Estructura del documento para la estructura del Resumen Analítica Especializado -RAE

Tamaño de letra: 12

Tipo de letra: Arial

Interlineado: Sencillo

Borrar letra de color gris*

Fecha de Realización:	03/06/2023
Programa:	Especialización en seguridad informática
Línea de Investigación:	Proyecto aplicado
Título:	ANÁLISIS A LA SEGURIDAD DE LOS ACTIVOS TECNOLÓGICOS DE RED DE LA EMPRESA SEGUROS COMERCIALES BOLÍVAR S.A.
Autor(es):	Gutiérrez Ramírez Diego Andrés
Palabras Claves:	IWAN, PTES, SD-WAN, Infraestructura Tecnológica, Vulnerabilidad.
Descripción:	Trabajo de grado: Proyecto aplicado.

Fuentes bibliográficas destacadas:

AREVALO Ochoa, Adrián P. Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio. Revista Tecnológica-ESPOL, [En Línea] Cuenca, (Ecuador), 15 de noviembre de 2015 [Consultado 20 de abril 2022] disponible en: http://rte.espol.edu.ec/index.php/tecnologica/article/view/373/258

FUNCION PUBLICA, Ministerio TIC. [Sitio Web] Bogotá. Guía para la administración del riesgo y el diseño de controles en entidades públicas. [Consultado 30 de marzo de 2022] Disponible en: https://dapre.presidencia.gov.co/oci/normograma/Guia-administracion-riesgo-diseno-controles-entidades-publicas.pdf

RODRIGUEZ GAHONA, G. Análisis comparativo de los modelos defensa en profundidad y mspi, para la implementación de la seguridad informática en el sector privado del país. [En Línea] Monografía especialización seguridad informática, Universidad Nacional Abierta y a Distancia, 2020 [Consultado 20 de abril 2022] disponible en: https://repository.unad.edu.co/bitstream/handle/10596/38717/grodriguezgah.pdf?sequence=1&isAllowed=y

SABILLÓN, R., & Cano, J. J. Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. Revista Ibérica de Sistemas e Tecnologías de Informação, [Sitio web], 2019 [Consultado 16 de abril 2022]. Disponible en:

http://openaccess.uoc.edu/webapps/o2/bitstream/10609/124326/1/Sabillon_RISTI_Auditorias_Ciberseguridad.pdf	
Contenido del documento:	
Marco Metodológico:	Para el desarrollo de este proyecto la metodología implementada fue PTES la cual consta de 7 fases que garantizan una buena práctica de pentest efectivo a los sistemas e infraestructura objetivo. **Fase 1, Interacciones Previas:** Se establecen los alcances y profundidad que se requiera o necesite. Configuraciones físicas y lógicas de redes LAN, WAN y WLAN. **Fase 2, Recolección de la información:** Se recopila la información en equipos activos de red, LAN, WAN y WLAN. **Fase 3, Modelado de amenaza:** Se comparan estándares de configuración y buenas prácticas versus los encontrados en las maquinas y sistemas objetivo. **Fase 4, Análisis de vulnerabilidades:** Mediante aplicación de entrevista se valida estado de red, en aspectos de gobierno, tecnología, arquitectura. Además se evalúan requerimientos no funcionales como: capacidad, cumplimiento, disponibilidad, documentación, estándares, rendimiento y seguridad. **Fase 5, Explotación:** Esta fase tabula los datos indicados en la entrevista Agrupando los aspectos relevantes y dando una visión global del estado de la red de Seguros comerciales Bolívar S.A. **Fase 6, Post-Explotación:** Se evidencian y agrupan todas las recomendaciones en matriz indicando su relevancia y costo para el negocio. **Fase 7, Informe Final:** al llegar a esta fase ya se cuenta con información documentada

	la cual deberá ser organizada para presentarla de manera ejecutiva y técnica a quien corresponda en la compañía, aunque la metodología no cuente con los formatos específicos, si se requiere que se entreguen de manera detallada los hallazgos del pentesting, en estos informes se debe incluir las vulnerabilidades encontradas, en que contexto fueron halladas y bajo lineamientos, así como los objetivos alcanzados.
Conceptos adquiridos :	Con el desarrollo del trabajo de grado se logró profundizar en los conceptos de seguridad, obsolescencia de tecnología y buenas prácticas de configuración en equipos activos de red, los cuales son fundamentales para mitigar riesgos de seguridad informática. También se entendieron conceptos funcionales y técnicos con los cuales opera la red de comunicaciones de la compañía de Seguros Comerciales Bolivar S.A. tales como IWAN, SD-WAN. Y la importancia de estos a la hora de brindar una comunicación fiable y segura en una red donde se manejan altos flujos de información sensibles de los usuarios y clientes de esta compañía.
Conclusiones:	Una deficiencia crucial en la red de Seguros Comerciales Bolívar S.A. es la falta de actualización y documentación de inventarios de equipos de red, como Access Points y Switches. No existe un registro preciso de las cantidades ni de las ubicaciones físicas de estos equipos, lo que dificulta el acceso y la validación del tráfico de la red tanto de manera física como remota. La ausencia de mapas topológicos y de conexiones, así como de información sobre propagación y cantidades de VLAN, dificultan aún más la visibilidad y el control de la red. Para abordar este problema, se debe implementar un sistema de gestión de activos de red actualizado y completo,

	Configuraciones por defecto y prácticas de seguridad: Las configuraciones por defecto en los dispositivos activos de red presentan riesgos de seguridad significativos, ya que a menudo no se modifican ni desactivan. Estas configuraciones pueden incluir protocolos inseguros, contraseñas predeterminadas y puertos abiertos que pueden ser explotados por atacantes. Para mejorar la seguridad de la red, es necesario endurecer las configuraciones y reemplazar los protocolos inseguros. A pesar de los problemas mencionados, el análisis de la red de la compañía reveló ciertas fortalezas, como el uso de diferentes tipos y combinaciones de enlaces (MPLS, Internet dedicado e Internet de Banda Ancha) según la importancia y criticidad de las oficinas remotas. Esta diversificación permite a la empresa adaptar la conectividad y la disponibilidad de la red a las necesidades específicas de cada ubicación. Sin embargo, para aprovechar al máximo estos enlaces y garantizar una mayor seguridad.