignos y virus. Otra herramienta importante es el filtrado de direcciones de control de acceso a medios (MAC), que utiliza identificadores específicos del dispositivo para filtrar a los usuarios y crea listas blancas o negras para el acceso a la red.

1.1.6 Protocolos de seguridad – Infraestructura de Red

1.1.5.1.1 IPsec

IPSec es la unión de varios modelos y formar funciones de seguridad en los conceptos de IP, donde principalmente trabaja en los 3 pilares de seguridad, los cuales son confidencialidad, integridad y autenticidad. Este sistema se basa en criptografía y se maneja varias tecnologías de seguridad de clave publica, alegorismos de cifrado, algoritmo de hash y otros métodos de niveles de seguridad, pero principalmente garantizar que nuestros canales a implementar a través de la red tengan grados de ciberseguridad difíciles de irrumpir. A continuación, se menciona los algoritmos de cifrado y hashes más usados:

Algoritmos de Cifrado

- DES
- 3DES
- IDEA
- Blowfish

Algoritmos de Hash

- MD5
- SHA-1, SHA-2 Y SHA-3
- BLAKE

En general IP security tiene la capacidad de soportar la gran mayoría de algoritmos criptográficos, no se mencionan todo, pero hay una infinidad que teniendo claridad de los procesos y que información se va a transmitir se usan los métodos que se ajusten a la necesidad, este protocolo nos garantizara a nivel de seguridad las siguientes políticas:

Confidencialidad: Se utiliza por medio de cifrados seguros ocultamiento de información, para evitar ser leída en el camino por entidades externas.

Autenticación: Manejara la información detalladamente verificando que el origen de cada documento e información sea el original.

Integridad: Garantiza que la información trasmitida de extremo a extremo no sea alterada por terceros en el transcurso, además verificar que este documento no tenga errores que ocasión daños

Protección: Evita a toda consta que al momento de capturar la información pueda ser interpretada.

También nos permite tener claves que se asocian a la seguridad de nuestros sistemas, con esto podemos tener más otro nivel de seguridad al momento de establecer VPN esta política permite que el usuario no manipule las contraseñas y evita que se haga manualmente.

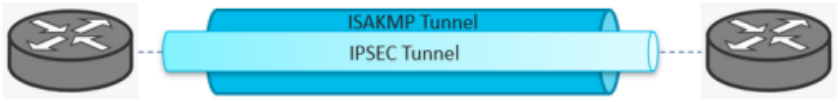


Ilustración 11 IPsec Tunnel (CISCO, 2017)

1.1.7 Políticas de seguridad

Se observa hoy en día muchos servicios de Internet que afecta exponencialmente la información que manejamos en nuestras empresas, esto se ve comúnmente por medio de las conexiones de red que se implementan en todo momento. Con la política de seguridad tendremos un conjunto de reglas que se aplican a las actividades del sistema y a los recursos de comunicaciones que pertenecen a una organización. Estas medidas de

protección incluyen varios elementos tanto físicos, lógicos y personal que maneja a diario las tecnologías de la red.

La política de seguridad determinar que se puede proteger y estructurar en el ámbito personal y laboral, definido detalladamente que cosas protegeremos por usuarios. Se proporciona una base de acuerdo con las aplicaciones y procesos que se tienen dentro de la organización, sabiendo que cualquier aplicación. proceso y equipo debe estructurar y diseñar para tener una seguridad dentro y fuera de la empresa.es importante describe responsabilidades del usuario, para discriminar y detallar las políticas de seguridad que le aplican a nivel de confidencial de la información, estos métodos suelen ser sencillos, pero siempre se ve el problema hasta con la creación de contraseñas. La política de seguridad supervisa la efectividad de las medidas de seguridad que se están tomando. Esta supervisión le ayudará a determinar si alguna persona podría intentar burlar sus defensas o podemos detectar espacios o procesos que generen baches de seguridad. A configuración se mostrará algunos objetivos de seguridad que se basa en tener métricas medibles para el desarrollo de la política.

Protección de Recursos: Garantizar que los usuarios autorizados puedan ingresar a su información, pero asegurar que los recursos a los que se accederá deberán tener categorización, para aislar de procesos que no pertenece, con la política se definen los roles y funciones e ingresos a plataformas dependiendo el cargo en la compañía.



Ilustración 12 Triada de seguridad (ServiTux, 2018)

Autenticación: Es objetivo es muy importante definirlo porque es uno de los niveles de la seguridad o la verificación que hace una persona ejecuta en sus sistemas operativos, plataformas, entre otros dentro de la organización, es importante que no se tengan riegos de seguridad como la falsa identidad o acceso personal no autorizado, es importante que en la política definida se siga al pie de la letra ya que esta tiene como protección la autenticación de usuario y contraseña midiendo los accesos y conexiones, además los certificados digitales que garantizan ser segura la plataforma además, no tendremos filtros ni ingresos de falsas personas.

"Una diferencia importante entre Internet y una intranet es la capacidad de confiar en la identidad del usuario que inicia la sesión. Por lo tanto, debe considerar seriamente la

posibilidad de utilizar unos métodos más potentes de autenticación que los que proporcionan los procedimientos tradicionales de conexión mediante nombre de usuario y contraseña" (IBM, 2021) es importante declarar que las políticas y categorías el usuario tendrá acceso verídico que garantiza su autenticidad y autorización al medio.

Integridad: Este apartado de seguridad es sin dudar a dudas es el más importante, ya que este es el que garantiza que la información que viaja sea la misma que se está enviando al receptor, para velar por este objetivo en la política se debe entender claramente los procesos internos de cada plataforma usada y la criticidad de la data. Este concepto desglosa un sin número de conceptos, pero se tomará como punto principal el de la integridad de datos en la organización.

Datos: Están asegurados por métodos de seguridad que permitían los cambio en tiempo real y no dejara que agentes externos manipulen o extraigan la información, nos ayuda en gran medida esta integridad a proteger los datos enviados y garantiza que estos lleguen sin ser alterado al destinatario, con este también tendremos nuestro almacenamiento seguro, pero también es importante tener medidas adicionales como Backups que, en caso de riegos, además tenemos información externa que en algún caso es uno de los grandes peligros de seguridad, pero las medidas correctas de seguridad mantendrá nuestra fuentes confiables y de no ser así desecharlas y analizarlas. Es de vital importancia que los sistemas o información pública se le dé un tratamiento diferente, ya

que es más difícil de controlar y analizar, pero si se posee la claridad de los métodos de seguridad podemos mitigar y proteger la información en todo momento.

No repudio: “Prueba de que se ha producido una transacción o de que se ha enviado o recibido un mensaje. El uso de certificados digitales y de la criptografía de claves públicas para firmar transacciones, mensajes y documentos es la base del no repudio”. (IBM, 2021) , es importante que para que esto tenga a lugar las dos personas que están transmitiendo la información deben estar de acuerdo esto se puede saber con la firma digital del sistema o plataforma de transferencia.

Confidencialidad: Para este con los métodos de cifrado seguro tales como Certificados digitales en nuestras plataformas y sistemas que garanticen la confianza al ingresar, además esto brinda nivel de seguridad cifrados con SSL en este caso, también tenemos las conexiones remotas a nuestros sistemas que se han vuelto hoy en día un punto clave, para nuestro trabajó diario, pero es importante que esto se realice por medio de conexiones seguras como VPN asegurando que el traslado de información por medio de las redes privadas y públicas en nuestra organización sea confidencial la política debe ser clara en su momento más con el personal que hace parte de la compañía a usar estos métodos para garantizar que la confidencialidad de la información que se usa siempre este segura e inalterable por externos.

Para tener unas políticas bien establecidas se debe tener varios lineamientos para el entendimiento de todos los lectores que verificarán y darán cumplimiento de las políticas de seguridad, es importante que todos los involucrados puedan entender claramente esto y

no sea solo concetos técnicos que en teoría no muchas personas entenderán, por eso es de vital importancia que se cumplan los siguientes pilares para que la política de la compañía sea cumplible.



Ilustración 13 Ciclo

1.1.7.1 Política de protección

La política de protección abarca varios temas y todos se centralizan en garantizar la protección, en toda organización debemos establecer seguridad a los elementos tecnológicos que día a día se usan para procesar los datos dentro y fuera de la empresa, debe tener unos controles rígidos que eviten la divulgación información a terceros, las actualizaciones periódicas y cultura seguridad del manejo de cómputo mitigaran en gran medida los niveles de vulnerabilidad que en la gran mayoría se ven por agentes externos,

pero también nuestras medidas deben tener parámetros que locativos que vigile y manejara una seguridad minuciosa a personal no autorizado a las áreas sin previa supervisión, se evitara extracción de datos e ingreso a intrusos.

1.1.7.3 Política de prevención de intruso

"Un sistema de prevención de intrusos es un conjunto de acciones predefinidas que tienen como objetivo prevenir el acceso de orígenes conocidos o desconocidos que tengan acciones sospechosas protegiéndolo de manera proactiva y eficaz". (Bernal Gutierrez & Dueñas Guerrero, 2019)

Los IPS realizan verificaciones para validar las firmas de las actividades más comunes en la red y ver que entes externos están intentando atacar, esta política mantendrá un monitoreo constante por medio de un software licenciado que realiza análisis completos, a comparación del firewall este método IPS él siempre está verificando en tiempo real los ingresos no conocidos y de inmediato pone en previo aviso al administrador por medio de alertas. Un punto importante con este método de seguridad es que este aparte de su análisis puede detectar y avisar ataques internos.

La detección basada en firmas encuentra los puntos de daño o maliciosos en nuestro conjunto de servidores que tengamos y servicios cotidianos que se manejan garantizando protección y medidas de prevención, es importante que el sistema este en constante actualización y las firmas digitales también para disminuir el número de avisos ya que este sistema no dejara de mostrar alarmas si no se corrigen estos errores de seguridad.

Con IPS podemos crear perfiles para proteger segmentos de red, lo que puede realizar es una captura de paquetes en tiempo real y analiza en detalle los puntos de vulnerabilidad y valida en general para evitar ataques. “Los IPS de red se configuran en modo promiscuo para que pueda analizar cualquier tráfico sin necesidad que tenga algún destino en específico, este análisis se puede realizar a nivel TCP y de aplicación y es en tiempo real para una mayor eficacia.” (Bernal Gutierrez & Dueñas Guerrero, 2019)

Los IDS es un sistema que permite monitorear el tráfico de la red, deferencia de las trazas que se realizan con un sniffer, este es capaz de verificar los códigos maliciosos en todo el detalle de los paquetes que proceso la red, esto sin dudar es efectivo por que a veces el filtrado incluso de puertos en el firewall no se ven. Al igual que el anterior este realiza un análisis en tiempo real mostrando todo lo encontrado y detectado en la capa de red. Con este método podemos mejorar las configuraciones que se tenga mal como las vulnerabilidades de seguridad y puertos definidos. Existe varios sistemas de detección de intrusos que pueden funcionar como mecanismos de monitoreo en tiempo real para varios sistemas que en algunas medidas el firewall se queda corto para el tema de administración y seguridad de los datos de la información, sin embargo, podemos unificar los procesos para que trabajen en conjunto.

1.1.7.4 Control de aplicaciones

Lo que se busca con esta política de control de aplicación es limitar el acceso a las páginas locales y externas y evitar baches de seguridad a demás tendremos un mejor control de uso de recursos tanto tecnológicos como de red que optimizara y controlara más centralizada la data a usar.

1.1.8 Topología - Sucursales Baracoff

Topología Sucursales Baracoff.

Considerando la información la información suministrada y recopilada en las visitas técnicas, se graficará la topología actual con la que trabaja la empresa actualmente y otra topología mostrando los nuevos diseños de conexiones e integración de las nuevas sucursales con los equipos tecnológicos que garanticé la comunicación seguridad entre ellas.

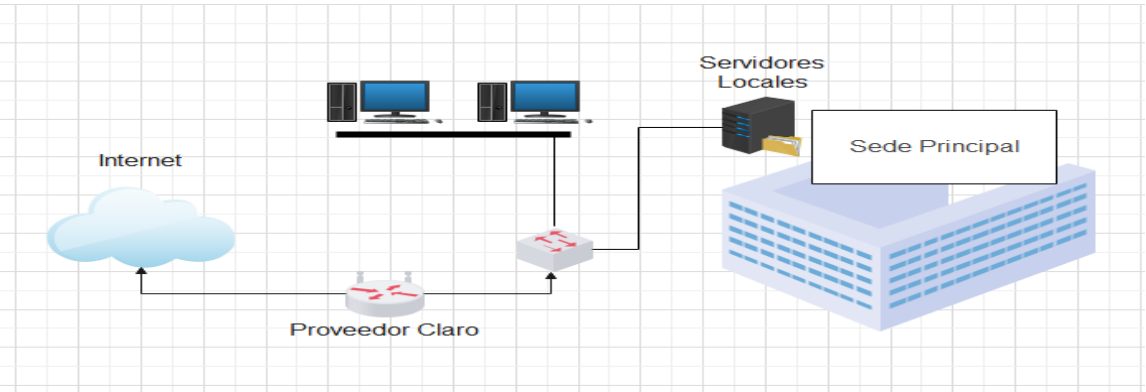


Ilustración 14 Topología Actual

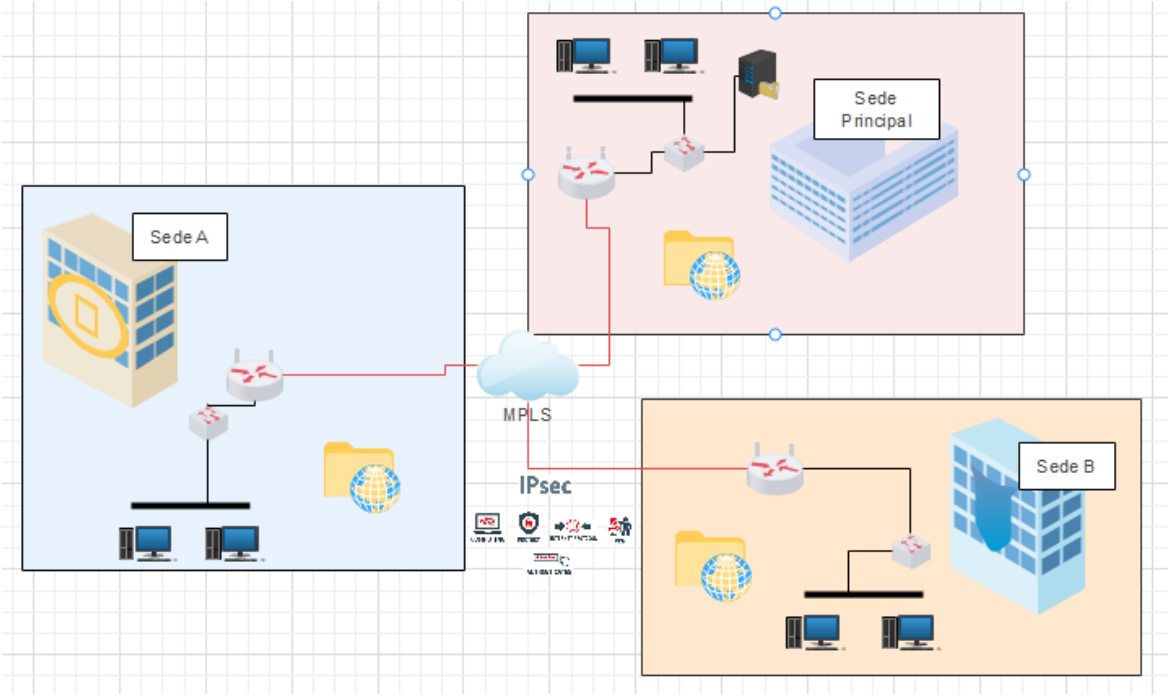


Ilustración 15 Diagrama topológico - Integración Sede A y Sede B

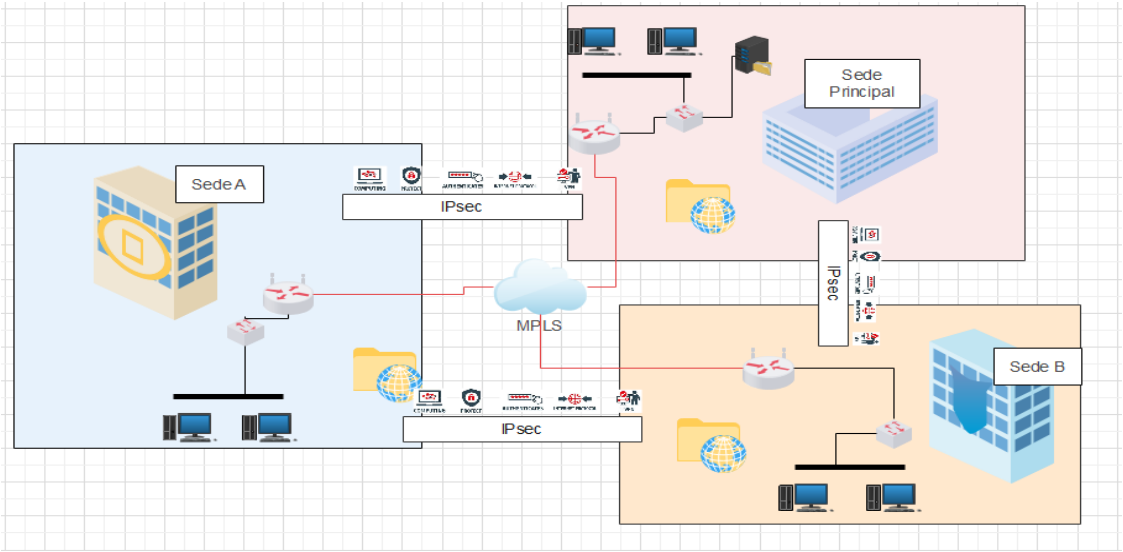


Ilustración 16 Diagrama topológico con protocolo IPsec

Requisitos Técnicos

En la implementación se debe cumplir con ciertos requisitos mínimos para el éxito del proyecto.

- Se debe contar con la administración de los equipos actuales de la compañía, para verificar parámetros iniciales e iniciar con las integraciones correspondientes.
- Se debe tener disponibilidad del personal involucrado, para coordinar paulatinamente las capacitaciones del uso adecuado de las herramientas de trabajo y metodologías de seguridad.
- Es necesario garantizar los canales de internet de cada sucursal.
- Es necesario realizar un plan de trabajo en conjunto con el líder del proyecto y establecer las metodologías de conectividad y políticas de acceso a documentos e información de la empresa.

Diseño Metodológico

Para esta consultoría a realizar se opta por un tipo de investigación correlacional en donde se pretende dar a conocer una solución mediante el estudio de relaciones variables en entornos reales, sin realizar una manipulación tangible de estas. Dado este caso se puede observar que al ser una consultoría a futuro no habrá dicha manipulación y el enfoque será cualitativo.

Como se mencionó nuestro tipo de investigación es correlacional, es decir que se debe realizar también una búsqueda de información secundaria toda esta basada en el análisis realizado a la empresa Baracoff de la cual nace la consultoría.

Las fuentes de información secundarias a las cuales se recurre son primero que todo la solicitud de la información de la infraestructura que actualmente tiene la organización Baracoff, la cual es una infraestructura bastante simple que consta de un computador y un sistema de cámaras que almacena sus grabaciones mediante un DVR, adicional a la ampliación de la infraestructura que esta organización pretende, posterior a esto se recurre a información basada en diferentes medios para poder establecer las condiciones para que Baracoff establezca la conectividad con sus sucursales de manera segura usando mecanismos tecnológicos que garanticen la seguridad de los datos.

Tercero se realiza una recolección de datos de forma investigativa para poder evaluar y determinar los siguientes datos en cuanto ataques de ciberseguridad ocurridos en el presente año, estos datos recolectados de diferentes revistas informativas:

- "Los errores humanos representan el 22% de los ataques de ciberseguridad" (CISCO DUO, 2020).
- "El 41% de los clientes afirma que no compraría a un negocio que haya sido víctima de un ataque de ransomware" (METRO, 2020).
- "El 94% de los ciberataques comienzan con un correo electrónico" (CSO Online).
- "El 72% de las violaciones de datos se dirigen a las grandes empresas" (FM, 2020)
- El 25% de los ciberataques incluyen phishing.

- Las bandas de delincuencia organizada son responsables del 55% de los ataques.

- “El 43% de las violaciones de datos son aplicaciones web basadas en la nube” (GlobeNewswire, 2020)

- “Colombia ocupa el cuarto lugar en la región con 11.200 millones de intentos de ciberataques y solo quedó por debajo de México con 156.000 millones, Brasil con 88.500 millones y Perú con 11.500 millones.” (ACIS, 2022)

Resultados

Dentro del principal hallazgo, se han medido en el marco del presente estudio el desarrollo de prácticas de seguridad, con las capacidades innovativas a nivel de equipos y el personal, dadas estas condiciones en la principal sucursal sobre la seguridad de los datos implementada, se fue estructurando, tomando como base el diseño actual en esta, de igual manera a corto plazo con las demás sucursales el flujo de la información de una manera segura.

Los aportes del proyecto en las gestiones tecnológicas, organizativas y financieras, incluidas en la compañía con la inversión en nuevos conocimientos. Algunas de estas actividades se usarán en un futuro para la anexión de las sucursales para el correcto tratamiento de los datos obtenidos diariamente en la compañía por el canal seguro estructurado por el protocolo IPsec.

Discusión

Dentro del análisis de los resultados obtenidos es posible precisar que Baracoff al ser una pequeña empresa y querer hacer una inversión en su expansión, también debe hacer esto mismo con su infraestructura tecnológica teniendo como prioridad la seguridad en los datos que esta posee.

Dentro de la consultoría se da a la organización metodologías para implementar y sugerir protocolos de envío y recibido de información de manera segura.

Conclusiones y recomendaciones

- El avance de nuevas tecnologías genera una clara necesidad de conexión y servicios de red los cuales hasta el más pequeño de los negocios pueden apostar para mejorar la forma en cómo administrar y controlar sus negocios.

- El protocolo IPSec permite operar a las aplicaciones de forma remota utilizando un acceso seguro y transparente donde se ofrece un buen servicio de confidencialidad que dispondría en la red local de su empresa.

- IPSec mantiene un estándar de seguridad, flexible y potente, de tipo flexible porque permite implementar cuyo adoptar a cualquier circunstancia, siendo modular para poder seleccionar de un conjunto de protocolos para su implementación, y potente por la arquitectura que lo conforma.

- Seguir recomendando a las personas en el sector público y privado, a la implementación de las tecnologías IPV6 donde se desarrollen nuevas redes, servicios y aplicaciones sobre IPV6 para así, poder ofrecer toda la seguridad de IPSec.

- La implementación IPSec requiere de un conocimiento amplio de diversas tecnologías y protocolos que podemos utilizar, para escoger la mejor que se adapte a nuestro caso o escenario, el hardware usado en la implementación de IPSec, como también nuevas tecnologías que se acoplen a él.

Bibliografía

ACIS. (01 de 11 de 2022). *ACIS*. Obtenido de ACIS: https://acis.org.co/portal/content/as%C3%AD-puede-evitar-los-ataques-cibern%C3%A9ticos-viviendas-y-empresas#:~:text=Este%20documento%20precis%C3%B3%2C%20que%20Colombia,y%20Per%C3%BA%20con%2011.500%20millones.

Arévalo Ascanio, J. G., Bayona Trillos, R. A., & Rico Bautista, D. W. (01 de 10 de 2015). *Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información.* Obtenido de Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información: https://revistas.udistrital.edu.co/index.php/Tecnura/article/view/9551

Bernal Gutierrez, C. L., & Dueñas Guerrero, J. A. (01 de 11 de 2019). *IMPLEMENTACIÓN DE UN SISTEMA DE PREVENCIÓN DE INTRUSOS EN LA.* Obtenido de IMPLEMENTACIÓN DE UN SISTEMA DE PREVENCIÓN DE INTRUSOS EN LA: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6265/00005169.pdf?sequence=1

CISCO. (10 de 08 de 2005). *CISCO*. Obtenido de CISCO: https://www.cisco.com/c/es_mx/support/docs/multiprotocol-label-switching-mpls/mpls/13736-mplsospf.html

CISCO. (05 de 02 de 2017). *CISCO*. Obtenido de CISCO: https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protocol.pdf

CISCO. (11 de 05 de 2022). *CISCO*. Obtenido de CISCO: cisco.com/c/es_mx/tech/lan-switching/lan-quality-of-service/index.html

CISCO DUO. (20 de 05 de 2020). *CISCO DUO*. Obtenido de CISCO DUO: https://duo.com/blog/unpacking-2020s-verizon-dbir-human-error-and-greed-collide

Ecorp. (05 de 10 de 2015). *Entel Corp*. Obtenido de Entel Corp: https://www.entel.cl/corporaciones/fija/public/images/redes-privadas/Esq02.jpg

FM. (13 de 07 de 2020). *FM*. Obtenido de FM: https://www.fm-magazine.com/news/2020/jul/data-insecurity-rise.html

GlobeNewswire. (19 de 05 de 2020). *GlobeNewswire*. Obtenido de GlobeNewswire: https://www.globenewswire.com/news-release/2020/05/19/2035340/0/en/Money-still-makes-the-cyber-crime-world-go-round-Verizon-Business-2020-Data-Breach-Investigations-Report-is-live.html

IBM. (14 de 04 de 2021). *IBM*. Obtenido de IBM: ." https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

JavaTPoint. (02 de 09 de 2018). *JavaTPoint*. Obtenido de JavaTPoint:

METRO. (08 de 06 de 2020). *METRO*. Obtenido de METRO: https://metro.co.uk/2020/06/08/who-responsible-when-cyber-attack-hits-company-people-say-ceo-12820037/

PATIÑO, H. D. (02 de 10 de 2019). *Construcción de una red MPLS .* Obtenido de Construcción de una red MPLS :

https://repositorio.upct.es/xmlui/bitstream/handle/10317/5251/tfg682.pdf?sequence=1&isAllowed=y

ServiTux. (22 de 03 de 2018). *ServiTux*. Obtenido de ServiTux: https://www.servitux.es/2018/03/22/ponentes-de-seguridad-informatica-en-el-i-congreso-transformacion-digital-en-los-despachos-de-abogados/