Pontificia Universidad Católica del Ecuador
FACULTAD DE INGENIERÍA
COORDINACIÓN DE POSGRADO

PUCE

PUCE

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERIA

Trabajo de Titulación como requisito previo para la obtención del título de Magíster en Tecnologías de la Información, mención en Gestión y Administración de TI.

ANÁLISIS DE VULNERABILIDAD EN INFRAESTRUCTURA DE RED UTILIZANDO OPENVAS/GVM EN UNA ESTACIÓN TELEVISIVA 2023.

Autor: Carolina Elena Alcívar Agurto
Director: Dr. Edison Javier Guaña Moya

Quito, marzo de 2023

DECLARACIÓN Y AUTORIZACIÓN

Yo, **CAROLINA ELENA ALCÍVAR AGURTO,** con C.I. **0915975338**, autor (a) del trabajo de investigación titulado **ANÁLISIS DE VULNERABILIDAD EN INFRAESTRUCTURA DE RED UTILIZANDO OPENVAS/GVM EN UNA ESTACIÓN TELEVISIVA 2023,** previa a la obtención del grado académico de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN, MENCIÓN EN GESTIÓN Y ADMINISTRACIÓN DE TECNOLOGÍA EN** la Facultad de Ingeniería:

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador (PUCE), de conformidad con el Artículo 144º de la Ley Orgánica de Educación Superior, de entregar a la SENESYT en formato digital una copia del referido trabajo de investigación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador (PUCE) a difundir, a través del sitio web de la biblioteca virtual, el referido trabajo de investigación, respetando las políticas de propiedad intelectual de esta Universidad.

Quito, 31 de marzo de 2023.

_____
CAROLINA ELENA ALCIVAR AGURTO
C.I. 0915975338

APROBACIÓN DEL TUTOR

En mi carácter de Director (a) – Tutor (a) del Trabajo de Posgrado titulado **ANÁLISIS DE VULNERABILIDAD EN INFRAESTRUCTURA DE RED UTILIZANDO OPENVAS/GVM EN UNA ESTACIÓN TELEVISIVA 2023**, presentado por la estudiante de maestría **CAROLINA ELENA ALCIVAR AGURTO**, titular de la Cédula de Identidad **N.º 0915975338** para optar al grado de Magíster en Tecnologías de la Información, mención en Gestión y Administración de Tecnología, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ingeniería.

En la ciudad de Quito, a los 31 días de marzo de 2023.

_____
DR. EDISON JAVIER GUAÑA MOYA
C.I. 1713265369
eguana953@puce.edu.ec
(+593) 0995000484

NOTA:
Se comunica que en el servicio de análisis Turnitin, el referido trabajo de titulación alcanzó el siguiente resultado: 8**%** índice de similitud con otras fuentes.

TURNITIN: INCLUIR HOJA DEL INFORME

CON EL PORCENTAJE

Tesis

por Carolina Alcívar

Tesis

INFORME DE ORIGINALIDAD

8%	7%	1%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

ENCONTRAR COINCIDENCIAS CON TODAS LAS FUENTES (SOLO SE IMPRIMIRÁ LA FUENTE SELECCIONADA)

< 1%

★ www.globalstd.com

Fuente de Internet

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, **CAROLINA ELENA ALCIVAR AGURTO**, titular de la Cédula de Identidad N.º **0915975338**, declaro que los resultados obtenidos en la investigación, como requisito previo para lo obtención del Grado Académico de Magíster en Tecnologías de la Información, mención en Gestión y Administración de Tecnología, son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos, que se desprenden del trabajo de investigación, y luego de la redacción de este documento, son y serán de mi sola y exclusiva responsabilidad legal y académica.

En la ciudad de Quito, a los treinta y un día del mes de marzo de 2023.

_____
CAROLINA ELENA ALCIVAR AGURTO
C.I. 0915975338

DEDICATORIA

A mi esposo Enrique por su paciencia y apoyo en el logro de mis metas.

A mi hija Isabel por empujarme a que siga creciendo académicamente.

A mi hijo Enrique, por su confianza en mí.

AGRADECIMIENTOS

Agradezco siempre a Dios por guiar cada uno de mis pasos.

Agradezco de forma especial a mi gran amigo Edison Espinosa quien me impulsó a seguir este estudio y por apoyarme a culminarlo.

Agradezco a mi tutor, el Dr. Edison Javier Guaña por su profesionalismo, guía y consejos que me permitieron culminar de este trabajo.

A los profesores de esta Maestría por sus valiosos aportes de conocimientos.

A mis compañeros de estudio con quienes armamos grandes grupos de trabajo.

Y finalmente a la querida PUCE por abrirme sus puertas del conocimiento.

.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERIA
MAESTRIA EN TECNOLOGÍAS DE LA INFORMACIÓN
MENCIÓN GESTIÓN Y ADMINISTRACIÓN DE TECNOLOGÍA

ANÁLISIS DE VULNERABILIDAD EN INFRAESTRUCTURA DE RED UTILIZANDO OPENVAS/GVM EN UNA ESTACIÓN TELEVISIVA 2023

Autor:
Carolina Elena Alcívar Agurto
Director -Tutor:
Dr. Edison Javier Guaña Moya
Fecha:
Marzo, 2023

RESUMEN

El presente trabajo tiene como objetivo elaborar un plan de análisis de vulnerabilidades informáticas en la red de un canal de televisión a través de la herramienta OPENVAS/GVM. La metodología se desarrolló en base a las recomendaciones de la norma ISO 27001 que tiene como punto determinante la evaluación de riesgo, teniendo entre sus fases la identificación de los activos, las amenazas, vulnerabilidades, entre otras, determinando como objeto de estudio a los equipos que forman parte de la red de transmisión al aire del canal. Se realizaron valoraciones de tipo cuantitativo y cualitativo para la identificar a las posibles amenazas enfocado principalmente al análisis de las vulnerabilidades informáticas usando la herramienta de escaneo OPENVAS/GVM la cual presenta soluciones sugeridas para corregir la vulnerabilidad y en conjunto con el proceso teórico y práctico permitirá al personal encargado de la Seguridad Informática del canal elaborar un plan de acción con los procesos a seguir para minimizar el impacto de dichas vulnerabilidades encontradas, permitiendo a la organización elaborar nuevos planes y estrategias para el tratamiento del riesgo que es otra de las fases de la norma ISO 27001.

Palabras clave: Análisis de vulnerabilidad, Verificación de ataques, OpenVAS/GVM, ISO 27001, escáner de vulnerabilidad

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERIA
MAESTRIA EN TECNOLOGÍAS DE LA INFORMACIÓN
MENCIÓN GESTIÓN Y ADMINISTRACIÓN DE TECNOLOGÍA

VULNERABILITY ANALYSIS IN NETWORK INFRASTRUCTURE USING OPENVAS/GVM IN A TELEVISION STATION 2023.

Author:
Carolina Elena Alcívar Agurto
Director - Counselor:
Edison Javier Guaña Moya, Ph.D.
Date:
December, 2022

ABSTRACT

The objective of this work is to elaborate a plan for the analysis of computer vulnerabilities in the network of the television channel through the OPENVAS/GVM tool. The methodology was developed based on the recommendations of the ISO 27001 standard, which has risk assessment as a determining point, having among its phases the identification of assets, threats, vulnerabilities, among others, determining the equipment as the object of study that are part of the channel's on-air transmission network. Quantitative and qualitative assessments were carried out to identify possible threats, focused mainly on the analysis of vulnerabilities using the OPENVAS/GVM scanning tool, which presents suggested solutions to correct the vulnerability and, together with the theoretical and practical process, will allow the personnel in charge of the channel's Information Security to prepare an action plan with the processes to follow to minimize the impact of said vulnerabilities found, allowing the organization to develop new plans and strategies for risk treatment, which is another of the phases of the standard ISO 27001.

KEY WORDS: vulnerability analysis, attack verification, OpenVAS/GSM, ISO 270001, vulnerability scanner.

INTRODUCCIÓN

La seguridad de la información toma cada día mayor importancia tanto a los encargados del área de tecnología como de la Alta Gerencia de las organizaciones debido a la serie de ataques de bastante relevancia que han tenido importantes organizaciones entre ella incluso a Agencias de Seguridad Gubernamentales tales como la del Gobierno de México en el año 2022, en la que se divulgó mucha información sensible sobre las fuerzas armadas de ese país (The New York Times, 2022). En el Ecuador la empresa estatal Corporación Nacional de Telecomunicaciones (CNT) sufrió de un ataque cibernético en julio 2021 afectando la administración y operación de la empresa (El Comercio, 2021). Esto demuestra la alta exposición que enfrentan las empresas a los ataques en redes de datos que podrían representar pérdidas de varias índoles tales como daños a infraestructuras lo que impulsa la necesidad de priorizar la seguridad de la información en este tipo de proyectos, más aún si son impulsado por el Gobierno de un país. Sin embargo, el estado ecuatoriano a través del Consejo Nacional de Telecomunicaciones (CONATEL) aprobó el Plan Maestro de Transición a la Televisión Digital Terrestre (TDT) para mejorar la calidad de la señal televisiva a través de tecnología digital con enlaces de redes de datos, pero a su vez dicha implementación puede pasar por alto el tema de seguridad si no está indicada como parte del proyecto. El canal de televisión objeto de este estudio ha migrado su tecnología de señal análoga a digital en todos sus equipos de comunicación con la implementación de sistemas informáticos y redes de datos, haciendo necesario un análisis de las vulnerabilidades que podrían afectar la operación en TDT.

En este trabajo se propone el uso de la herramienta OPENVAS/GVM que cuenta con una amplia base de datos de reconocimiento de vulnerabilidades y acciones recomendadas para mitigar o anular dichas vulnerabilidades.

CAPITULO I: en el cual se plantea la formulación del problema del problema junto con los objetivos tanto general como específicos y justificación del presente estudio.

CAPITULO II, se plantea las bases teóricas y conceptuales que sustentan el diseño de la presente propuesta de análisis de vulnerabilidades. Se indica la revisión de investigación, estudios, antecedentes, normas, artículos científicos y demás documentos electrónicos relacionadas con el presente trabajo.

CAPITULO III, sobre la metodología de trabajo, se detallan las técnicas, procesos para la recolección de información, población, muestra, operacionalización de variables y herramientas para dicha recolección de datos.

CAPITULO IV, trata de la presentación y análisis de datos a través de herramientas a aplicación estadísticas, así como el de la herramienta propuesta para el análisis de la información y fundamento de la presente propuesta.

CAPITULO V, establece la propuesta, presentación, objetivos, diseño y evaluación del análisis de vulnerabilidades en el canal de televisión.

Al final de este trabajo se encontrarán las conclusiones y recomendaciones que se encontraron en este proceso.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

En el canal de televisión, según los últimos informes que el Proveedor de Servicios de Internet (ISP Internet Service Provider) ha enviado de parte del ECUCERT con la detección de vulnerabilidades encontradas en la red de la empresa, estas se han incrementado con relación a años anteriores, generando mayores riegos en la operación. Esta situación se presenta luego del proyecto de infraestructura de televisión digital (TDT). En el Anexo 5 se observa el detalle de los códigos de ECUCERT.

Los informes muestran que existe una falencia en la protección de la red y se espera que estas se solucionen a corto plazo.

1.1. Formulación del Problema

Años atrás el concepto de seguridad de la información era un término relacionado a diseño de cifrados para la protección de los datos, pero hoy en día interactúa de forma directa con la economía de la empresa. Debido al auge de servicios en la nube, redes sociales y la navegación web, ha aumentado los casos de violaciones de seguridad en los sistemas informáticos, causando gran perjuicio a las empresas. Estas violaciones en tecnología son llamadas vulnerabilidades las cuales en su mayoría son causadas por usuarios poco colaborativos o de quienes no pueden distinguir un software seguro de otro que no lo es, sin descartar los malos diseños de los sistemas, en este punto la inversión en seguridad se vuelve un aliado estratégico.

Los canales televisivos en Ecuador a través del Ministerio de Telecomunicaciones (MINTEL, 2012) fueron notificados de la proyección de implementación de la televisión digital en Ecuador hacia el apagón analógico, este proceso comprendió la implementación de infraestructura e incorporación de equipos de planta, estudios y equipos de transmisión necesarios para la generación y operación de señales digitales, así como dispositivos de infraestructura de red para la comunicación y transporte de datos, para lo cual es necesario la contratación de un Proveedor de Servicios de Internet (ISP) para el servicio de portador de enlace de datos, así como para los servicios de internet. En la activación de este servicio debe considerarse que los canales de televisión en Ecuador según la Asamblea Nacional de la República del Ecuador (ASAMBLEA NACIONAL, 2015) deben cumplir la Ley Orgánica de Telecomunicaciones (LOT), dicha ley en su Capítulo II Art. 24 numeral 15 señala: “Adoptar las medidas para garantizar la seguridad de las redes”.

Es importante describir que, en varias ocasiones la cadena televisiva por medio del ISP ha sido alertada de riesgo de vulnerabilidades en sus sistemas a través del ECUCERT

(ARCOTEL, 2022) que es un gestor de incidentes de la Agencia de Regulación y Telecomunicaciones (ARCOTEL).

Con los antes expuesto, se presentan las siguientes preguntas en esta investigación:

- ¿Cuál es la situación actual de la red de datos en lo referente a temas de ciberseguridad en el canal de televisión?,
- ¿Cuáles son los procedimientos o tareas que ejecuta el personal de ingeniería del canal de televisión en el momento que son alertados de una vulnerabilidad?, y
- ¿Cuál sería el diseño de una propuesta de análisis de vulnerabilidades con el software OPENVAS/GVM, dirigido al Dpto. de Ingeniería del canal de televisión en el año 2023?

1.2. Objetivos de la Investigación

1.2.1. Objetivo General

Analizar las vulnerabilidades en la infraestructura de red usando la herramienta OPENVAS/GVM, dirigida al Departamento de Ingeniería del canal de televisión en el año 2023.

1.2.2. Objetivos Específicos

- Fundamentar los Sistemas de Gestión de Seguridad de la Información (SGSI) y las aplicaciones informáticas para el análisis de vulnerabilidades.
- Diagnosticar la situación actual de la infraestructura de red en el canal de Televisión en el año 2023, mediante entrevistas al personal especializado del área de Ingeniería.
- Analizar las vulnerabilidades informáticas en el Departamento de Ingeniería del canal de televisión utilizando el software OPENVAS/GVM
- Diseñar el plan de acción para el departamento de Ingeniería para la mitigar las vulnerabilidades en la infraestructura de red en el canal de Televisión en el año 2023.

1.3. Justificación

La adopción de televisión digital forzó el uso de redes de datos en todas las bases (torres y antenas) de transmisiones del país, implicó cambios en infraestructura, pero ésta debe ir de la mano con un software de gestión y control de riesgos a la red. Es importante señalar que la seguridad de los datos ha tomado relevancia con el incremento de la tecnología, el uso de internet a pesar de su amplio uso tiene como principal problema la seguridad de la información.

Actualmente los datos son activos muy valiosos para las empresas, el mal manejo puede ocasionar grandes pérdidas e incluso el cierre de la organización. En el caso del canal de televisión la emisión de la señal según la Ley Orgánica de Telecomunicaciones (LOT, 2016) no puede tener interrupciones sin que se hayan justificado previamente, por lo que una caída de la señal debido a la falta de prevención por fallos en la seguridad de la información no es justificable.

Adicional a esto es importante mencionar que la Constitución de la República del Ecuador (CRE, 2008, pág. 33) se estable el derecho a la protección de datos de carácter personal, la ley que controla dicho derecho está vigente desde Mayo 2021 (Asamblea Nacional, 2021) haciendo necesaria la implementación de sistemas de análisis de vulnerabilidades para proteger los datos y evitar las fuertes multas económicas e incluso retiro de frecuencias del canal de televisión de acuerdo a la infracción cometida según la ARCOTEL.

El uso del sistema abierto de evaluación de vulnerabilidades OPENVAS/GSM desarrollado por la empresa GreenBone Networks pretende ser un gestor de prevención de incidentes, empleando medidas correctivas a través de la aplicación de políticas de seguridad y creando informes de vulnerabilidades para gestionar las debilidades en la infraestructura de red, esto lo realiza mediante la verificación de puertos y servicios visibles con la opción de hacerlo de forma automática, Chalvatzis et al., (2019) en su estudio señalan que dentro de las ventajas de OpenVAS es que sus complementos están escritos en Nessus Attack Scripting Language (NASL) y que todos sus productos son de software libre teniendo licencia pública general (GNU GPL), haciendo que esta herramienta sea una excelente alternativa para su investigación de automatizar el proceso de evaluación de riesgos en una empresa sin incurrir en grandes costos gracias a su código abierto y gratuito, además según Richard Stallman, creador de GNU en el año 1983, el software libre respeta la libertad del usuario y promueve en su comunidad la solidaridad social, hecho destacado en Commnunity-Greenbone (2022) OPENVAS a través de sus múltiples tutoriales, foros, blogs entre otros.

Por lo antes expuesto es necesario que el canal de televisión cuente con una red segura que le evite problemas tanto económicos como la de pérdida de información sensible. El uso de una herramienta como OPENVAS/GVM permitirá analizar las vulnerabilidades y minimizar el riego de amenazas. OpenVAS se considera como una herramienta de código abierto confiable y de gran uso. De acuerdo con Vimala & Fugkeaw (2022) esta herramienta fue desarrollada por la empresa Greenbone Networks en el año 20016, dentro de sus funcionalidades tiene el análisis de vulnerabilidades en cualquier sistema informático conectado. Según el artículo científico “Uncover Security Weakness Before the Attacker

Through Penetration Testing" de Hines & Chowdhury (2022) las prácticas de piratería ética se realizan a través de pruebas de penetración para encontrar las vulnerabilidades tanto en la red como en los sistemas, software y aplicaciones web, recopilando la información de cada etapa de esta penetración con el propósito de generan un informe detallando cada vulnerabilidad y lo que ocurrió en esta explotación. Su estudio destaca lo invaluable que es tener este recurso con pruebas realistas de ataques en riesgo mínimo de equipos y luego con esta información reforzar la seguridad, también enfatiza la utilidad de herramienta OpenVAS para el escaneo de una gran cantidad de servicios en una amplia cantidad de hosts a través del uso de su base de datos de más de 55.000 vulnerabilidades.

Los avisos de ECUCERT hacia la empresa televisiva es una alerta del riesgo que tiene actualmente la organización frente a vulnerabilidades que antes en tecnología analógica no estaban presentes, la importancia de la ciberseguridad, de la protección de los datos hacen necesaria la implementación de la presente propuesta. Este proyecto tiene la finalidad de bajar el riesgo de seguridad, presentando la propuesta de análisis de las vulnerabilidades actuales para mejorar las defensas y la gestión de seguridad de la cadena televisiva. Con esto la continuidad del negocio estará más protegida y evitará grandes pérdidas tales como las económicas e incluso de reputación de la empresa.

Se pretende realizar con esta propuesta de investigación un diseño de un sistema de análisis de vulnerabilidad en infraestructura de red utilizando OPENVAS/GVM (Open Vulnerability Assessment System) partiendo desde un estudio inicial de las vulnerabilidades actuales con el fin de minimizar los riesgos del negocio.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1. Antecedentes de la Investigación

Desde la perspectiva de Wang et al., (2020), los sistemas informáticos son la fuente principal para procesar la seguridad y bienestar de los seres humanos, esto tiene como consecuencia que el nivel de tolerancia a las vulnerabilidades sea muy bajo. El uso de las tecnologías de la información y comunicación tienen un crecimiento acelerado que ha ayudado en múltiples formas a maximizar el tiempo, procesos y recursos. En esa misma línea, lamentablemente desde el enfoque de Wang et al., (2020), se establece que se han incrementado los ataques a los sistemas, en su investigación demuestra que entre el año 2017 y 2018 hubo un incremento del 30% de nuevas vulnerabilidades causando grandes pérdidas a las organizaciones, dando lugar a que la seguridad de la información se convierta en un eje fundamental en todo diseño de sistemas. En su investigación maneja las estadísticas de NVD (National Vulnerability Database), hasta el año 2018 por lo que se tomó la misma fuente para analizar el comportamiento hasta el año 2022, reflejando que el número de nuevas vulnerabilidades siguen en aumento tal como lo muestra la Figura 1, concluyendo su investigación indicando que el escaneo de vulnerabilidad es parte de la protección y seguridad de la red como un medio eficaz.

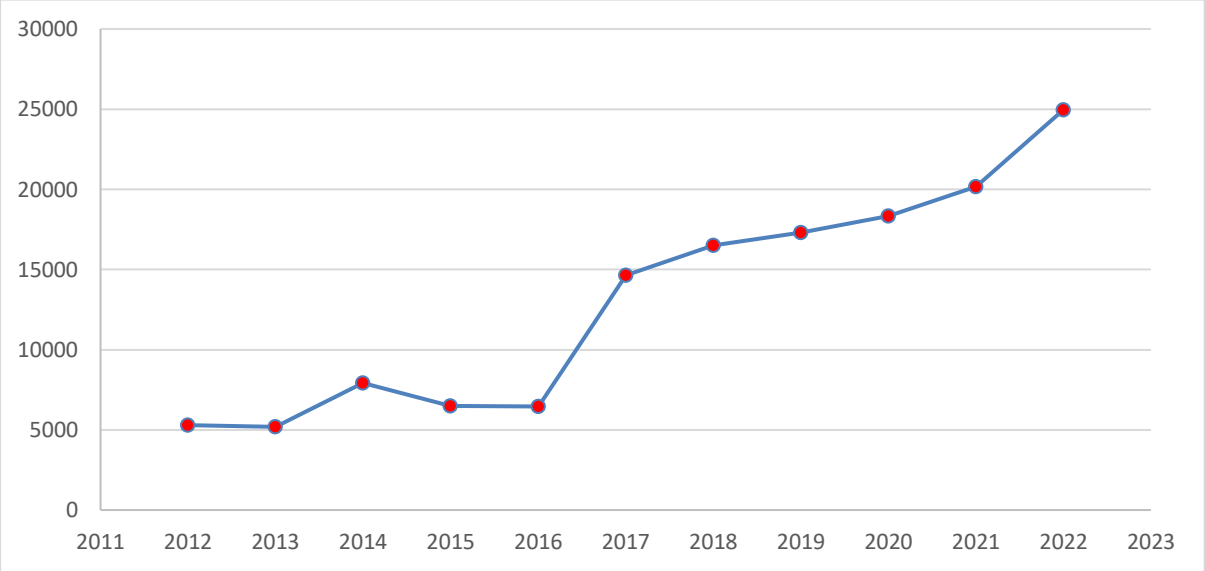


Figura 1. Estadísticas de nuevas vulnerabilidades de 2012 a 2022

Fuente: Adaptado de NIST (s.f.)

Según Gorbenko et al., (2020) la vulnerabilidad se define como una debilidad mediante la cual un intruso puede entrar acceder a dicha información vulnerable causando daño al aseguramiento de la información. Estos mismos autores mencionan que la vulnerabilidad puede estar en el sistema operativo, en la aplicación o en ambas, siendo la más crítica la del sistema operativo, su caso de estudio examinó datos estadísticos de cómo se revelan y eliminan vulnerabilidades tanto en el sistema de exposiciones como vulnerabilidades comunes en una amplia gama de sistemas operativos en sus diferentes arquitecturas que afecten la disponibilidad, integración y confidencialidad de los datos.

De acuerdo con las normativas técnico-legales del MINTEL (s.f.) se establece la obligatoriedad de pasar la señal análoga de los canales de televisión a señal digital, y enfatiza que esta tecnología obtiene muchas ventajas como la mayor integridad de la señal, mejor sonido, más flexibilidad, más funciones, muchas más ventajas por lo que ha sido implementado por la mayoría de los países en Latinoamérica. El canal de televisión en su señal original es análogo, trasmitiendo el video en amplitud modulada (AM) y el audio en frecuencia modulada (FM) con la alta probabilidad de tener interferencias, dependiendo de la distancia y ubicación del televisor receptor de la señal, usando un gran espectro de radiofrecuencia que en la tecnología TDT se optimiza. El Ecuador adopta el estándar japonés brasileño ISDB-T (Integrated Services Digital Broadcasting Terrestrial) de Televisión Digital Terrestre (TDT) reglamentado en el Registro Oficial No. 149 (2013) que tienen su canal de retorno a través de las conexiones de datos con internet permitiendo que los espectadores puedan acceder a datos enriquecidos, transmisión de datos vinculados que pueden aportar por ejemplo en un programa deportivo el detalle del juego e información de los atletas. Esto representa mejor tecnología, pero también se agrega el riesgo de vulnerabilidad. Un canal de televisión utiliza el internet para su señal streaming en medios digitales y también para su señal digital, sólo por mencionar a estos dos en la parte operativa, en caso de un ataque a la red, la señal al aire se vería fuertemente comprometida, confundiendo a los televidentes, generando pérdida de audiencia y pérdida económica al canal.

La investigación de Monev, (2020): “Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002” tiene métricas y recomendaciones para la gestión de riesgos de seguridad utilizando un método similar a COBIT 5 basado en el estándar ISO 27001:2013 el cual fue usado de forma exitosa. Este análisis permite identificar las deficiencias en el sistema de gestión de seguridad, evaluar el nivel de madurez de la organización a través de la generación de informes donde se destacan el nivel de cumplimiento de la norma ISO 27001 y las recomendaciones.

De acuerdo con la investigación desarrollada por Astakhova & Muravyov (2019) la acción de los intrusos puede ser intencional o no, en su estudio menciona que en el primer semestre del año 2018 el 64.5% de las filtraciones de información fue por usuarios internos, superior al año 2017, por ello enfatiza en la necesidad de análisis de comportamiento del usuario a través de registro de sucesos. Finalmente se concluye que el inconveniente es que los delincuentes informáticos se camuflan en el internet con perfiles falsos, páginas falsas, negocios o redes sociales falsas haciendo muy complicada la tarea de identificar a los criminales.

Los estudios de Aksu et al. (2019) sobre la usabilidad de los escáneres de vulnerabilidades, destaca la herramienta OPENVAS como el de mayor uso entre profesionales de TI por ser de código abierto y su amplia biblioteca para la detección de vulnerabilidades, en este mismo estudio se enfatiza que la usabilidad de los software de seguridad ded TI son de gran importancia para prevenir los ataques de forma proactiva. Para efectos de este estudio, la herramienta OPENVAS para el análisis de vulnerabilidades en la infraestructura de red fue seleccionada por ser un potente escáner, a sus caracterísitcas de código abierto, con una gran comunidad que realiza aportes significativos para la detección de vulnerabilidades.

Las investigaciones mencionadas son aportes porque enfatizan la necesidad de analizar vulnerabilidades informáticas para aumentar el nivel de protección, así como el de generar mecanismos efectivos de soluciones contra las intrusiones debido al aumento progresivo de vulnerabilidades.

2.2. Infraestructura de Red del Canal de Televisión.

El canal de televisión ha evolucionado con el avance de la tecnología y mayormente con la introducción de la Televisión Digital Terrestre (TDT). La implementación de este cambio hizo que toda la infraestructura de red migrara a componentes digitales con conectividad a redes de datos haciendo necesario el uso de switcher y demás dispositivos para este fin, también se vio en la necesidad de actualizar su software de gestión de contenidos, de monitoreo y control. Se mencionan a continuación las aplicaciones principales que usa el canal de televisión para la transmisión al aire de su contenido:

- **NEXIO**: Plataforma de gestión de contenidos digitales con arquitectura de servidor de alta definición (HD) y de definición estándar (SD) de televisión. Tiene varios componentes:
    - *FTP Server*: se encarga del equilibrio de la carga de las colas de transferencia, maneja transferencias simultáneas.

- *Farad*: el cual es un sistema de almacenamiento en línea de alto rendimiento.
- *PlayList*: Software de reproductor que permite obtener vista previa de los clips o contenidos multimedia a transmitirse en TV.

En la Figura 2 se detalla el flujo de trabajo de esta plataforma.

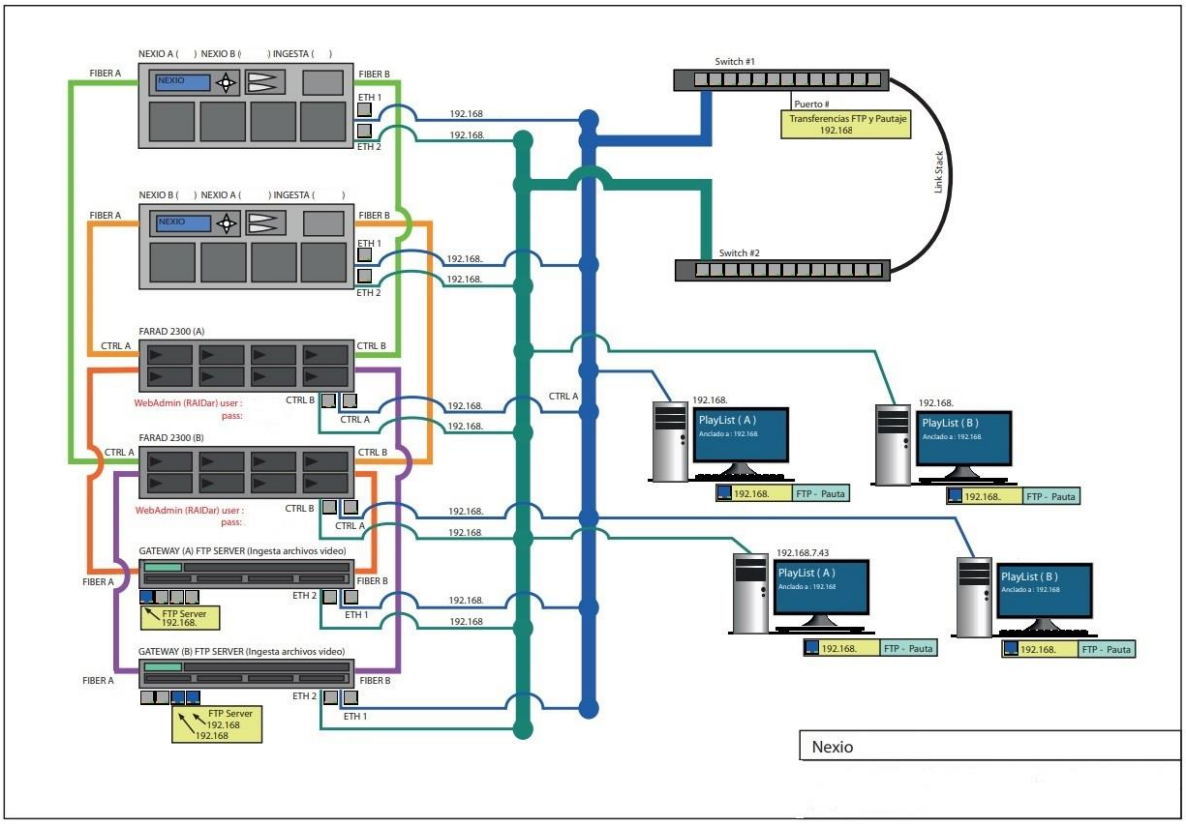


Figura 2. Sistema Nexio canal de televisión

- **GRASS VALLEY STRATUS**: Sistema de Producción de video y gestión de contenidos, gestión de flujos de trabajo de entretenimiento (GrassVAlley, s.f.). Permite la colaboración para administración del contenido de los clips. En la Figura 3 se observa el flujo de trabajo de este sistema con las respectivas conexiones de red.

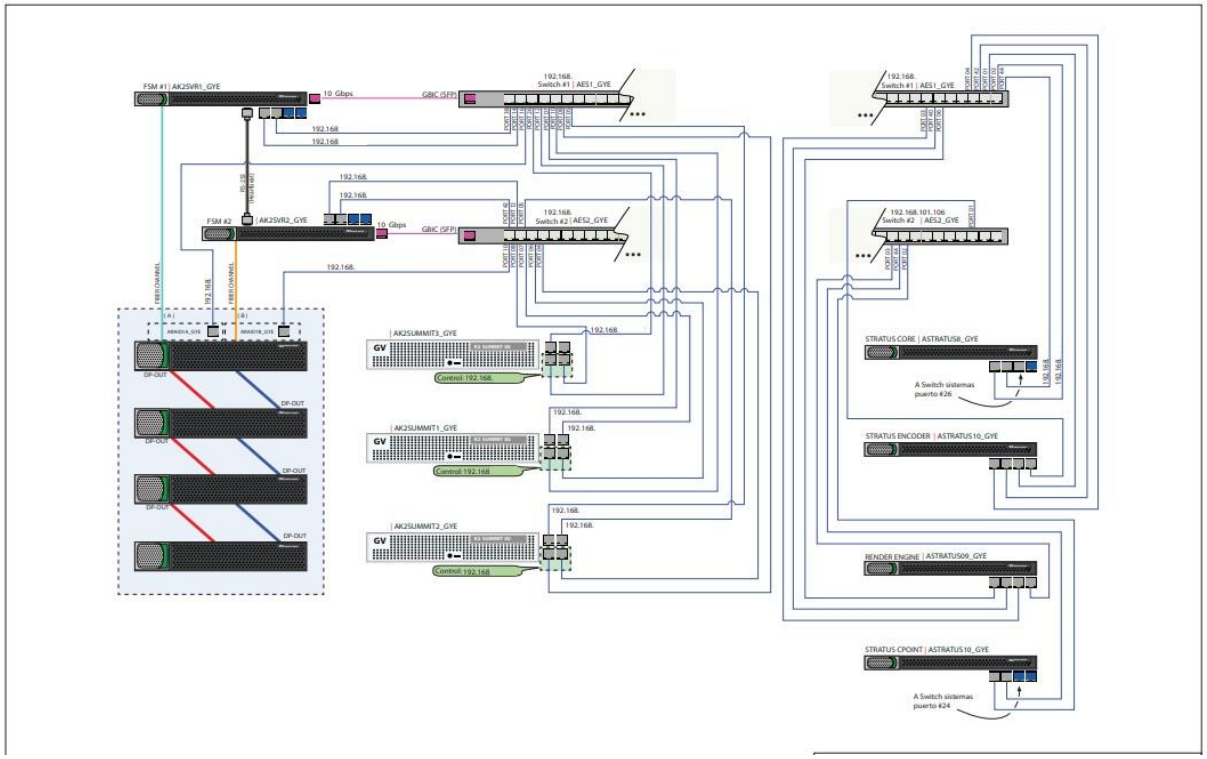


Figura 3. Sistema GrassValley Stratus

- **GRASS VALLEY MIRANDA:** Procesador modular de branding de canales, permite la renderización de imágenes y reproducción de clips de audio y voz en off.
- **THOMSON VIDEO NETWORKS:** También se incorporó a la red de infraestructura del canal equipos codificadores y decodificadores de la recepción de la señal del canal en cada una de las antenas de emisión de dicha señal. Su proceso consiste en codificar desde HD o SD y convertir en formatos MPEG-4, AVC o MPEG-2. Estos equipos también necesitan de red de datos para enviar la información digital con tecnología de compresión de videos. En la Figura 4 se muestra el panel back del decodificador de señal usado en la infraestructura de red del canal.

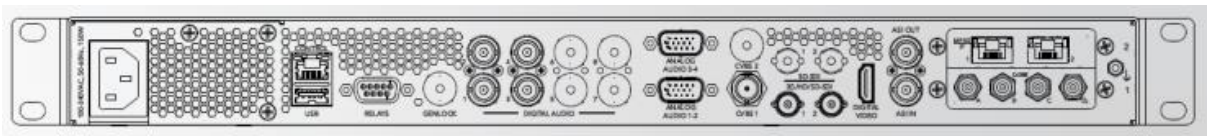


Figura 4. Decodificador de señal digital con puertos RJ45

Fuente: THOMSON, ViBE CP6000 Contribution Platform, s.f.

En la Figura 5 se muestra el panel back del codificador de señal digital con los puertos RJ45 para la conectividad.

Figura 5. Codificador de señal digital

Fuente: (THOMSON, s.f.)

En la infraestructura que se adoptó para la emisión de señal digital se incorporaron varios equipos de conectividad a la red de datos siendo necesaria la gestión de seguridad de estos para asegurar la transmisión al aire de la programación del canal, de acuerdo con la tecnología TDT adaptada para el Ecuador.

2.1. Análisis de Riesgos.

En esta propuesta de implementación se muestra una herramienta de análisis de vulnerabilidades que generan mucha atención debido a las mejoras de piratería informática que se centran en vulnerar servidores. Por ejemplo, si es vulnerado el servidor de Directorio Activo (AD Active Directory) será mucho más fácil distribuir políticas infectadas y causar daños a los datos y configuraciones de equipos anexados al dominio.

2.2.1. Amenazas

Los incidentes no deseados que causen daños a una entidad se denominan amenazas. Una organización puede tener diferentes amenazas de tipo accidental o intencionado en sus sistemas informáticos las cuales se clasifican en naturales, agentes externos y agentes internos. Dentro de las amenazas naturales se mencionan los incendios, inundaciones, fallas de energía, tormenta eléctrica, etc. Las amenazas con agentes externos son las ocurridas por ataques, sabotajes, virus informáticos, estafas, etc. Las amenazas de origen agente interno son las generadas dentro de la misma organización por el personal tales como descuidos, mal manejo de herramientas, sabotajes por personal insatisfecho, etc.

2.2.2. Vulnerabilidad

La palabra vulnerabilidad viene del vocablo latino vulnus, que significa herida o golpe, daño o perjuicio (RAE, s.f). Con esta definición, vulnerabilidad es alguien o algo que está expuesto a ser dañado o tiene alta probabilidad de recibir un daño. En el entorno informático es una debilidad en los sistemas al permitir que la amenaza se concrete y cause pérdidas en la empresa. Puede tener diferentes orígenes: fallos en el sistema, errores de configuración, falta de políticas o procedimientos, estos entre lo más destacados. En la Tabla 1 se muestra los

valores cualitativos y cuantitativos para el cálculo de probabilidad de que explote una vulnerabilidad.

Tabla 1

Cálculo de probabilidades de que explote una vulnerabilidad

Cualitativo	Cuantitativo	Descripción
Baja	1	La probabilidad de que la amenaza explote es cada año.
Media	2	La probabilidad de que la amenaza explote es cada mes.
Alta	3	La probabilidad de que la amenaza explote es cada semana.
Muy Alta	4	La probabilidad de que la amenaza explote es cada día o menos.

Nota: Evaluar el riesgo es la fase 5 dentro del proceso de análisis de riesgos. Fuente: Instituto Nacional de Ciberseguridad (INCIBE, ¡Fácil y sencillo! Análisis de riesgos en 6 pasos, 2017)

En la investigación científica de (Yosifova et al., 2021) se explica que existen varias organizaciones que recopilan y mantienen información de las vulnerabilidades de seguridad descubiertas. Este proceso consiste en asignar un identificador único a cada vulnerabilidad con una descripción del problema encontrado creando las bases de datos de vulnerabilidades, entre estas últimas las más conocidas en la base de datos de vulnerabilidades y exposiciones comunes (CVE Common Vulnerabilities and Exposures). Cabe resaltar que todos los días se descubren nuevas vulnerabilidades. En la Tabla 2 se muestra la clasificación de algunas vulnerabilidades.

Tabla 2

Clasificación de Vulnerabilidades

Tipo de Vulnerabilidad	Concepto
Buffer Overflow:	Desbordamiento de Buffer. Cuando se copian cantidades de datos superiores a la capacidad del buffer, puede provocar sobreescritura en las zonas de memoria adyacentes lo cual es aprovechado por ciberdelincuentes para ejecutar código malicioso.
Race Condition:	Condición de carrera. Vulnerabilidad en recursos compartidos que no controlan el acceso al mismo tiempo, cambiando estado de variables y obteniendo resultados erróneos.
Format String Bugs	Falta de validación en la entrada de datos, es un error de programación que puede provocar que se ejecute código malicioso en el ingreso de los datos.
Cross Site Scripting:	Ataques que pueden ocurrir con la ejecución de scripts en VBScripts o JavaScripts para hacer phishing y obtener los datos sensibles del usuario como usuarios y contraseñas.
Inyección de SQL	A través de la falta de validación de ingreso de datos u otras formas control a la Base de Datos puede provocar que se inyecte código SQL malicioso en el código de la aplicación SQL para alterar su funcionamiento.
Denegación del Servicio	Sobrecargas al servicio, pérdida de conectividad provoca que un servicio o recurso sea inaccesible para el usuario.

Tipo de Vulnerabilidad	Concepto
Windows Spoofing:	Ventanas que se le presentan al usuario con engaños para que acceda, siga la ventana y proporcione datos del ordenador para luego continuar con un ataque.

Nota: Los tipos de vulnerabilidades más comunes son SQL Injection y Cross Site Scripting (XSS). Fuente: Adaptado de (Bautista, 2022)

2.2.3. Análisis de Impacto

El impacto resultante de que una amenaza logre su objetivo se puede medir con la pérdida de ingresos y con los costos económicos de reparar el daño, por lo que la Alta Gerencia o propietarios de la organización deben calificarlo y entender su impacto. En la Tabla 3 se muestra la calificación de impacto definidas por NIST (National Institute of Standards and Technology) marco creado para que los negocios comprendan los riesgos en la seguridad de los activos de la información y puedan reducir estos a través del proceso de cinco fases:

1. Identificación
2. Protección
3. Detección
4. Respuesta
5. Recuperación

Tabla 3

Análisis de Impacto

Calificación del Impacto	Descripción
Alto	El impacto de que llegue la amenaza es muy costoso, puede provocar el cierre de la operación, comprometer su reputación o intereses.

Calificación del Impacto	Descripción
Medio	El impacto de que llegue la amenaza puede ser costoso, puede provocar que se detenga parcialmente la operación, puede provocar problemas con su reputación.
Bajo	El impacto de que llegue la amenaza puede provocar pérdidas, pero no de consideración.

Fuente: (NISCT, 2018)

2.3. Seguridad de la Información

2.3.1. Seguridad Informática

Las acciones y ejecución de planes de acción de medidas preventivas, de detección, corrección y recuperación orientados a proteger a los activos de la información se lo conocen como seguridad informática. En este concepto entra la confidencialidad, autenticidad e integridad conocida como la tríada CIA (Confidentiality, Integrity, Availability). La seguridad informática tiene controles físicos, técnicos y administrativos. Dentro de los físicos se puede mencionar el control de acceso al área donde se encuentran los dispositivos. En los controles técnicos entran las herramientas de gestión lógica. En las administrativas están los seguimientos de políticas de seguridad de la información dentro de la empresa, en seguridad de la información existen normativas internacionales, dentro de ellas la ISO 27001.

2.3.2. Gestión de Riesgos

El riesgo es la probabilidad de que una amenaza llegue al sistema informático a través de la vulnerabilidad con un impacto ya determinado por la empresa. En la Figura 6 se muestra la fórmula para medir el riesgo donde se observa a dos variables que se multiplican siendo la única manera de que no exista riesgo es que cualquiera de ellas tenga un valor de cero:

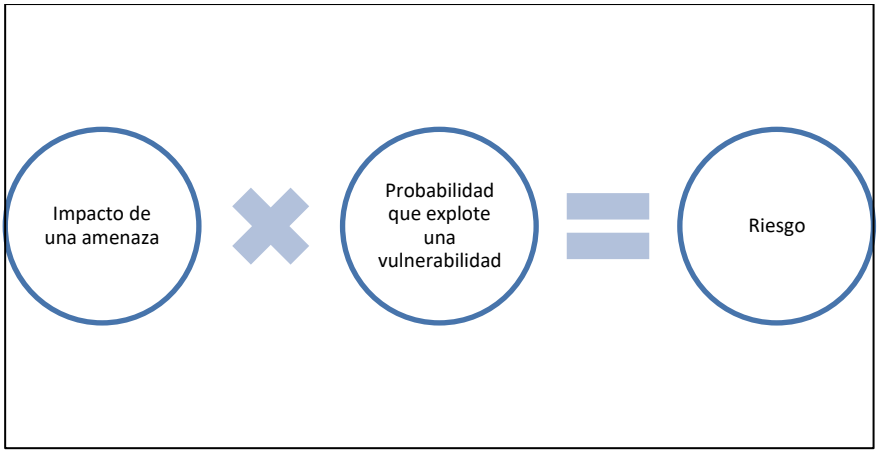


Figura 6. Fórmula de riesgo.

Fuente. Adaptado de INCIBE, ¡Fácil y sencillo! Análisis de riesgos en 6 pasos (2017)

En la gestión de riesgo se indica la criticidad de cada activo de la información con respecto a la continuidad del negocio y a su valor dentro de la empresa, por lo que es necesario identificar a cada activo para su correcta clasificación y evaluación de vulnerabilidad. El plan de remediación de la ciberseguridad es fundamental en la gestión de riesgos. En el marco de la seguridad ISO 27001, es necesario que el escaneo de vulnerabilidad esté indicado en la política de seguridad de la empresa, indicando frecuencia de ejecución. Una organización con seguridad sólida poder requerir que sus activos sean escaneados por lo menos una vez a la semana.

2.3.3. Ciberseguridad

Las formas, métodos, equipos, herramientas y demás elementos para proteger la seguridad de la tecnología de la información es definido como ciberseguridad. La seguridad está basada en tres elementos esenciales conocidas como la Triada (Ver Figura 7), en las tres se debe confirmar, asegurar que se cumple con la seguridad:

- **Confidencialidad**: Sólo personal autorizado tiene acceso a la información a la cual tiene competencia.
- **Integridad**: Los datos no son manipulados, ni modificados, tampoco se deben perder, en resumen, los datos no pueden verse comprometidos en ninguna forma.
- **Disponibilidad**: Los datos deben estar disponibles en el momento en que se necesiten. El acceso a los datos debe tener tiempos aceptables de respuesta.

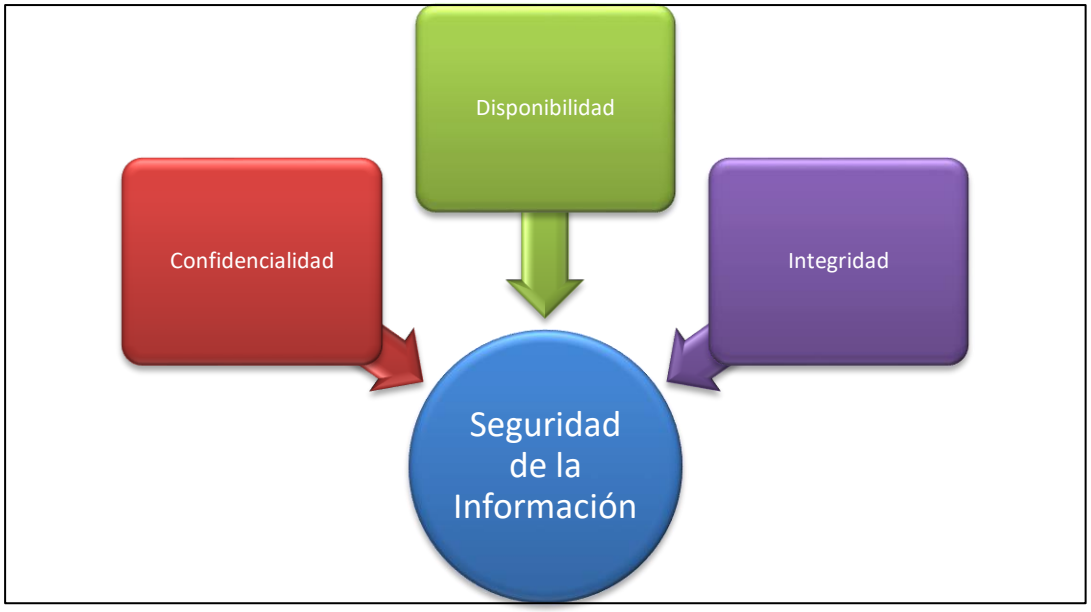


Figura 7. Fundamentos de Ciberseguridad

Estos tres elementos deben tener normas, políticas y procedimientos que garanticen su concepto.

2.4. Tipos de Atacantes.

En seguridad de la información existen el término de *atacante informático* que se define como una persona e incluso organización que intenta tomar el control de cualquier sistema informático con el objetivo de causar daño. Estos atacantes de clasifican en dos tipos: *atacantes pasivos* que logran ingresar a un sistema informático con el objetivo sólo de observar sin realizar modificaciones ni destrucción y los *atacantes activos* cuyo fin es dañar, modificar, destruir el objetivo alcanzado.

Hacker de sombrero negro: Atacantes activos, son criminales que usan sus capacidades y conocimiento para introducirse en redes informáticas para hacer daño a cualquier entidad, sea una empresa o una persona. Piensan en su propio beneficio o en su ideología. Son de difícil detección, dejan muy poco rastro, en caso de ser descubiertos, inician sus actividades desde otro sitio. El famoso hacker de sombrero negro, Kevin Mitnick[1], logró introducirse en muchas empresas de renombre tales como IBM y Motorola e incluso hackeó el sistema de alerta para la Defensa Nacional de los Estados Unidos de América, pudo ser arrestado y luego de cumplir su condena se convirtió en un hacker de sombrero blanco (Mitnick & Simon, 2021)

[1] Informático, apodado Cóndor, fue buscado por el FBI por diferentes delitos informáticos, comenzó su carrera delictiva a los 16 años cuando hackeó el sistema de seguridad de su colegio para ver las notas.

Hacker de sombrero blanco: Atacante pasivo. También denominados hackers éticos usan sus capacidades y conocimientos para emular un daño a una organización, crea el proyecto hipotético de penetración a un sistema con el objetivo de descubrir vulnerabilidades, fallas de seguridad, crear informes para que una organización se proteja ante ataques reales. Son expertos en ciberseguridad, usan sus conocimientos para denunciar problemas se seguridad y privacidad en sistemas. El famoso hacker de sombrero blanco Tsutomu Shimomura[2] contribuyó con sus conocimientos en ciberseguridad para detener a Kevin Mitnick y ponerlo en manos de la justicia.

2.5. Tipos de Ataques.

Los ataques informáticos intentan explotar alguna vulnerabilidad en las redes o sistemas informáticos para obtener algún beneficio económico o por el simple objetivo de causar daño. Los ataques se clasifican en activos y pasivos. El ataque pasivo se enfoca en monitorear para obtener información tales como contraseñas que pueda ser usada en futuros ataques activos por ello es una alerta para prevenirlos. En el ataque activo ocurre la acción directa de penetración con fines de daño, sabotaje, secuestro y otras formas de destrucción. Según el informe de Global Cybersecurity Outlook (2022) dentro del Foro Económico Mundial los tres tipos de ataques que más preocupan a los responsables de la seguridad de la información son: Fallo de la infraestructura debido a un ataque, robo de identidad y ransomware. En la Figura 8 se detallan las preocupaciones del personal encargado de seguridad de IT con respecto a los tipos ataques según el informe Global Cybersecurity de WEF & Accenture (2022).

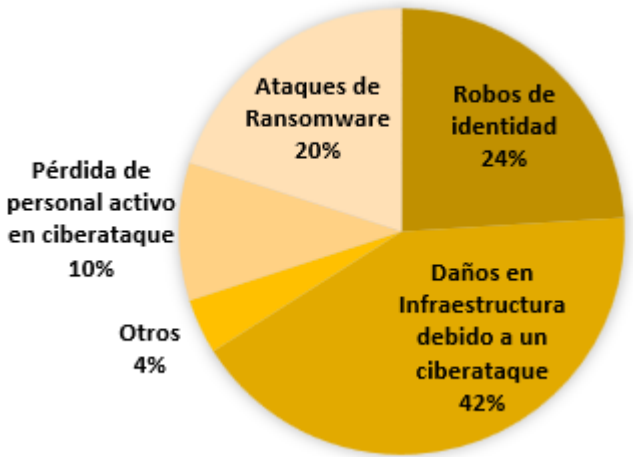


Figura 8. Preocupaciones de los responsables de TI sobre seguridad cibernética.

[2] Físico japonés, experto en ciberseguridad, ha sido consultor de varias agencias gubernamentales. Ayudó a atrapar a Kevin Mitnick al rastrear

Fuente: Adaptado de (WEF & Accenture, 2022)

La seguridad de los sistemas se ha vuelto prioritaria frente a los diferentes tipos de ataques que tiene entre sus principales causas:

Ingeniería Social: El arte de persuadir o influir mediante engaño a personas y convencerlas de que entreguen información es lo que se conoce como ingeniería social. También se usa esta habilidad de obtener información con el uso de la tecnología con el objeto de hackear un sistema.

Pruebas de Penetración: Las pruebas de penetración se hacen bajo un acuerdo legal entre la organización y hacker de sombrero blanco para piratear los sistemas de una empresa a través de cualquier medio que esté indicado en dicho acuerdo. Puede usar diferentes mecanismos incluidos en el acuerdo, pero no se limita a ellos. Comienza la prueba de penetración con la recopilación de información open-source es decir revisando la información de dominio público de la organización y de sus empleados, como ejemplo puede realizar búsquedas de Google, whois, correo electrónico, etc., esta fase es llamada pasiva y no está en el acuerdo. La siguiente fase, llamada activa, es la que protege legalmente al probador y consiste en varias actividades como la exploración de puertos, servicios activos para luego buscar las vulnerabilidades en lo encontrado.

La siguiente fase es usar herramientas para explotar la vulnerabilidad obteniendo acceso al sistema y conseguir mayores privilegios para obtener datos confidenciales y realizar tareas de mayor impacto en la organización. En la Tabla 4 se detallan algunas herramientas para la detección de vulnerabilidades en los sistemas informáticos sin ningún orden en específico.

Tabla 4

Herramientas de Análisis de Vulnerabilidades

Nombre de la herramienta	Descripción
Nessus	Herramienta flexible, de fácil uso, portable y con gran capacidad para escanear tanto una red grande como una pequeña. Es compatible con varios sistemas operativos tales como Linux, Microsoft Windows, Sun OS, Mac OS, FreeBSD, OpenBSD, Solaris entre otros.

Nombre de la herramienta	Descripción
Nmap	Es una potente herramienta con varias funcionalidades. Permite descubrir hosts en internet y verificar si están conectados, puede obtener información del tipo de sistema operativo, así como de los puertos que están en uso.
OpenVAS	Tiene un marco de trabajo con varias herramientas, dentro de las principales es el escáner de seguridad. Es fácil de instalar y usar.
Retina CS Community	Su principal función es encontrar vulnerabilidades en la red, problemas de configuración y actualizaciones pendientes.
Metasploit	Permite localizar y explorar vulnerabilidades, es muy usada para realizar pentesting.
Nexpose Community	Herramienta versátil, monitorea las amenazas y ayuda al desarrollo de las correcciones

Para el presente estudio se seleccionó la herramienta OpenVAS por ser una aplicación de bajo costo en relación con otras herramientas, lo que permite que pequeñas y grandes empresas puedan implementarlo sin depender del presupuesto. Adicional a su ventaja sobre costos posee las siguientes características:

- Tiene licencia GNU, es de código abierto
- Sus NVTs son actualizadas diariamente
- La comunidad GreenBone es muy amplia y está en crecimiento constante.
- Interfaz CLI amigable y flexible
- GreenBone Community Feed puede ejecutar 50,000 pruebas de vulnerabilidad.
- Los informes de fundamentos sólidos se pueden exportar en HTML, PDF, CSV.
- Tiene integración con OSSIM (Open Source Securiy Information Management) y Nagios herramientas para el monitoreo, detección y prevención de peligros en los dispositivos y en la red, ambas aplicaciones son de código abierto.

Otras herramientas no son de código abierto y el pago no es por perpetuidad (pago 1 sola vez) sino anuales con o sin soporte avanzado, ofrecen más características, compatibilidad en varios sistemas operativo que justifican el costo de sus licencias.

2.6. Normas y Estándares.

Las normas ISO (International Organization for Standardization) fueron creadas para asegurar la calidad, eficiencia, seguridad de los productos o servicios a través de la normalización de los procesos. En Telecomunicaciones también existen varios estándares que regulan los servicios de audio, video y multimedia para proteger su calidad.

2.6.1. Norma ISO 27001.

Es un estándar internacional desarrollada por ISO (Organización Internacional de Normalización) para la gestión de seguridad en los sistemas de información que tiene como objetivo proteger los activos de la información a través de la confidencialidad, integridad, disponibilidad y cumplimiento legal, incluye el tratamiento de riesgos de seguridad de la información. Está compuesto por varias fases en su implementación, dentro de dichas fases de se encuentra la planificación del SGSI que cuenta con varios procesos tales como el inventario de activos, identificación de amenazas, análisis de riesgos entre otros procesos llamados controles. En su control de gestión de vulnerabilidades técnicas tiene como objetivo el evitar la explotación de estas. El control de Organización de la seguridad de la información establece un marco de gestión para la implementación y operación de la seguridad de la información en una organización (ISO, 2013). Cada norma tiene su ciclo por ejemplo En Octubre 2022 se publicó la norma ISO 27001:2022 con nuevas actualizaciones, retirando ISO/IEC 27001:2013.

Familia ISO 27000: Las normas de la familia ISO/IEC 27000 tiene las mejores prácticas para la seguridad de la información, ciberseguridad y protección de la privacidad, en esta norma hay varios estándares (Ver Figura 9).

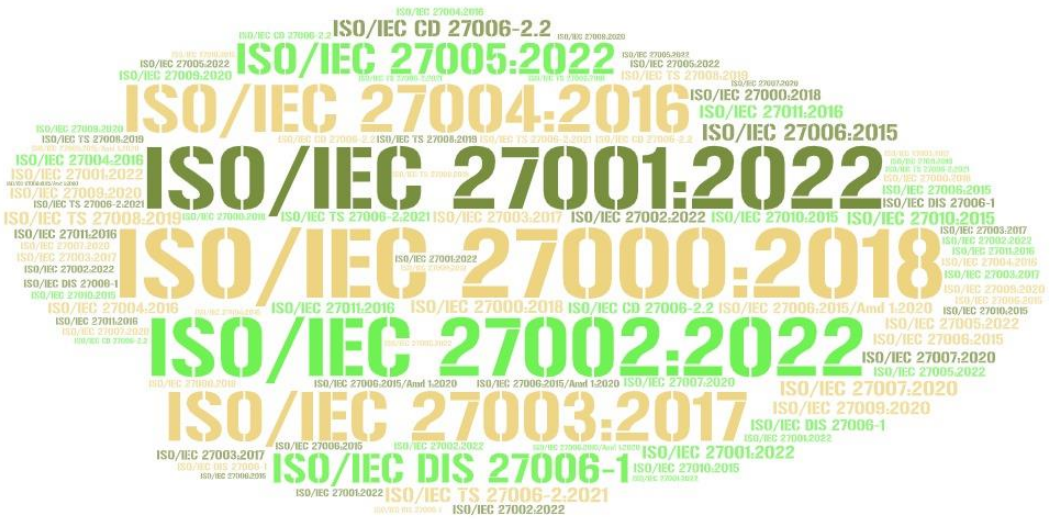


Figura 9. Familia ISO 27000.

Fuente: Adaptado de Catálogo ICS #35 Tecnología de la información

https://www.iso.org/standards-catalogue/

Se mencionan a continuación los más conocidos (normastecnicas.com, s.f.):

ISO/IEC 27000: Información básica sobre las normas de esta familia de seguridad de la información.

ISO/IEC 27001: Estándares para la implementación de un SGSI en una empresa.

ISO/IEC 27002: Certificación profesional.

ISO/IEC 27003: Guía específica para la implementación del SGSI.

ISO/IEC 27004: Estándares sobre medición e informes del SGSI.

ISO/IEC 27005: Estándares sobre gestión de riesgos del SGSI.

ISO/IEC 27006: Estándares de los requisitos para auditorías externas del SGSI.

ISO/IEC 27007: Estándares de las referencias para auditorías del SGSI.

ISO/IEC 27008: Estándares de los controles para auditorías del SGSI.

ISO/IEC 27010: Estándares de los SGSI para los negocios de intercomunicaciones.

ISO/IEC 27011: Estándares de los SGSI para los negocios de intercomunicaciones basado en ISO 27002.

2.6.2. Marco NIST Cybersecurity Framework (CSF).

El marco de seguridad de ciberseguridad NIST (Instituto Nacional de Estándares y Tecnología) es una metodología creada para reducir el riesgo asociada a las amenazas en la seguridad de la información. Se basa en estándares NIST SP 800-53, ISO/IEC 27001:2013, COBIT 5 y otros aceptados para controles en ciberseguridad, usando un enfoque participativo

y compromiso continuo para lograr mejoras entre las partes interesadas (gobierno, industria y academia). Tiene 5 funciones básicas que son la columna vertebral del Marco: identificar, proteger, detectar, responder y recuperar (Almagro, 2019).

En la *identificación* se da un entendimiento para que la empresa priorice sus recursos y esfuerzos según las estrategias para la administración de riesgos. En *proteger* se detallan las medidas que deberían ejecutarse para contener un posible ataque y garantizar los servicios de aplicaciones críticas. *Detectar*, ejecuta las actividades que permitan identificar cualquier posible evento de ciberseguridad para prevenirlo. *Responder*, tiene el plan de acción en caso de que un evento de ciberseguridad se presente. *Recuperar*, si un evento de ciberseguridad tuvo éxito, se ejecuta en esta fase los planes de contingencia y restauración de forma oportuna para continuar con la operación de forma inmediata.

2.6.3. Estándar ISDB-T.

Radiodifusión Digital de Servicios Integrados. Son un conjunto de normas para regular los servicios de audio, video y multimedia creado en Japón por ARIB (Asociación de Industrias y Negocios de Radios), esta norma usa el método de modulación OFDM (Multiplexación por división de frecuencias ortogonales) la cual proporciona una estructura segmentada. En Ecuador este estándar trabaja en el canal de los 6 MHz (MINTEL, s.f.). Dentro de las características técnicas se mencionan:

- OFDM para mejor control de interferencias. En la Figura 10 se observa la segmentación de este método.
- SFN (Red de frecuencia única)
- One-Seg, servicio de transmisión de audio y video para equipos móviles (MINTEL, s.f.)

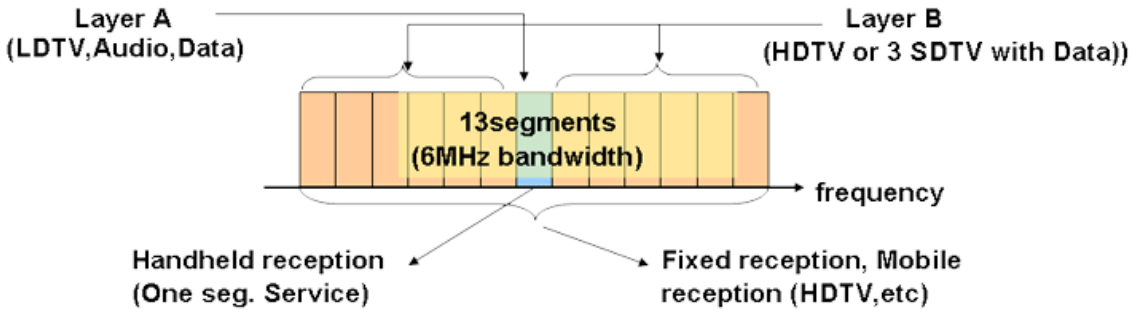


Figura 10. OFDM Segmentado

Fuente: Obtenido de https://www.dibeg.org/wp/wp-content/uploads/techp/what/image9.gif

2.6.4. Televisión Digital Terrestre (TDT).

La transición de señal analógica de los canales de televisión abierta a señal digital dio paso a las Televisión Digital Terrestre (TDT) con estándares de codificación de la información a través de algoritmos lógicos que se pueden identificar y corregir, comprime la señal haciendo más eficiente el uso del espectro radioeléctrico. Por el uso de la multiplexación puede emitir más canales a diferencia de la señal análoga donde sólo se podía transmisión un solo programa de televisión. Esto hace posible que el espectro sobrante pueda dedicarse a otros fines, pero uno de los avances más importantes es la forma de ver la televisión con mejor calidad de imagen y sonido, interactividad con el proveedor del servicio, más programación. Es importante aclarar que este sistema representa un gasto significativo para el canal de televisión debido a la necesaria actualización de su infraestructura por lo que debe garantizar su seguridad en todos los niveles.

2.7. Software OpenVAS/GVM.

En este estudio se utiliza la herramienta OpenVAS/GVM junto con funcionalidades del software Kali Linux. OpenVAS (Open Vulnerability Assessment Scanner), es una herramienta de escaneo de vulnerabilidades desarrollada por la empresa Greenbone Network desde el año 2006, se publica bajo licencia de código abierto, los complementos aún están escritos en Nessus Attack Scripting Language (NASL), sus distribuciones se crean en el sistema operativo Linux (GreenBone, 2022). Esta herramienta tiene su base en programación Nessus, tiene varias optimizaciones de rendimiento que le permiten enfrentar la creciente pruebas de vulnerabilidades. OpenVAS usa las pruebas de vulnerabilidad de red (NVT Network Vulnerability Test) para detectar vulnerabilidades en los equipos.

OpenVAS es compatible con la tecnología SSL (Secure Sockets Layer) que ayuda a proteger la información enviada entre sistemas, puede usarse incluso con otras herramientas como OSSIM (Open Security Information Management) para el monitoreo y administración en la protección de dispositivos. En su arquitectura general cuenta con los siguientes módulos (Ver Figura 11)):

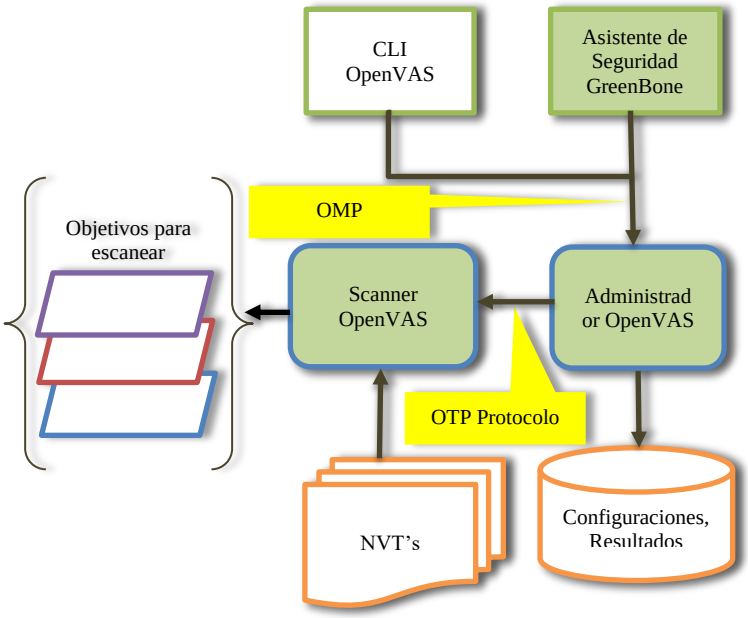


Figura 11. Arquitectura general de la herramienta OPENVAS/GSM.

Fuente: Adaptado de Kim et al. (2016)

- ***Greenbone Security Assistant (GSA):*** Aplicación que complementa el Manager. En la Figura 12 se observa una visión general del asistente.

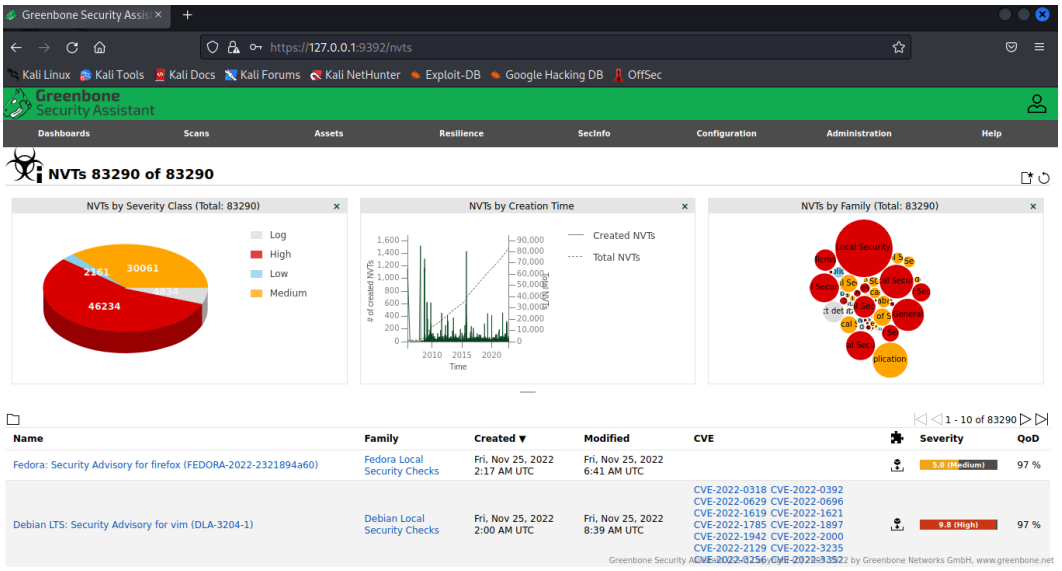


Figura 12. Overview de Greenbone Security Assistant

- ***OpenVAS CLI***: Aplicación que complementa el Manager. Maneja la compilación para controlar OPENVAS Manager. En la Figura 13 se observa la interfaz de ingreso a la herramienta en ambiente web.

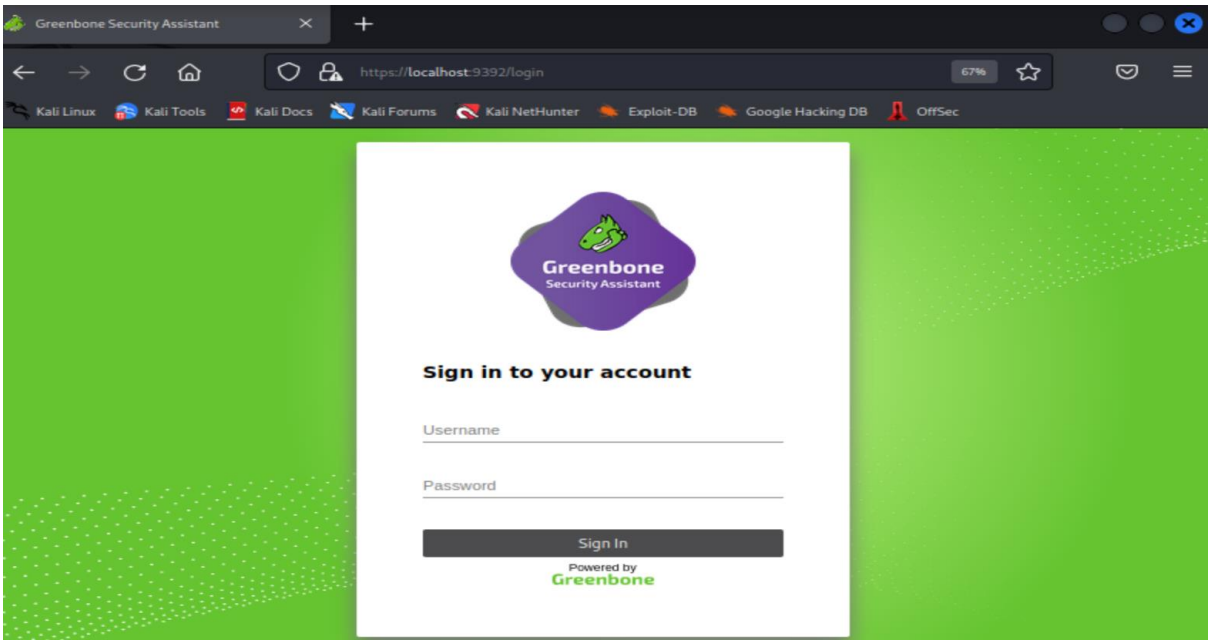


Figura 13.Interfaz en ambiente web de OPENVAS/GVM

- ***OpenVAS Manager***: Maneja el servicio principal con la administración de vulnerabilidades, así como el control de escáner mediante OTP (Open Transfer Protocol).
- ***OpenVAS Scanner:*** Núcleo principal que realiza las pruebas de vulnerabilidad de la red (NVT Network Vulnerability Test)

En sus inicios OpenVAS sólo era un motor para el escaneo de vulnerabilidades, luego se agregaron varios componentes creando una solución gestora de vulnerabilidades con la transparencia de ser un software libre. Esta solución se llama GreenBone Vulnerability Management (GVM).

CAPÍTULO III: METODOLOGÍA

3.1. Tipo de Investigación

La metodología de tipo aplicada busca generar mayor contenido y conocimiento en un problema de un sector productivo, realizada de forma directa (Cordero Vargas, 2009). Este estudio utiliza este tipo de metodología de aplicación directa para proponer una solución a un problema real en el canal de televisión con el conocimiento de vulnerabilidades que tienen los procesos en la conectividad, crear informes con propuestas de acción para resolver los problemas de seguridad, realizando una investigación práctica enfocada en el diagnóstico.

Para el desarrollo de este estudio se tomó como referencia la norma ISO/IEC 27001 en la parte de análisis de vulnerabilidades. Esta norma exige la realización del inventario de activos como una necesidad para gestionar y controlar lo que una organización tiene.

En la Figura 14 se muestra el flujo de los procesos de evaluación de riegos.

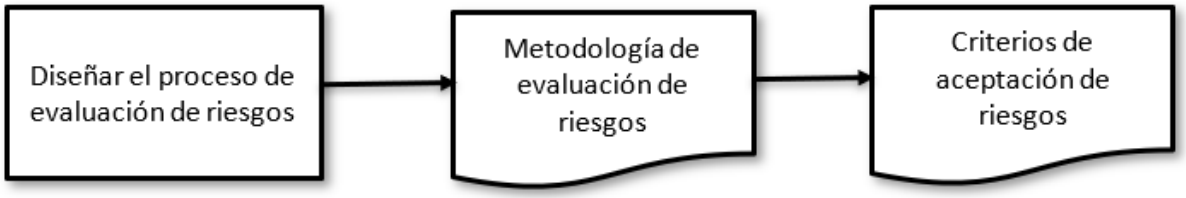


Figura 14. Procesos de evaluación de riesgos

La ISO 27001 en la parte operacional se enfoca en desarrollar la cultura organizacional de estar en alerta frente a los riesgos en la seguridad de la información y que tenga conocimiento de cómo enfrentarlos gracias a la implementación de controles. Esta implementación tiene beneficios económicos, comerciales, tranquilidad y más beneficios como dar confianza a los clientes. Las organizaciones dependen de la seguridad de la información y es con la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) que se concretará dicha seguridad. La norma ISO 27001 tiene como pilar el ciclo PHVA (Planificar, Hacer, Verificar, Actuar) representada en la Figura 15.

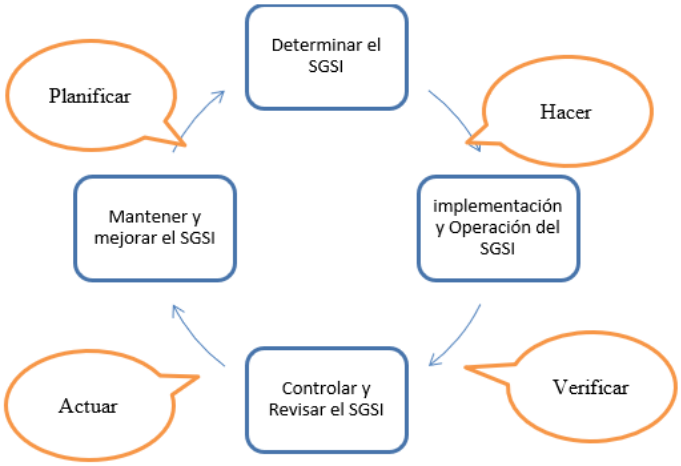


Figura 15. Ciclo PHVA (Planificar, Hacer, Verificar, Actuar)

Fuente: Adaptado de Berrío et al., (2016)

Esto proporciona el fundamento de mejora continua. La ISO 27001 es una guía en la identificación de riesgos de seguridad de la información, es la evaluación de riesgos el núcleo de todos SGSI, su diseño permite que la organización evalúe los riesgos asociados con un sistema. En su implementación segmenta el análisis de riesgos en (Ver Figura 16):

1. *Identificar los riesgos*
2. *Calcular el nivel de exposición al riesgo.*
3. *Identificar los controles de mitigación*
4. *Calcular el riesgo remanente*
5. *Aceptabilidad del riesgo remanente.*

Figura 16. Ciclo del análisis de riesgos.

Fuente: (INCIBE, s.f)

Evaluación de Riesgos: Se definen los niveles de amenaza de acuerdo con factores de aceptabilidad del riesgo para proteger los activos de una organización y que esta pueda operar según su misión objetiva, se definen estos en una tabla con los niveles de criticidad. En este caso de estudio para el canal de televisión se determinan los valores de acuerdo con la Tabla 5 con calificación de 0 al 9 donde 9 es muy riesgoso y 0 sin ningún riesgo.

Tabla 5

Evaluación y Calificación del Riesgo.

Puntuación del Riesgo (Probabilidad)	**Descripción (Impacto)**
Muy Alto (7-9)	Cero tolerancias al riesgo, muy crítico para el negocio, este nivel paralizará la actividad esencial de la empresa, no podrá continuar con la operación. Debe tomarse medidas de acción inmediatas.
Alto (5-6)	Crítico para el negocio, no es aceptable, la evaluación para minimizar este riesgo debe realizarse lo antes posible.
Medio (3-4)	El riesgo es aceptable, pero a corto plazo debe tomarse las acciones necesarias para mitigar el riesgo.
Bajo (0-2)	Se acepta el riesgo, no representa peligro para la operación del negocio, sin embargo, deben tomarse las medidas para mejorar la seguridad.

Fuente: Adaptado de INCIBE, ¡Fácil y sencillo! Análisis de riesgos en 6 pasos (2017)

3.2. Diseño de Investigación

En el diseño corresponde a la investigación de campo con enfoque cuantitativo, se usó el modelo de acción que propone la metodología de análisis de vulnerabilidad en la red del canal de televisión a través de la observación, encuestas y acciones en los riesgos existentes. Según Hernández & Mendoza (2018) en la investigación cuantitativa se tiene como fortaleza la representación, generalización de resultados y predicción, muy necesario en este estudio de seguridad.

Dentro del mapa del diseño de investigación (Ver Figura 17) el presente trabajo se realiza sin manipular de forma deliberada las variables, lo que según Hernández & Mendoza (2018) se define como diseño no experimental. La recolección de datos es de tipo transversal porque se recolectará los datos en un solo momento.

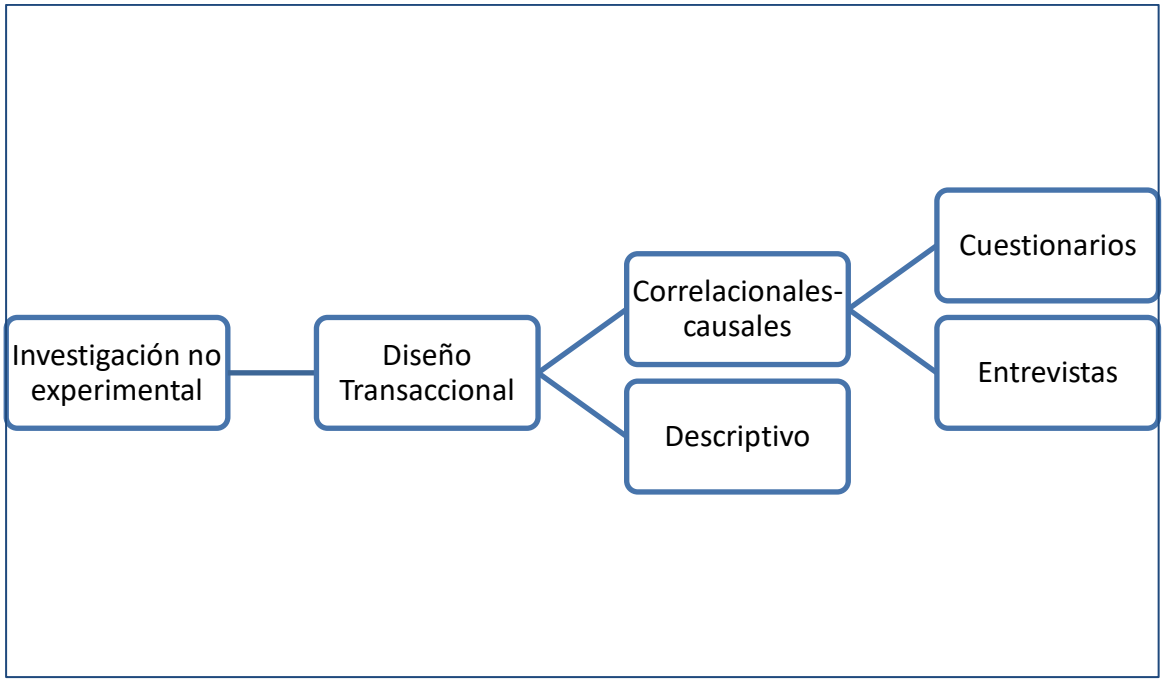


Figura 17. Mapa Diseño de Investigación

Fuente: Hernández & Mendoza (2018)

3.3. Unidades de Estudio

De acuerdo con Hernández & Mendoza,(2018), se define como unidad de estudio aquella que produce la información que será analizada. Las unidades de análisis en esta investigación son las personas especializadas en el área de tecnología y los activos de la información. En la Tabla 6 se muestran las preguntas de la investigación con su unidad de estudio.

Tabla 6

Preguntas de investigación y unidad de estudio

Pregunta de Investigación	Unidad de Estudio
¿Cuáles son los riesgos de seguridad de la información que el canal de televisión debe minimizar para cumplir con las regulaciones	Personal especializado del área de tecnología en el canal de televisión con

Pregunta de Investigación	Unidad de Estudio
y no parar la operación de transmisión al aire?	conocimiento de las leyes con los entes reguladores de los medios de comunicación.
¿Cuáles son los procedimientos o tareas que ejecuta el personal de tecnología del canal de televisión en el momento que son alertados de una vulnerabilidad?, y	Personal del área de tecnología en el canal de televisión
¿Cuál sería el diseño de una propuesta de análisis de vulnerabilidades con el software OPENVAS/GVM, dirigido al Dpto. de Tecnología del canal de televisión en el año 2023?	Activos de la información del área de tecnología del canal de televisión

3.4. Población

Según Hernández & Mendoza (2018) se denomina población al conjunto de casos que coincidan en datos especificados. Para este estudio se definirán dos grupos de población:

3.4.1. Los Activos de la Información, Excluyendo a las Personas.

Los equipos de Transmisión al aire – del canal de televisión, conectados a la red tiene un tamaño de 163 activos. Esta población se la tomó de manera manual proporcionada por los especialistas del área de Ingeniería. Con esta información se clasificó los activos de acuerdo con la Tabla 7.

Tabla 7

Clasificación de Activos

Tipo de Activo	Descripción
Hardware	Equipos físicos usados en la red de transmisión de la señal digital del canal de TV

Tipo de Activo	Descripción
Software	Herramientas de software, aplicaciones usadas en el proceso de gestión en la emisión de la señal de TV
Personas	Recursos de personas que laboran en el área de transmisión
Información	Datos de las aplicaciones para la gestión del proceso de emisión de transmisión de la señal de TV
Red	Dispositivos de conectividad en la red

Nota: INCIBE CERT (2020)

3.4.2. Personal Especializado, Parte de los Activos de la Información

El personal especializado del área de Ingeniería del canal de televisión se detalla en la Tabla 8 quienes conocen las comunicaciones y operaciones de cada equipo de transmisión de la señal televisiva.

Tabla 8

Personal especializado del área de ingeniería

No.	Cargo	Área
1	Gerencia de Ingeniería	Ingeniería
2	Jefe de Ingeniería	Ingeniería
3	Administrador de Redes	Ingeniería
4	Técnico de Transmisiones	Ingeniería
5	Ingeniero de Enlaces y Telemetría	Ingeniería

3.5. Muestra

La muestra es un subgrupo de la población, en este modelo cuantitativo se usará la estrategia de muestro probabilístico que tiene como principal ventaja reducir el error al mínimo. Según Hernández & Mendoza (2018) en las muestras probabilísticas todos los elementos de la población tienen la misma posibilidad de formar parte de la muestra. Para el cálculo de la muestra se utilizó el programa STATS ™ el cual es un software que realiza cálculos estadísticos básicos y ayuda a determinar el tamaño de la muestra. Esta herramienta de software se la puede bajar de internet. En la población del personal especializado en el área de ingeniería se tomará el 100% como muestra. Con una población de 163 activos, se debe determinar el número de la muestra a analizar. Esta herramienta maneja cuatro parámetros, en la Tabla 9 se describen estos.

Tabla 9

Parámetros de STATS

Parámetro	Concepto	Valor
Universe Size	Tamaño de la muestra	Para este estudio se colocará 50.
Maximum Acceptable Percentage Point	Error	Los niveles más comunes están en el rango del 5 al 1%, para este estudio se utilizará el 5% lo cual indica que se acepta 5 errores por cada 100 casos.
Estimated Percentage Level	Porcentaje estimado de la muestra	Esto maneja la probabilidad de que la unidad de estudio, la muestra sea o no representativa, se usa generalmente 50/50 en donde se asume que tendrá 50% de que si ocurra y 50% de que no ocurra.
Desired Confidence Level	Nivel de confianza	Lo óptimo, ideal es un 100% de confianza, pero esto sería examinando el 100% de los casos se recomienda un 95%.

El resultado de la muestra es de 114 activos (Ver Figura 18). Este tipo de cálculo se llama muestreo aleatorio simple (MAS) y es usado tanto por STATS™ como por las otras herramientas diseñadas para este fin.

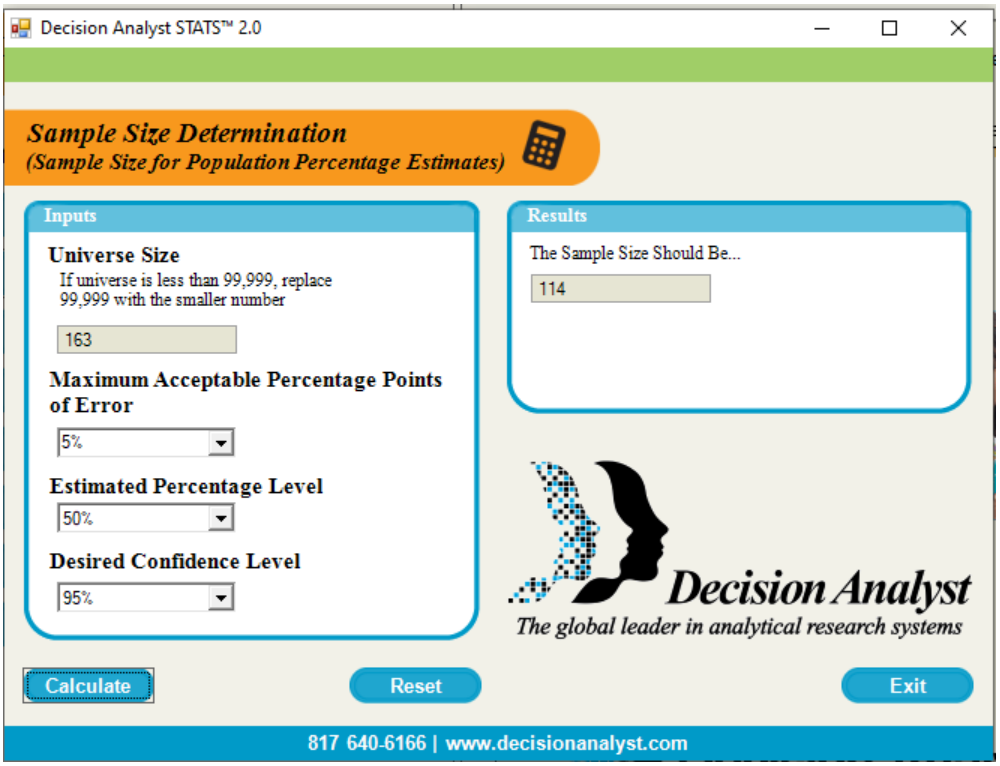


Figura 18. Resultado con ingreso de parámetros en STATS

Los casos (activos o hosts) de la muestra se etiquetan con numeración del 1 al 163. En este tipo de muestra es posible utilizar 4 métodos:

1. Tómbola
2. Número aleatorios
3. Uso de software aleatorio
4. Selección sistemática

Se usa la misma herramienta STATS ™ para la generación aleatoria de los números del listado (Ver Figura 19).

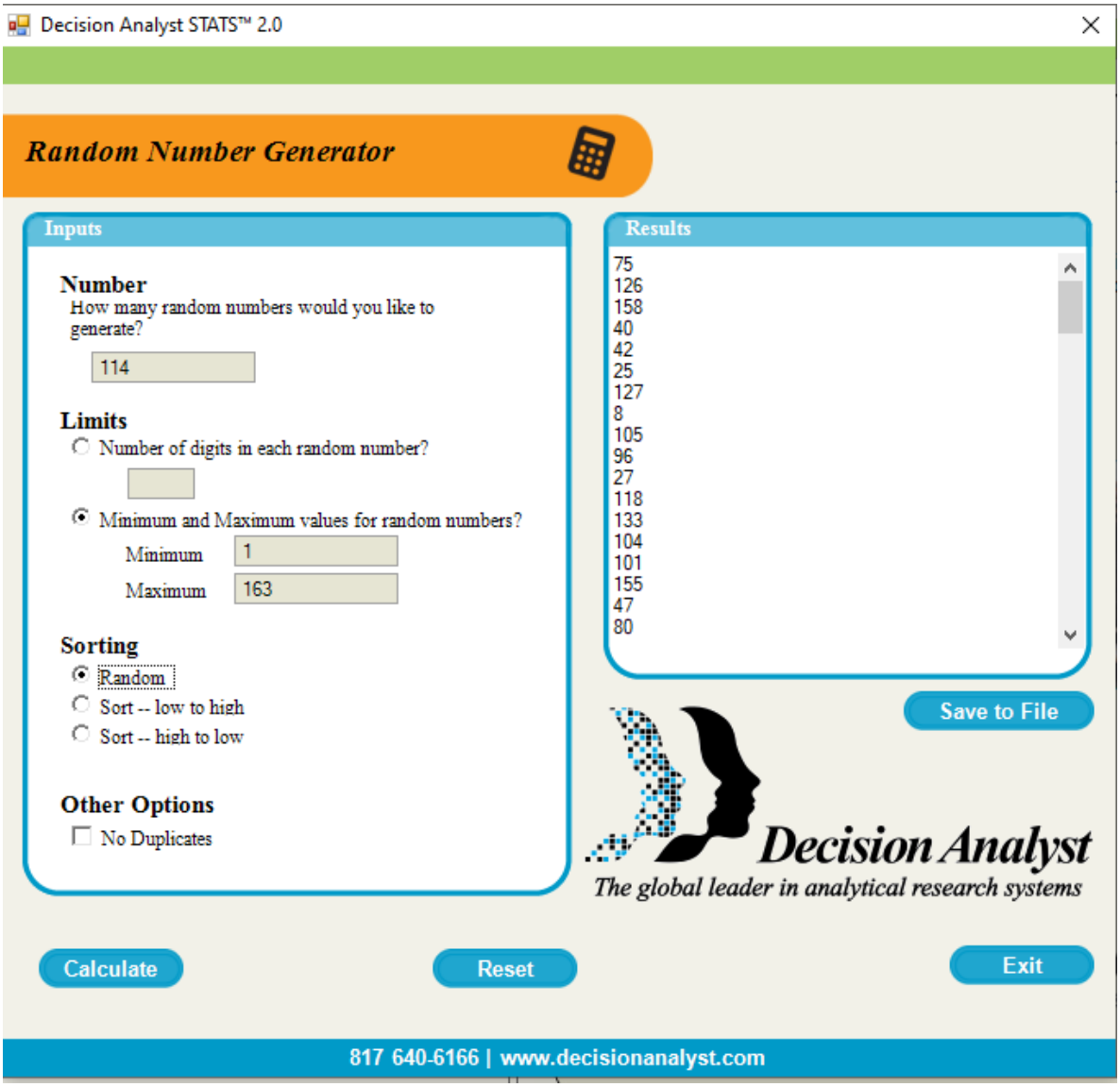


Figura 19. Generador aleatorio de la muestra

En el Anexo 3 se muestra la Tabla 17 con los números aleatorios de la muestra probabilística.

3.6. Técnicas de recolección de datos

La recopilación de datos se realizará mediante entrevistas, visitas de campo, encuestas, indicadores de la herramienta OPENVAS/GVM dentro de la infraestructura de la red de Ingeniería del canal de televisión.

La entrevista se realizará al personal del Dpto. de Ingeniería del canal de televisión que está conformada por personal especializado en los equipos del medio televisivo, conocen la infraestructura y todos los componentes de la red de televisión, en dicha área coinciden los sistemas de cómputo, las telecomunicaciones, la red además del procesamiento de datos. Su

labor en el canal de televisión es el de emitir correctamente la señal al aire, por lo tanto es un área crítica de mucha responsabilidad e importancia en el control, supervisión y planificación de dicha tarea.

3.6.1. Fuentes Primarias

Según los métodos de recolección de datos indicada por Torres et al., (s.f.), las fuentes primarias son aquellas tomadas directamente de la población o muestra, en el presente trabajo la fuente primaria son las encuestas. Como parte de las unidades de estudio de la propuesta, se ha determinados dos factores esenciales: los activos de la información y el talento humano que labora en la organización. En el caso de los activos de la información no se aplicó el estudio total de ellos, por lo que se estableció una muestra finita de equipos del área de transmisión de señal para realizar su análisis dependiendo de la criticidad. Para definir los diferentes tipos de vulnerabilidades informáticas se realizó un muestro no probabilístico con una muestra finita de 4 colaboradores teniendo en cuenta las características afines o conocimientos previos de los encuestados.

Cuestionarios: Se define como cuestionario al conjunto de preguntas para medir una o más variables. La medición del cuestionario tiene diversas propiedades, en este estudio se revisará la dirección (positiva o negativa) e intensidad (alta o baja). Estas a su vez forman parte de las propiedades de la actitud, la cual se define como la predisposición de responder coherentemente de forma positiva o negativa ante otro ente tal como un ser vivo, objeto, etc.

En la medición de variables se usará el escalamiento de Likert el cual es un conjunto de ítems que se presente en forma de afirmación ante lo cual se solicita a los participantes que intervengan con una reacción. En la Figura 20 se muestran las diferentes alternativas para las escalas de Likert.

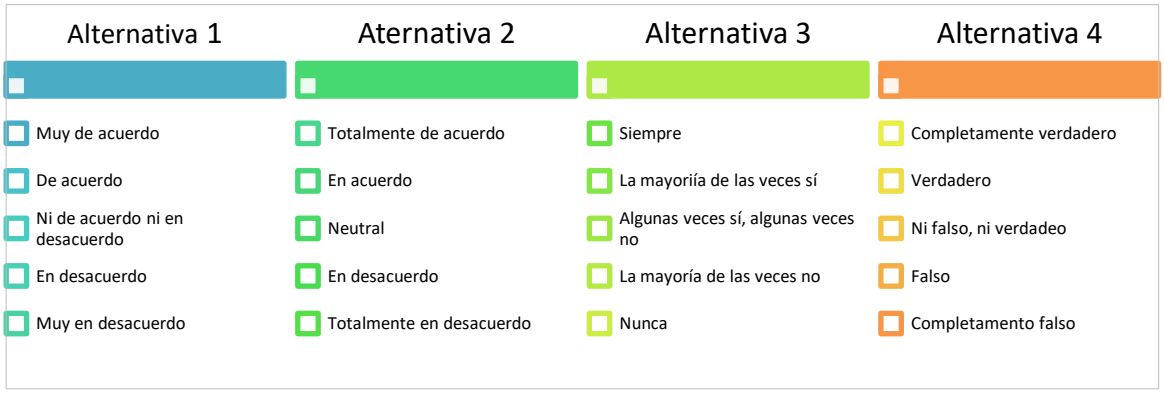


Figura 20. Opciones en la escala de Likert

Fuente: Hernández & Mendoza (2018)

Para el presente estudio se usará la Alternativa 1 para medir el nivel de desacuerdo que tiene el personal especializado del área de Ingeniería con respecto a la seguridad de sus procesos, la ponderación de la escala se muestra en la Tabla 10.

Tabla 10

Ponderación de Escala de Likert Alternativa 1 usada en este estudio

Escala de Likert	Ponderación
Muy de acuerdo	5
De acuerdo	4
Ni de acuerdo ni en desacuerdo	3
En desacuerdo	2
Muy en desacuerdo	1

3.6.2. Análisis de cuestionario mediante tablas

Se elaboró el cuestionario (Ver Anexo 4) para el personal especializado del área de Ingeniería del canal de televisión, la importancia de esta área en el conocimiento, mantenimiento, ejecución de las tareas diarias para la emisión de la señal con los componentes de cómputo, telecomunicaciones, redes entre otras, hacen pertinente que el cuestionario sea dirigido al personal antes mencionado.

Las respuestas se tabularon en la Tabla 11 para determinar con un enfoque cuantitativo la situación actual del sistema de transmisión, tomando como referencia el punto máximo de la escala de Likert para el resultado óptimo.

Tabla 11

Resultado del Cuestionario personal especializado del área de ingeniería

CUESTIONARIO	PERSONAL ESPECIALIZADO DEL ÁREA DE INGENIERIA A: Jefe de Ingeniería B: Administrador de Redes C: Técnico de Transmisiones D: Ingeniero de Enlaces y Telemetría			
	A	**B**	**C**	**D**
¿Tiene la empresa un Sistema de Gestión de la Seguridad de la Información (SGSI)?	1	2	4	3
¿Existen políticas de Seguridad de la Información?	3	3	4	3
¿Está la Alta Gerencia involucrada en la gestión y procedimientos de seguridad de la Información?	1	1	1	1
¿Existen dispositivos móviles o equipos en ambientes remotos?	5	5	5	5
¿Tienen un listado de los activos de Información del área de Ingeniería?	5	3	2	3
¿Están los activos debidamente etiquetados?	4	3	5	4
¿Existen servicios de archivos compartidos con políticas acceso de Directorio Activo u otro control de acceso?	3	2	4	4

CUESTIONARIO	PERSONAL ESPECIALIZADO DEL ÁREA DE INGENIERIA A: Jefe de Ingeniería B: Administrador de Redes C: Técnico de Transmisiones D: Ingeniero de Enlaces y Telemetría			
	A	**B**	**C**	**D**
¿La información entre los enlaces viaja de forma encriptada o cifrada?	1	1	3	3
¿Existe monitoreo de las actividades de los enlaces de Transmisión en TV?	4	2	4	5
¿Se tienen herramientas para controlar posibles amenazas en la seguridad de la información?	3	2	4	3
¿Existen políticas de respaldo de la información?	3	3	3	3
¿Existen seguridad perimetral?	4	4	5	5
¿Las aplicaciones y desarrollos implementados se cuentan con procesos de seguridad?	3	2	3	3
¿Existe un sistema de registro de incidentes?	1	1	3	3
¿Existen procedimientos para continuidad de negocio?	3	3	5	4

Se considera como fuente primaria los indicadores de la herramienta de detección de vulnerabilidades OPENVAS/GVM, la instalación de este software incluyó otras herramientas que se indican en la Tabla 12.

Tabla 12

Herramientas usadas en este estudio

Herramienta	Descripción
Sistema Operativo Windows	Sistema operativo instalado en equipo que realiza el análisis.
VMware	Software de Virtualización.
Kali Linux	Software especializado en auditorías y pruebas de penetración en seguridad informática
OpenVAS	Software open source especializado en el escaneo de vulnerabilidades en una red

3.6.3. Fuentes Secundarias

Siguiendo a Torres et al. (s.f.) las fuentes secundarias se basan en datos preelaborados. Las fuentes secundarias que se utilizaron son trabajos de tesis doctorales, publicaciones de internet, revistas y artículos científicos relacionados con herramientas de análisis de vulnerabilidades y gestión de riesgos.

3.6.4. Procesamiento de datos

Se realizarán análisis de la información recopilada con gráficos estadísticos que proporcione una forma visual y ágil para indicar el escenario actual del estado de la red de transmisión de señal digital del canal de televisión.

3.6.5. Técnica de Análisis de Datos

El proceso de análisis de datos se realizó con matrices de tablas, gráficos con la valoración cuantitativa de las amenazas en lo referente a los indicadores de la herramienta de escaneo de vulnerabilidades. Con respecto a los cuestionarios se realizaron gráficos estadísticos usando la herramienta Microsoft Excel. Con los datos de detección de vulnerabilidades se trabajó con los reportes de la herramienta de escaneo OpenVAS/GVM.

3.7. Operacionalización de variables

En un estudio no sólo es importante identificar el problema también es necesario que se identifiquen las variables del objeto de estudio, estas variables son las propiedades o atributos característicos medibles de dicho estudio. La operacionalización trata de medir la variable desde su concepto hasta una definición operacional que se pueda revisar a través de instrumentos. En el análisis de vulnerabilidades se detallan dichas variables en la Tabla 13.

Tabla 13

Operacionalización de variables

Variables	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición
Vulnerabilidad en servidores de transmisión	Variable cualitativa de tipo ordinal. La vulnerabilidad implica un riesgo de un ataque	La variable vulnerabilidad en servidores se observará en 3 dimensiones: Equipo, configuración y servicio con los indicadores de revisión, cambios y mejoras. La medición se lo realizará en la escala de Likert	Equipos Configuración Servicio	Revisión Cambios Mejora Revisión Cambios Mejora Revisión Cambios Mejora	Escala de Likert • Totalmente en desacuerdo • En desacuerdo • Ni de acuerdo ni en desacuerdo • De acuerdo • Totalmente de acuerdo
Ciberseguridad	Variable cualitativa de tipo ordinal.	La variable ciberseguridad se observará en 3 dimensiones: Prevenir, Detectar y Actuar	Prevenir	Revisión Cambios Mejora	Escala de Likert • Totalmente en desacuerdo

Variables	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición
	Esta variable mide los procesos de seguridad en los sistemas informáticos	con los indicadores de revisión, cambios y mejoras. La medición se lo realizará en la escala de Likert	Detectar Actuar	Revisión Cambios Mejora Revisión Cambios Mejora	• En desacuerdo • Ni de acuerdo ni en desacuerdo • De acuerdo • Totalmente de acuerdo

CAPÍTULO IV: PRESENTACIÓN Y ANÁLISIS DE DATOS

4.1. Introducción

Con las dos poblaciones que se tomó para este estudio se utilizaron diferentes métodos de recolección indicados en el capítulo anterior. Para la población de personal especializado en el área de ingeniería se elaboró cuestionarios con la herramienta de Google Forms con posterior envío de dicho enlace a cada una de las personas de esta área. La representación gráfica de estos resultados se los elaboró en Microsoft Excel en base a las respuestas recolectadas en archivo de extensión .csv de la herramienta de Google.

Para los activos de la información se aplicaron técnicas para armar las listas de hosts que fueron tomados del inventario manual proporcionado por el personal del área de ingeniería. Estos activos fueron procesados según la clasificación de herramientas para este tipo de inventario.

4.2. Análisis e interpretación de resultados

El tratamiento de los datos recolectados ayudará al análisis del estado de vulnerabilidad de la red de infraestructura del canal de televisión tanto con la herramienta OpenVAS así como la percepción que tiene el personal de ingeniería sobre temas de seguridad con las respuestas obtenidas de los cuestionarios.

4.3. Informe de Resultados

Se generaron dos diferentes informes de resultados, uno para cada población. En la población del personal especializado del área de Ingeniería del canal de televisión se realizó una valoración cuantitativa con escala de Likert estableciendo cinco como la puntuación más alta por cada ítem. En la población de hosts se analizaron los datos generados por el escáner de vulnerabilidad.

4.3.1. Resultados Cuestionario Personal.

Una vez recolectada la información de la encuesta enviada al personal del área de ingeniería se proceda valorizar las respuestas en la escala de Likert donde la calificación de 5 es si la respuesta es que está “Muy de Acuerdo” (Ver Tabla 10), siendo 4 personas el puntaje total de respuestas en una pregunta es de 20 puntos si todos estuvieran “Muy de Acuerdo”. El resultado de este cuestionario se muestra en la Figura 21.

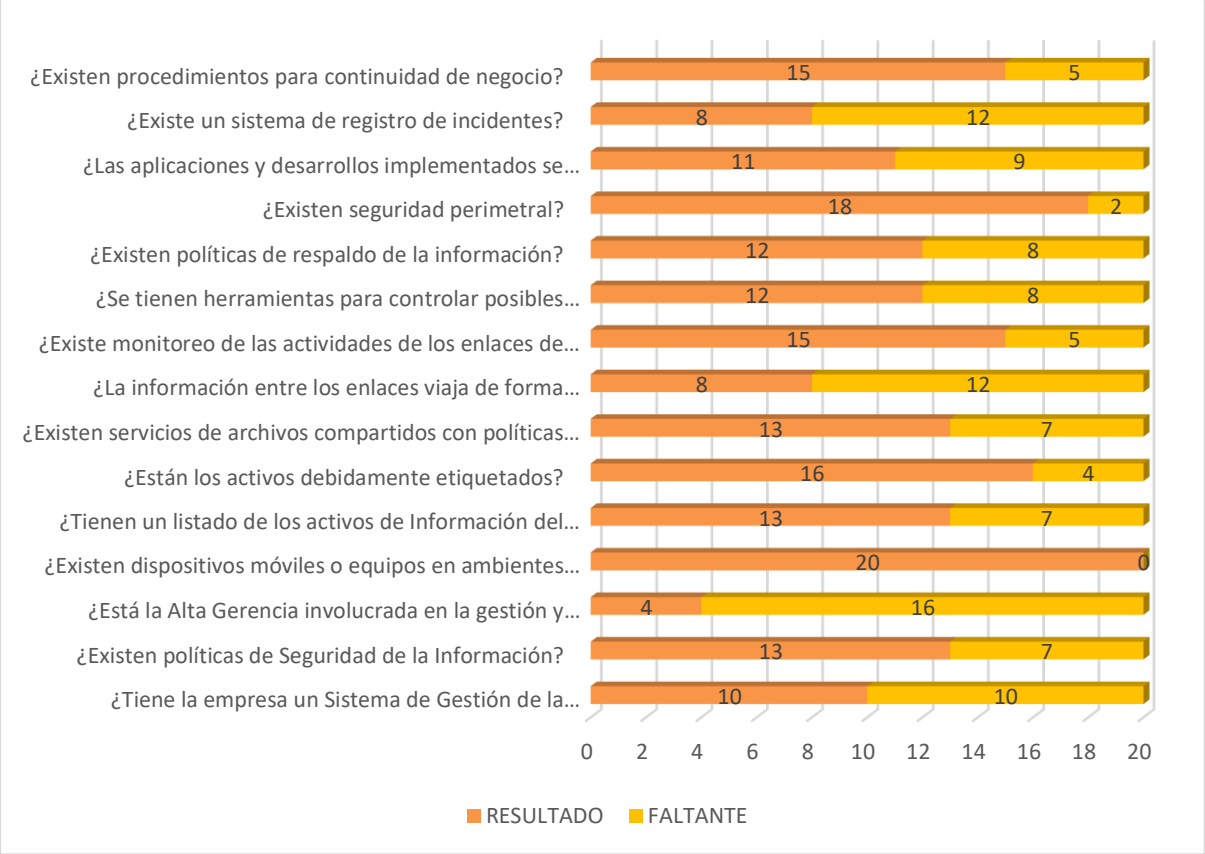


Figura 21. Resultado de cuestionario al personal especializado del Área de Ingeniería del canal de televisión

Se observa en la gráfica de resultados que el personal especializado del área de Ingeniería del canal comparte diferentes criterios en lo que respecta al sistema de seguridad de los activos.

La pregunta “Existen dispositivos móviles o equipos en ambientes remotos”, fue la única en que todos coincidieron, el resto de las preguntas tuvo respuestas variables, lo que confirma que el personal necesita de una adecuada capacitación con respecto a la seguridad de los activos de la información para una correcta alineación de conocimiento.

La pregunta “¿Está la Alta Gerencia involucrada en la gestión y procedimientos de seguridad de la Información?” enfatiza que el personal de ingeniería no tiene la gestión, procedimientos ni políticas que involucren a la Alta Gerencia en las decisiones de seguridad de la información, esto también puede ser desconocimiento del personal del área de ingeniería. El estado de desacuerdo de estas preguntas se grafica en la Figura 22 en la que se observa la falta en gestión de seguridad que tiene el Dpto. de Ingeniería del canal de televisión.

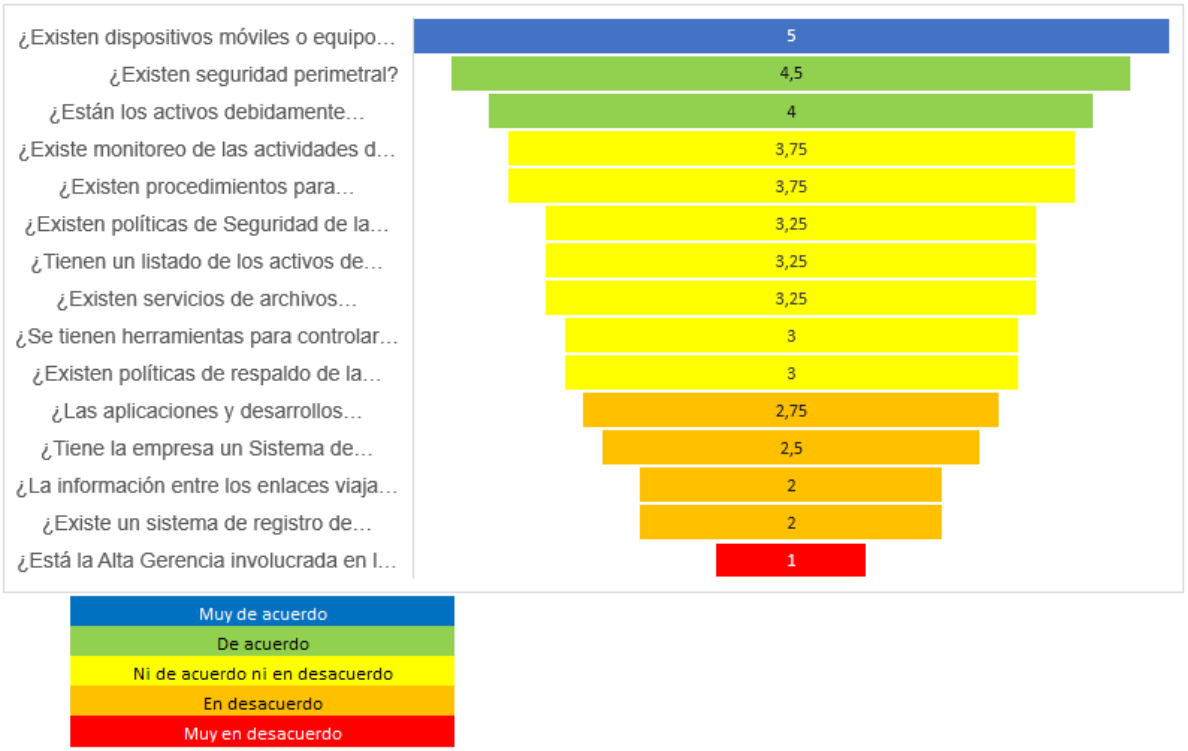


Figura 22. Promedio de respuestas en escala de Likert sobre los desacuerdos en gestión de seguridad del Dpto. de Ingeniería del canal de televisión

En resumen, el cuestionario refleja la importancia y énfasis que debe darse a las capacitaciones al personal, la falta de mismo genera también vulnerabilidad debido a que en situaciones de riesgo no hay un adecuado procedimiento a seguir.

4.3.2. Resultados Escáner OPENVAS/GVM.

La instalación de OPENVAS/GVM se detalla en el Anexo 1, en la ejecución de la herramienta es necesario establecer el objetivo (Target) y la tarea (Task) del escaneo. Los parámetros del objetivo en este estudio se muestran en la Figura 23, en la cual se ingresa principalmente los hosts objetivo desde un archivo o de forma manual y la lista de puertos.

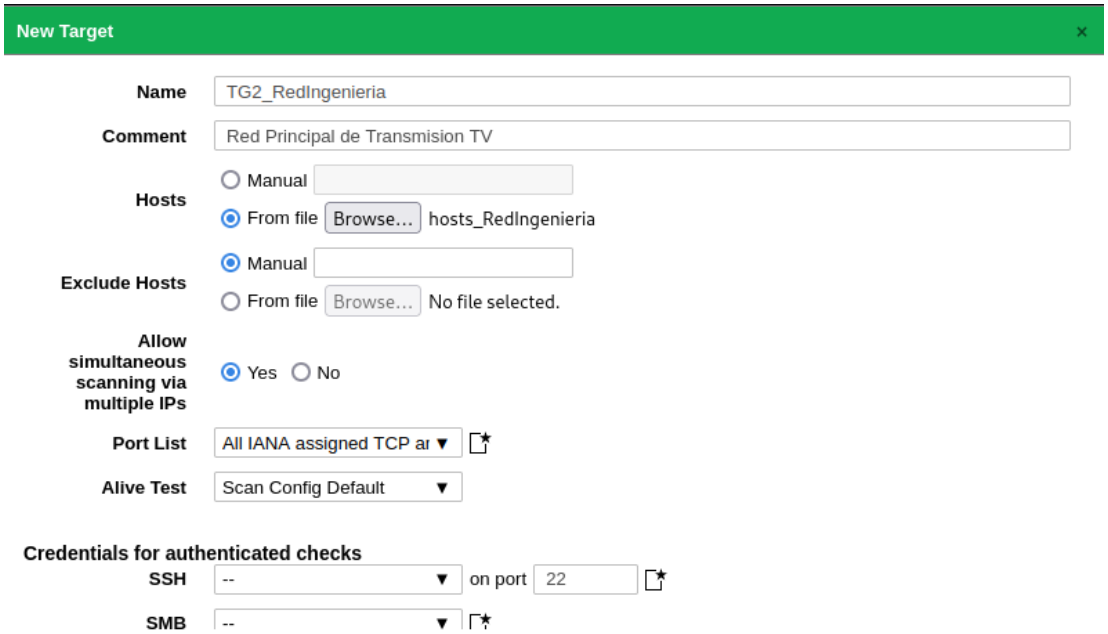


Figura 23. Parámetros del Objetivo por escanear

Fuente: GreenBone (2022)

El proceso continúa con la creación de la tarea, la cual solicitará el Target y el tipo de Scanner, como por ejemplo OpenVAS, CVE u otros que se hayan instalado. Los parámetros de esta tarea se muestran en la Figura 24.

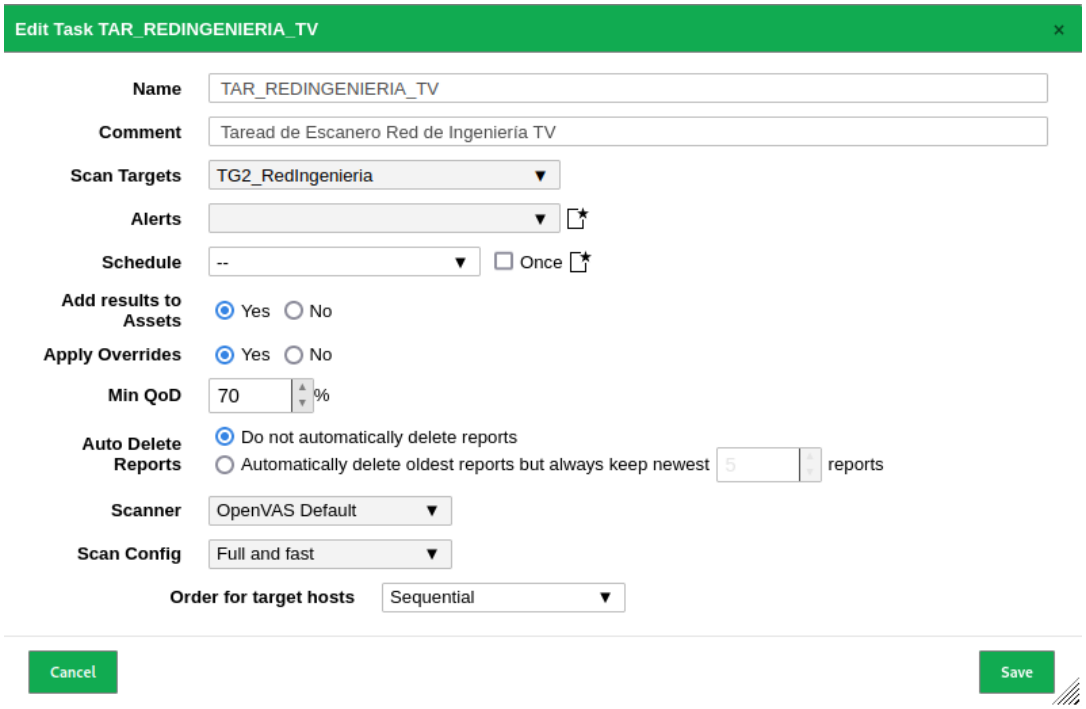


Figura 24. Creación de la tarea en la herramienta de escaneo

Fuente: GreenBone (2022)

La herramienta de escaneo tiene la siguiente tabla de puntación para valorar la gravedad de la vulnerabilidad calificándola de alta, media o leve de acuerdo (Ver Figura 25)

ESTIMACIÓN DE GRAVEDAD DE VULNERABILIDAD	
Valor	**Calificación**
7.4 - 10	Alta
4,0 - 7,3	Media
0,1 - 3,9	Baja
0	Log

Figura 25. Matriz para estimar la valoración de la gravedad de la vulnerabilidad

Fuente: GreenBone (2022)

En el reporte del escáner de vulnerabilidad muestra la clasificación de los hosts por clase de gravedad de vulnerabilidad, esta se muestra en la Figura 26, indicando que el 13% está en alta, 49% en media puntuación de gravedad. Entre estas dos calificaciones se tiene más del 50%, lo que indica que es necesario gestionar de inmediato un plan de acción para minimizar el impacto del riesgo.

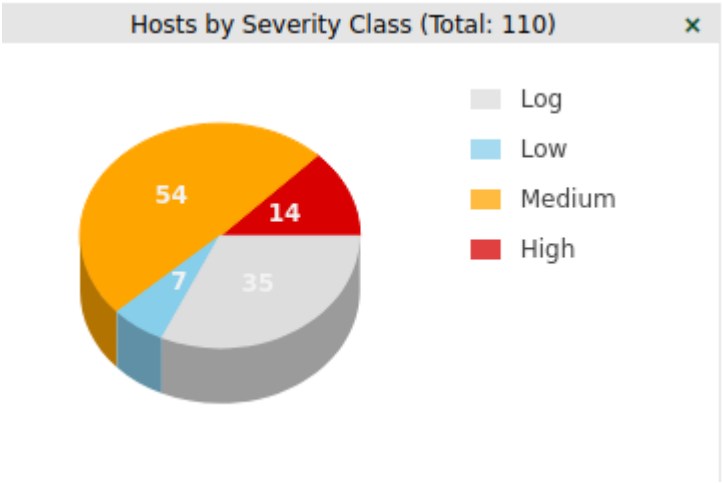


Figura 26. Clasificación de gravedad de vulnerabilidad por hosts

Fuente: GreenBone (2022)

El resultado del escaneo indica que el 4.5% del total de certificados de la muestra están expirados, contribuyendo este reporte a un estado de estos, con la información de los hosts en los que está instalado dicho certificado (Ver figura 27).

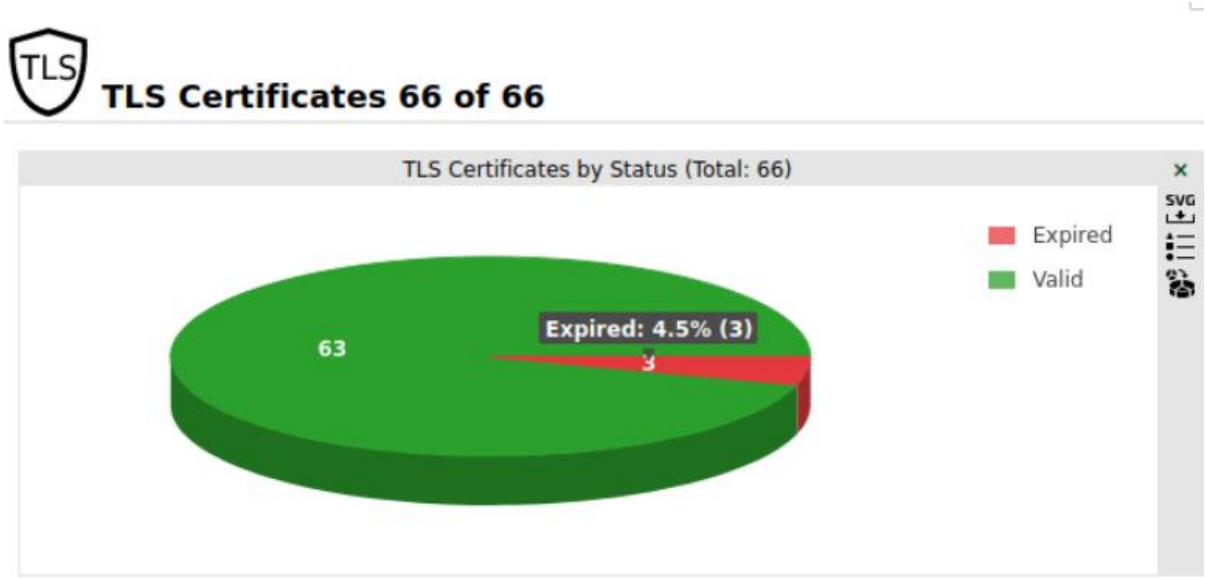


Figura 27. Estado de certificados después del escaneo de la herramienta OPENVAS

Los tipos de vulnerabilidades encontradas se detallan en la Tabla 14 con la puntación de cada tipo.

Tabla 14

Vulnerabilidades Encontradas en activos de la información

ID	VULNERABILIDAD	PUNTAJE	CALIFICACIÓN
11367	Check for discard Service	10	Alta
19782	FTP Writeable Directories	10	Alta
103674	Operating System (OS) End of Life (EOL) Detection	10	Alta
100111	The rexec service is running	10	Alta
108188	Microsoft SQL Server End Of Life Detection	10	Alta
809096	Microsoft SQL Server Multiple Vulnerabilities (MS16-136)	8,8	Media
805815	Microsoft SQL Server Multiple Vulnerabilities (MS15-058)	8,5	Media
142239	MikroTik RouterOS Directory Traversal Vulnerability (CVE-2019-3943)	8,1	Media
810676	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	8.1	Media
4040	MikroTik RouterOS RCE Vulnerability (CVE-2021-41987)	8,1	Media
143081	MikroTik RouterOS < 6.44.6 (LTS), < 6.45.7 (Stable) Multiple Vulnerabilities	7,5	Media

ID	VULNERABILIDAD	PUNTAJE	CALIFICACIÓN
147752	MikroTik RouterOS < 6.47.1 Multiple DoS Vulnerabilities	7,5	Media
144720	MikroTik RouterOS < 6.45.5 DoS Vulnerability	7,5	Media
100080	rsh Unencrypted Cleartext Login	7,5	Media
142599	MikroTik RouterOS < 6.44.5 (LTS), < 6.45.1 (Stable) Multiple DoS Vulnerabilities	7,5	Media
103240	HTTP Brute Force Logins With Default Credentials Reporting	7,5	Media
10264	Report default community names of the SNMP Agent	7,5	Media
142020	MikroTik RouterOS Intermediary Vulnerability	7,5	Media
144572	MikroTik RouterOS < 6.46.7, <= 6.47.3, 7.x DoS Vulnerability	7,5	Media
801993	Deprecated SSH-1 Protocol Detection	7,5	Media
143630	MikroTik RouterOS <= 6.44.3 DoS Vulnerability	7,5	Media
105042	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	7,4	Media
124148	MikroTik RouterOS DoS Vulnerability (CVE-2022-36522)	6,8	Media
146341	MikroTik RouterOS <= 6.48.6 Multiple Vulnerabilities	6,5	Media
145885	MikroTik RouterOS < 6.46.5 Multiple DoS Vulnerabilities	6,5	Media

ID	VULNERABILIDAD	PUNTAJE	CALIFICACIÓN
146342	MikroTik RouterOS <= 6.48.6 DoS Vulnerability	6,5	Media
145883	MikroTik RouterOS < 6.46 DoS Vulnerability	6,5	Media
142803	MikroTik RouterOS File Deletion Vulnerability (CVE-2019-15055)	6,5	Media
146340	MikroTik RouterOS < 6.47 Multiple Vulnerabilities	6,5	Media
127012	MikroTik RouterOS < 6.48.2 Multiple DoS Vulnerabilities	6,5	Media
900600	Anonymous FTP Login Reporting	6,4	Media
111012	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5,9	Media
11213	HTTP Debugging Methods (TRACE/TRACK) Enabled	5,8	Media
117687	Weak Host Key Algorithm(s) (SSH)	5,3	Media
150713	Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5,3	Media
150710	SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits	5,3	Media
117761	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5	Media
103440	SSL/TLS: Report Weak Cipher Suites	5	Media

ID	VULNERABILIDAD	PUNTAJE	CALIFICACIÓN
146591	DNS Cache Snooping Vulnerability (UDP) - Active Check	5	Media
113054	SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection	5	Media
100075	echo Service Reporting (TCP + UDP)	5	Media
100072	Check if Mailserver answer to VRFY and EXPN requests	5	Media
10736	DCE/RPC and MSRPC Services Enumeration Reporting	5	Media
10043	Check for Chargen Service (TCP)	5	Media
103955	SSL/TLS: Certificate Expired	5	Media
108030	Check for Chargen Service (UDP)	5	Media
101015	Microsoft MS03-034 security check	5	Media
108522	Telnet Unencrypted Cleartext Login	4,8	Media
15855	POP3 Unencrypted Cleartext Login	4,8	Media
108440	Cleartext Transmission of Sensitive Information via HTTP	4,8	Media
108528	FTP Unencrypted Cleartext Login	4,8	Media
117274	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4,3	Media

ID	VULNERABILIDAD	PUNTAJE	CALIFICACIÓN
805142	SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	4,3	Media
902830	Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	4,3	Media
105611	Weak Encryption Algorithm(s) Supported (SSH)	4,3	Media
106223	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4	Media
105880	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4	Media
805188	SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)	3,7	Baja
802087	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	3,4	Baja
105610	Weak MAC Algorithm(s) Supported (SSH)	2,6	Baja
80091	TCP timestamps	2,6	Baja
103190	ICMP Timestamp Reply Information Disclosure	2,1	Baja
146440	ICMP Netmask Reply Information Disclosure	2,1	Baja

En los equipos de capa dos del modelo OSI (Interconexión de Sistemas Abiertos) de la infraestructura de red del canal de televisión, la herramienta de escaneo muestra una baja vulnerabilidad en la configuración de direcciones MAC de dichos dispositivos (Ver Figura 28).

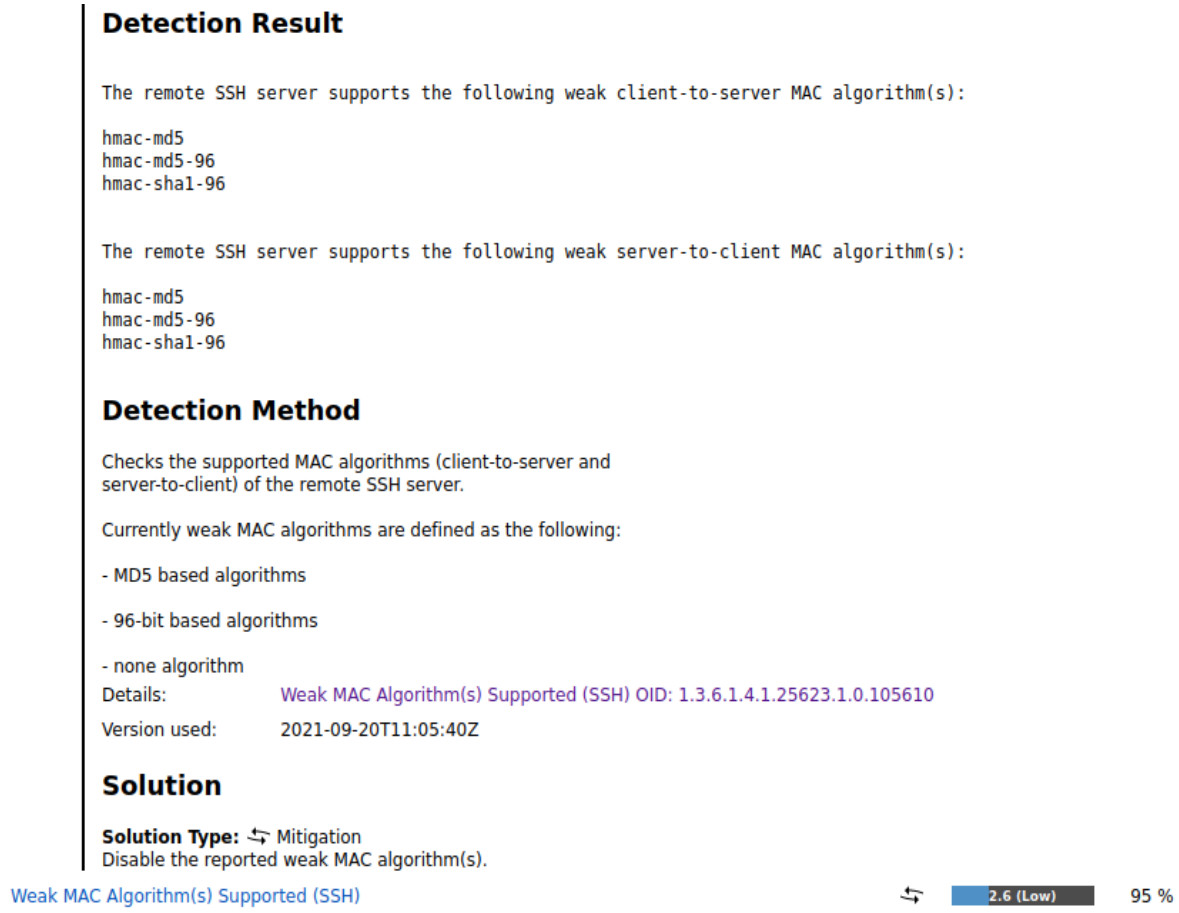


Figura 28. Resultado de escaneo dispositivos capa dos del modelo OSI

Es necesario indicar que la herramienta OPENVAS emite resultados de ataques de MAC en dispositivos de capa dos (enlace), pero en la capa de enlace pueden ocurrir otros tipos de ataques que no serán objeto de este estudio pero es importante mencionarlos para la seguridad de la red y debido a la cantidad considerable de estos equipos en la infraestructura de red del canal. El estudio de Chaparro et al.(s.f.) detalla esta lista de ataques en la capa de enlace:

- Sniffing: Captura el tráfico de una comunicación, es necesario usar cifrados para evitar este tipo de ataques.
- Man in The Middle: Intercepta mensajes entre emisor y receptor, puede realizar secuestro de una sesión.
- Session hijacking: Realiza el secuestro de una sesión con un ataque activo.

- Tormenta broadcast: Saturación de la red con emisión constante de paquetes.
- MAC flooding: Sucede cuando se desborda la tabla CAM dentro de la memoria del switch en el almacenamiento de direcciones MAC aprendidas.
- ARP spoofing: Cambio de direcciones MAC de un dispositivo de red a otro.
- VLAN Hopping Attack: Suplantación del protocol DTP (Dynamic Trunk Protocol) enviando mensajes a VLAN externas.
- DHCP Starvation: Satura la solicitud de IPs hasta agotarlas generando denegación del servicio.

Los protocolos de administración de los dispositivos de capa dos deben ser seguros, con prevención de seguridad de puertos y uso de protocolos seguros.

4.3.2.1 Acciones de Remediación.

Con las vulnerabilidades descubiertas con su respectiva calificación de gravedad, es necesario continuar con el proceso de ejecución de la acción para eliminar la vulnerabilidad. La herramienta muestra una página de detalles de los planes de acción haciendo clic en cada una de las vulnerabilidades, así como un reporte en formato PDF con el resultado de la tarea ejecutada.

En la página de detalles de cada vulnerabilidad (Ver Figura 29) se clasifica la lista de acciones en categorías tales como:

- **VendorFix**: La solución indicada está disponible en una corrección oficial del autor del producto con la vulnerabilidad.
- **Mitigation**: La solución ayuda a mitigar el riesgo, pero no resuelve el problema de vulnerabilidad, puede ser indicada tanto por el autor del producto como por otro proveedor.
- **Workaround**: Soluciones alternas al autor de producto con la vulnerabilidad.

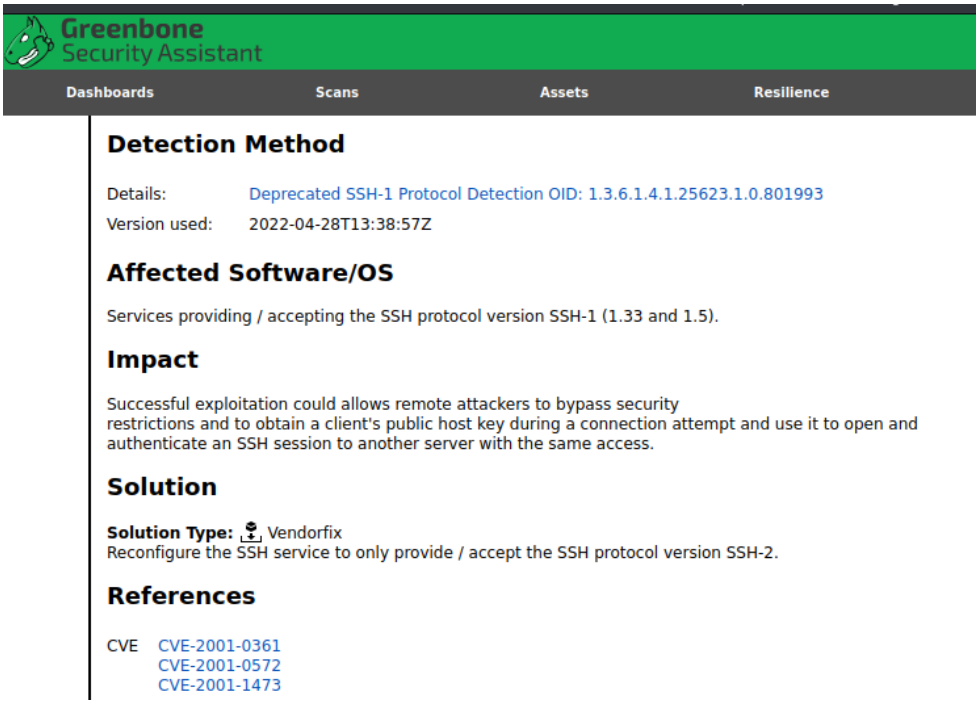


Figura 29. Plan de acción para mitigar cada vulnerabilidad encontrada

Fuente: GreenBone (2022)

CAPITULO V: PRESENTACIÓN DE LA PROPUESTA

5.1. Denominación y Descripción de la Propuesta

5.1.1. Denominación

Análisis de vulnerabilidad en infraestructura de red utilizando OpenVAS/GVM en una estación televisiva.

5.1.2. Descripción

Se realiza la propuesta de diseño de métodos y estrategias para el análisis de vulnerabilidades en la red de internet y datos que el canal de televisión usa para sus operaciones de TV Digital que minimicen el impacto de riesgo para la operación y continuidad del negocio.

5.2. Justificación de la Propuesta

Se realiza esta propuesta con el fin de mitigar los riesgos en el canal de televisión en su parte operativa a través de diagnóstico de la red, analizando la protección que tiene actualmente, analizando las posibles vulnerabilidades y generando planes de acción para las mismas.

Los llamados de atención de ARCOTEL a través del ECUCERT pueden provocar fuertes multas e incluso el retiro del permiso de frecuencia, es por ello por lo que la presente propuesta plantea no solo la detección de vulnerabilidades sino también la generación de informes para mejorar el sistema de seguridad de los activos de la información,

Esta propuesta puede ampliarse a la parte administrativa para que el canal de televisión conserve confianza antes sus clientes y proveedores de este sector como una empresa que cumple con estándares y protocolos de seguridad de la información.

5.3. Objetivos de la propuesta

5.3.1. Objetivo General

Diseñar el plan de acción de gestión para mitigar las vulnerabilidades encontradas en base a las pruebas realizadas con la herramienta OPENVAS/GVM.

5.3.2. Objetivos Específicos

Dentro de los objetivos específicos se detallan:

- Diseñar un esquema de trabajo con el personal especializado del área de ingeniería del canal de televisión para la ejecución de las pruebas de análisis de vulnerabilidades
- Crear el inventario de equipos activos en la red con la respectiva identificación de sus sistemas operativos
- Analizar las vulnerabilidades encontradas y ejecutar los planes de remediación indicadas en la herramienta.
- Generar un informe con las sugerencias indicadas por la herramienta para cerrar las vulnerabilidades encontradas o establecer su nivel de riesgo.
- Presentar conclusión del informe.

5.4. Temporización de la Propuesta

El presente trabajo fue desarrollado en el periodo académico agosto a diciembre 2022, considerando la fundamentación teórica junto con la metodología aplicada para el diseño e implementación. El cronograma de actividades se presenta en la Tabla 15.

Tabla 15

Cronograma de la propuesta

ID	Fases	Descripción	Fecha de Inicio	Fecha Fin	Días
1	Fase 1 - Acuerdos	Formularios de Acuerdos de Confidencialidad	01/08/2022	05/08/2022	5
2	Fase 2 - Planeación	Inventario de Activos de Ingeniería	08/08/2022	15/09/2022	29
3	Fase 3 - Análisis de vulnerabilidades	Identificación de IP Activas con NMAP	19/09/2022	23/09/2022	5
4	Fase 3 - Análisis de vulnerabilidades	Identificación de sistemas Operativos y Aplicaciones	25/09/2022	07/10/2022	10
5	Fase 3 - Análisis de vulnerabilidades	Análisis de vulnerabilidades con OPENVAS	10/10/2022	30/11/2022	38
6	Fase 4 - Evaluación	Evaluación de vulnerabilidades	01/12/2022	05/12/2022	3
7	Fase 4 - Evaluación	Evaluación de Impacto y riesgos	07/12/2022	12/12/2022	4
8	Fase 5 - Informe	Presentación de Informe a Alta Gerencia	13/12/2022	19/12/2022	5
9	Fase 5 - Informe	Presentación de Informe Técnico	19/12/2022	23/12/2022	5

Un recurso que ayuda al planteamiento de un proyecto es el Diagrama de Gantt, en el cual las tareas se ven representadas gráficamente por una barra horizontal. El tiempo estimado para la elaboración del proyecto está dato en 19 semanas, las tareas se realizan sin transponerse, una mejor visualización del cronograma puede ser observado en la Figura 30.

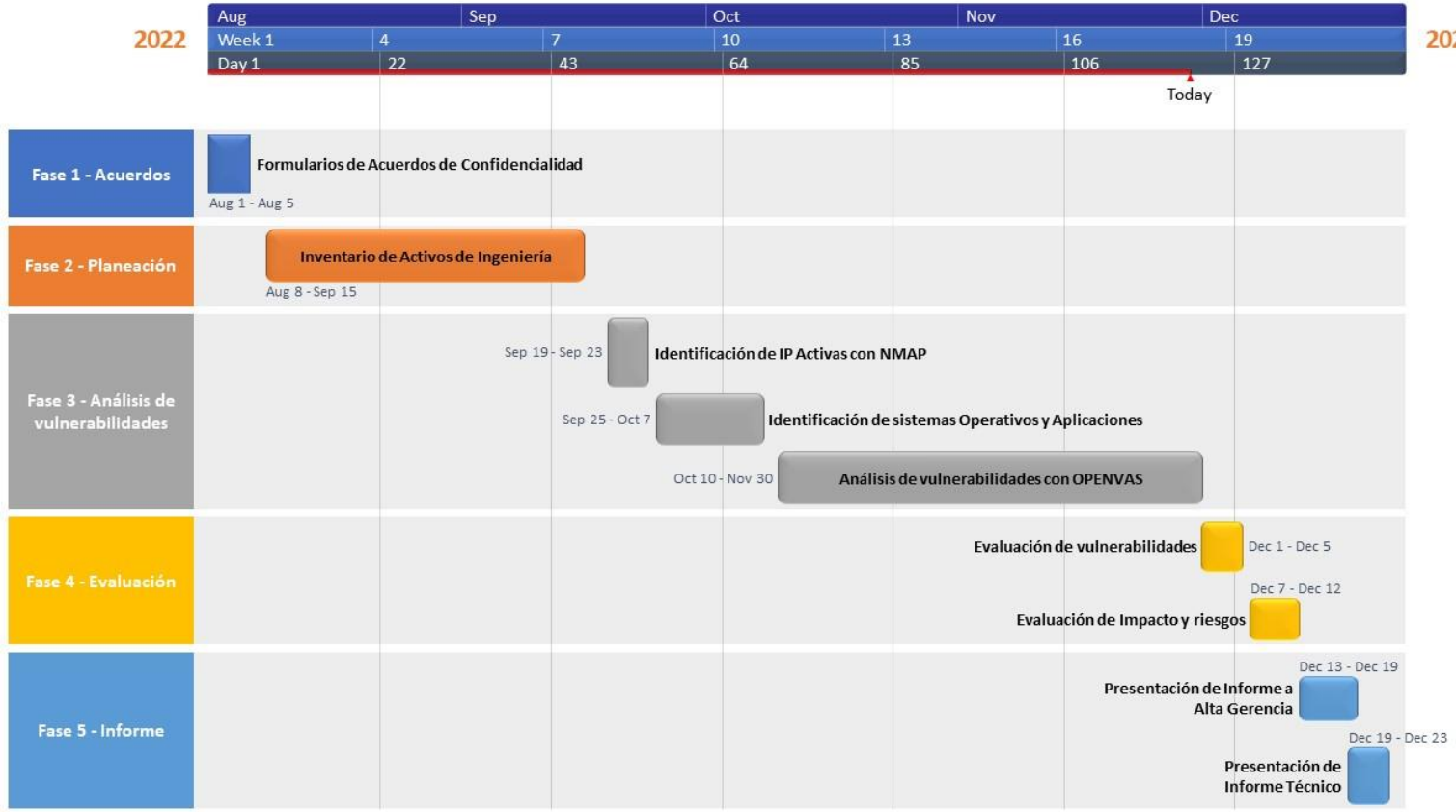


Figura 30. Diagrama de Gantt del cronograma de la Propuesta de Análisis de Vulnerabilidades

5.5. Descripción de los destinatarios y responsables

5.5.1. Destinatarios

Esta propuesta fue orientada al personal especializado del área de ingeniería, así como para su Alta Gerencia como base de conocimiento para la protección de los activos de la información. Al generar tareas y acciones en el análisis de vulnerabilidades se tienen también otros destinatarios de forma indirecta tales como el personal administrativo y legal de la empresa al contar con herramientas, políticas y estándares que justifiquen la operación en normas de seguridad.

5.5.2. Responsables

El diseño de esta propuesta tiene como responsable directo a Carolina Alcívar Agurto quien cursa la Maestría en Tecnologías de la Información, mención en Gestión y Administración de Tecnología quien también labora en el sector de medios televisivos, y del Dr. Edison Guaña Moya que se desempeñó como Director – Tutor del trabajo de titulación quien fue designado por la Facultada de Ingeniería de la Pontificia Universidad Católica del Ecuador.

5.6. Metodologías Aplicadas

La metodología aplicada en el análisis de vulnerabilidades se enfoca principalmente en la protección de los activos de la información mediante una estructura de módulos que deben ser interactivos debido a los cambios que sufre la tecnología día a día. Esta estructura se define en 5 fases expresadas en la Figura 31.

Figura 31. Fases de Funciones para protección de activos de la información

Fuente: (NISCT, 2018)

- **Identificación**

En esta fase es necesario identificar el modelo de negocio y dar entendimiento organizacional en materia de ciberseguridad. Haciendo un poco de historia debe considerarse

que la televisión se creó como un elemento de distracción y es a través de los canales de televisión que llega la señal de audio y video a estos receptores, dicha recepción puede ser realizada a través de ondas de radio o cable, siendo el televisor el receptor de la señal. En su señal análoga los canales de televisión tienen una imagen y sonido representadas por el tamaño analógico de una señal eléctrica ocasionado que el espectro de frecuencia ocupe un gran ancho de banda. La transmisión puede realizarse por satélite, cable o vía radiofrecuencia terrestre llamada TDT.

Con el ingreso de la Televisión Digital Terrestre (TDT) los parámetros se basan en el uso de los dígitos "1" y "0" creando una serie de ventajas para su uso, entre las principales está el menor consumo de frecuencias, mayor número de canales de televisión al transmitir mediante multiplexación más de una señal televisiva, alta definición, mejoras en el audio, multiprogramación, entre otras con el mismo acceso libre y gratuito al seguir siendo televisión abierta, siendo necesario la implementación de políticas de seguridad informáticas para precautelar los activos de la información.

En la Figura 32 se muestra el organigrama de la institución el cual identifica el área de Ingeniería como parte del área técnica para la administración de los activos de información incluida la red de infraestructura.

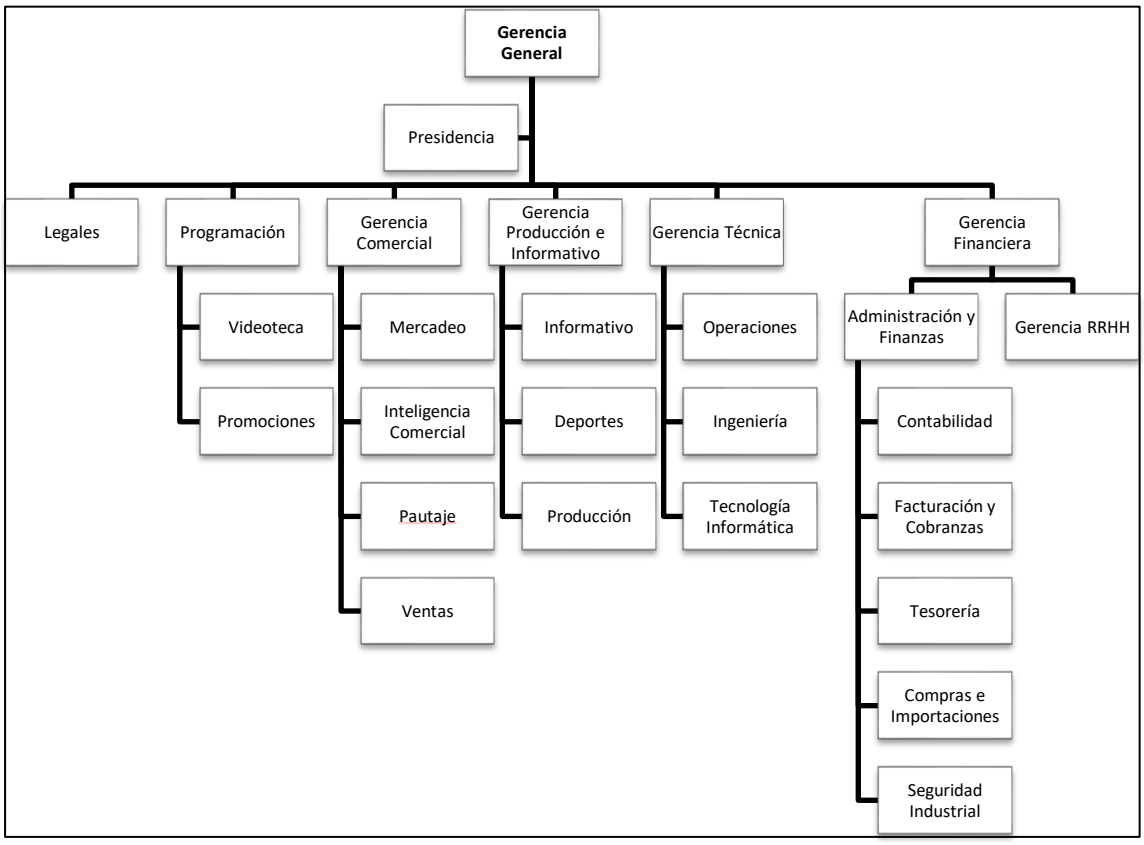


Figura 32. Organigrama de la empresa de Televisión

El personal de Ingeniería de la organización es el responsable de la infraestructura de red en todo su ciclo y puntos de acceso de los equipos de transmisión de la señal televisiva a nivel nacional. En la Figura 33 se muestra la topología tipo estrella del canal de televisión y los equipos de red en todos los puntos de acceso a nivel nacional comunicados por enlace dedicado de datos a nivel de capa 2 en estos segmentos de red.

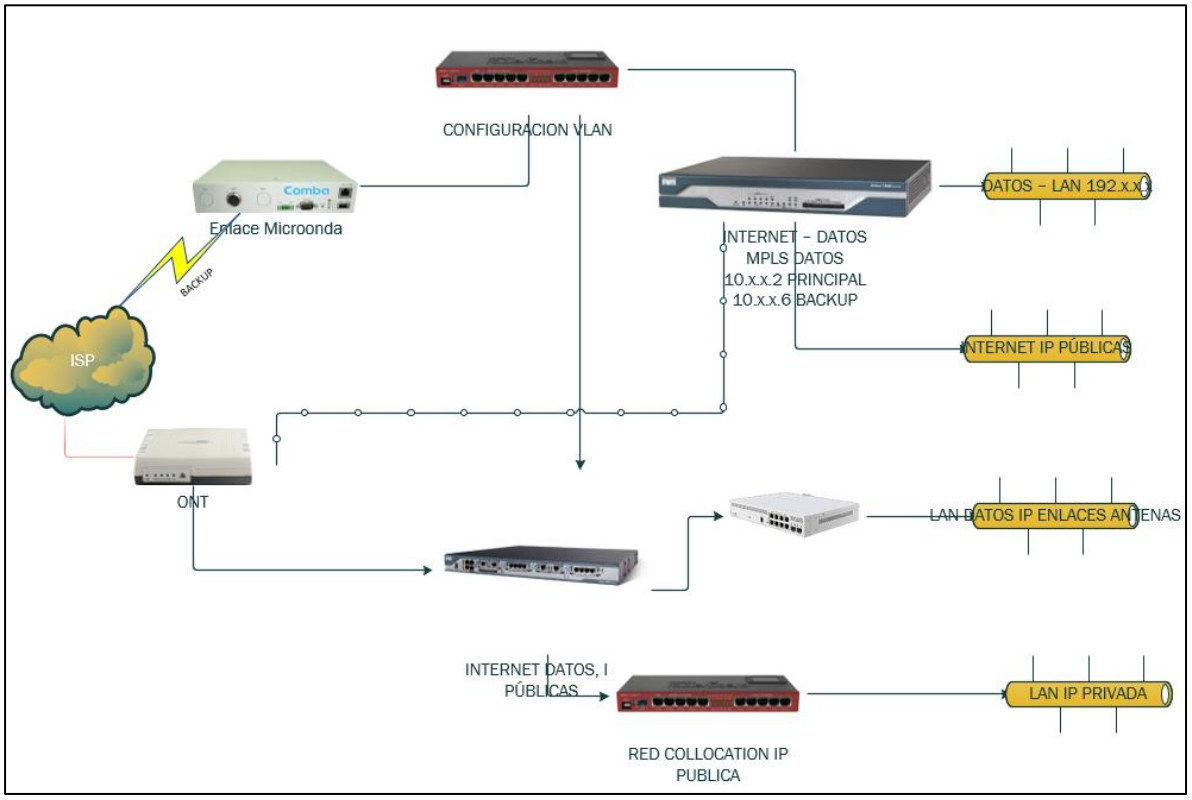


Figura 33. Topología de red de Ingeniería

La conectividad con cada una de las sedes con la matriz ubicadas en las principales ciudades del país de hace con tecnología MPLS (Multiprotocol Label Switching) la cual se define como la conmutación multiprotocolo de etiquetas que transfiere los datos a través de una red virtual y privada (Ver Figura 34). En cada una de las ciudades se tienen al personal operativo para la carga del material de transmisión: audio y videos de la programación diaria del canal de televisión. En estas sedes también se encuentra el personal administrativo y toda la planta del personal.

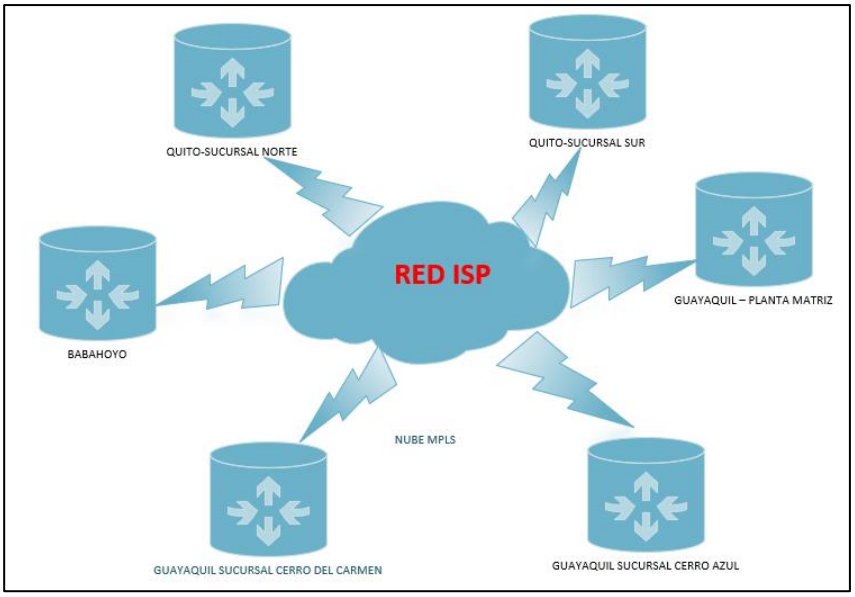


Figura 34. Red MPLS entre ciudades

A nivel nacional se encuentran distribuidas las antenas de transmisión con repetidoras de la señal, en estos puntos se estableció enlaces en capa 2 para el monitoreo de la señal. La Figura 35 muestra la distribución en las diferentes localidades en Ecuador a través de la nube MPLS.

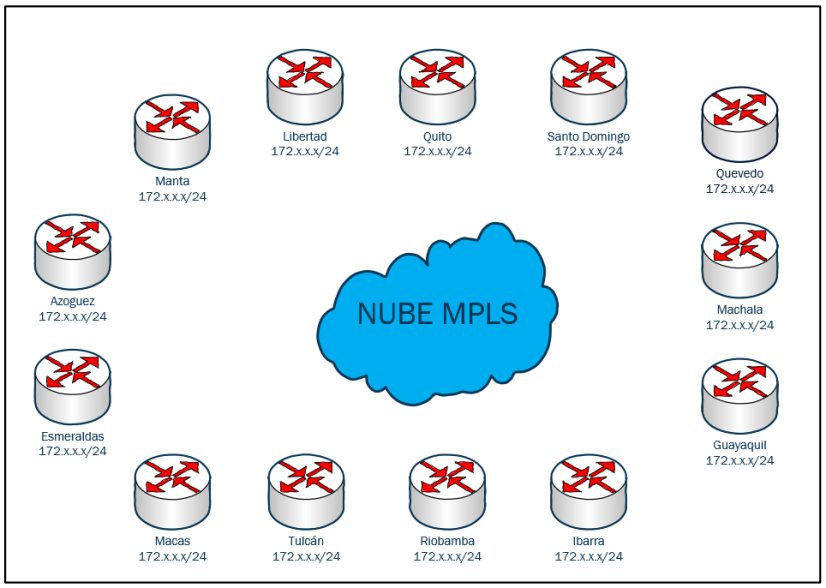


Figura 35. Nube MPLS para monitoreo de localidades en la señal televisión en el Ecuador

En la infraestructura expuesta surge la necesidad de implementación de herramientas que permitan analizar las vulnerabilidades en la red, calificar los riesgos y tener un plan de acción para mitigar el impacto por interrupción de servicio en caso de alguna falla debido a la

explotación de alguna vulnerabilidad.

Los procesos de que plantean en la propuesta como fase de identificación son:

- Área de Ingeniería debe catalogar la información sensible en sus sistemas: Nexio, Grass Valley Stratus, dispositivos capa 2 (codificadores y decodificadores)
- Área de Ingeniería debe reconocer y exponer las políticas de ciberseguridad.
- Área de Ingeniería debe clasificar e identificar los servicios esenciales para que la señal de televisión pueda emitirse.
- El acceso de los usuarios a los equipos debe inventariarse y mostrar la administración con políticas de actualización continúo.

- **Protección**

- El acceso a los equipos de la red de transmisión de señal de televisión debe ser s través de usuarios restringidos debidamente identificados y autorizados por la Gerencia Técnica.
- Los sistemas: Nexio, Grass Valley Stratus, dispositivos capa 2 (codificadores y decodificadores) y otros equipos de la red de transmisión que manejen información sensible deben tener la protección contra las vulnerabilidades reconocidas.
- Se debe proteger la cuenta de super administrador y otras privilegiadas en los accesos a equipos y sistemas, debe tener cero tolerancias a las vulnerabilidades de ataques informáticos.

- **Detección**

- El área de ingeniería debe usar herramientas para la detección de ataques a los sistemas informáticas. De acuerdo con la consultora Gartner Groups en su página web define a las soluciones de detección y respuestas de punto final (EDR) como plataformas que analizan y gestionan los comportamientos sospechosos para bloquearlos y dar soluciones de remediación frente a ataques (Gartner, s.f.). En la página oficial de Gartner se puede observar las herramientas que existen en el mercado tales como: Singularity Platform, Trend Micro, Harmony EndPoint, MDE de Microsoft, Cortex XDR, CrowdStrike, ESET Inspect entre otras.

- **Respuesta**

En esta fase el área de Ingeniería debe tener el plan de acción para responder a un evento de ciberseguridad que afecte la señal de transmisión del canal, el mismo que debe ser probado y ejecutado por los responsables del área.

- **Recuperación**

En esta fase el área de Ingeniería debe tener el plan de acción y contingencias para la remediación para garantizar la emisión de la señal de transmisión del canal en caso de alguna falla.

5.7. Diseño de la propuesta

La propuesta consiste en realizar testeo en toda la red de transmisión del canal de TV cumpliendo las siguientes fases:

- **Inventario de los activos de la información (Ver Anexo 2).**
- **Identificación de IP Activas con el uso de la herramienta NMAP**

El comando NMAP tiene algunos parámetros, dentro de ellos la detección de IP Activas ejecutando el comando: nmap -Sp [segmento de red].

- **Identificación de sistemas Operativos y Aplicaciones**

Con el comando NMAP a través del parámetro -o se activa la detección de sistema operativo, se debe ejecutar: nmap -o [segmento de red]. En la Figura 36 se tabula el resultado de la detección.

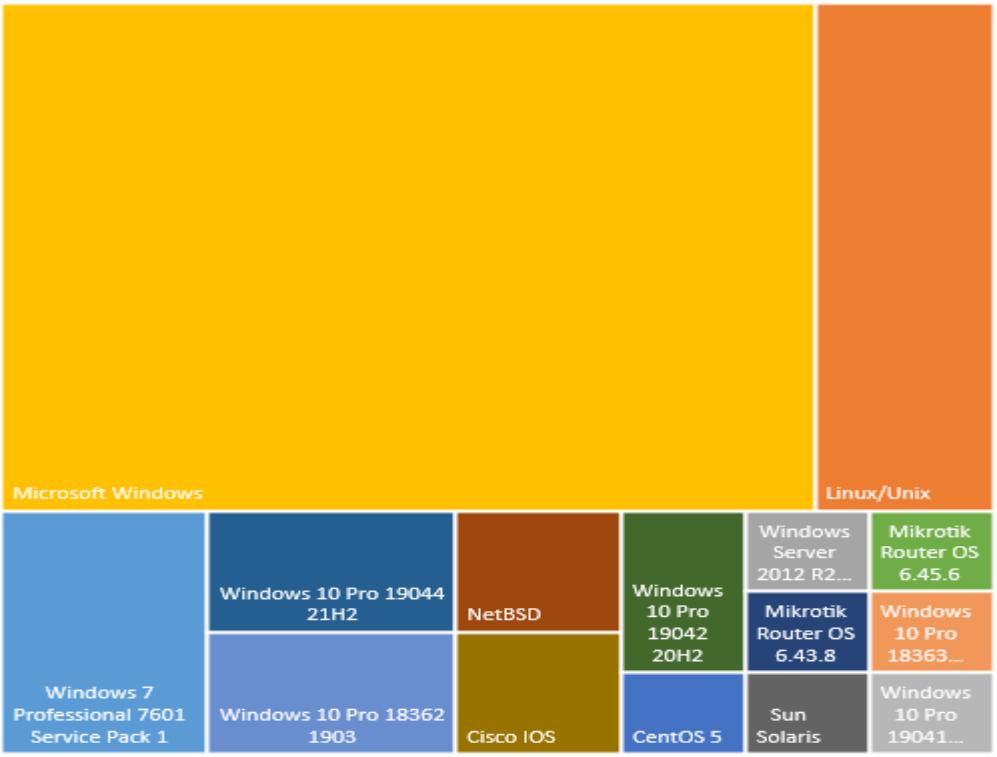


Figura 36. Inventario de Sistemas Operativos

- **Análisis de vulnerabilidades**

Ejecutar la herramienta OPENVAS/GVM, definiendo el Target (objetivo) de la tarea a ejecutarse con los parámetros básicos: Nombre, hosts objetivos, lista de puertos a escanear. La lista de puertos a escanear puede ser personalizada o las preconfiguradas por la herramienta (Ver Figura 37).

Name ▲		Port Counts		
		Total	TCP	UDP
All IANA assigned TCP (Version 20200827.)		5836	5836	0
All IANA assigned TCP and UDP (Version 20200827.)		11318	5836	5482
All TCP and Nmap top 100 UDP (Version 20200827.)		65635	65535	100

Figura 37. Listado de Puertos preconfigurados en la herramienta OpenVAS

En la Figura 38 se muestra las opciones del Target (Objetivo) para este estudio.

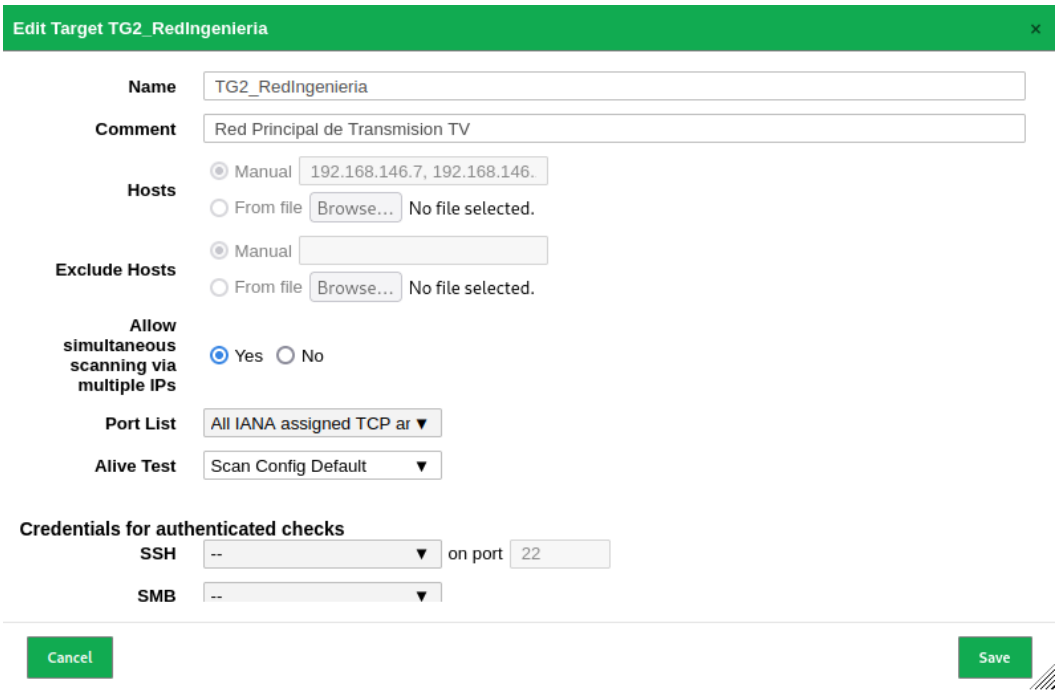


Figura 38. Parámetros de opción Target OpenVAS

En la tarea de la herramienta se coloca el nombre, el target establecido, el scanner. En la siguiente figura se muestran los parámetros de la Tarea a ejecutarse. (Ver Figura 39)

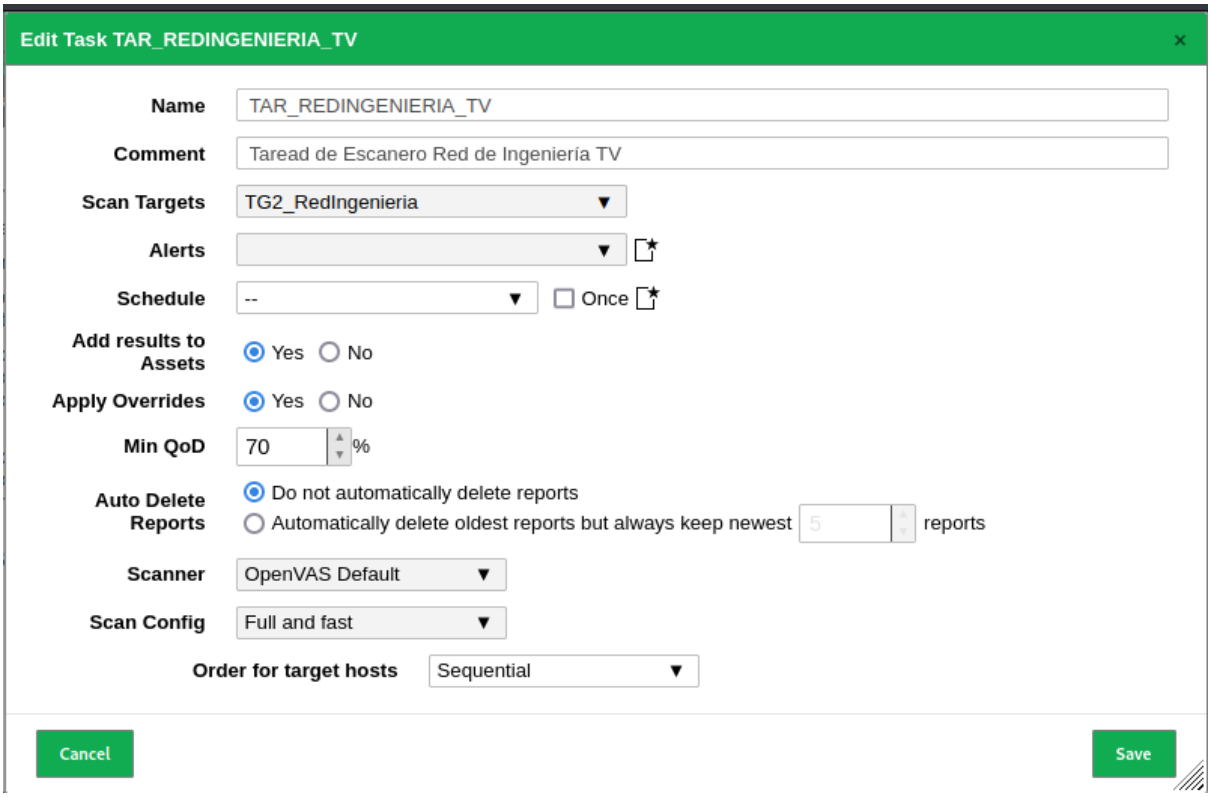


Figura 39. Parámetros de opción Tarea de OPENVAS

A continuación, se ejecuta la tarea con la opción “Start” de la misma opción (Ver Figura 40)

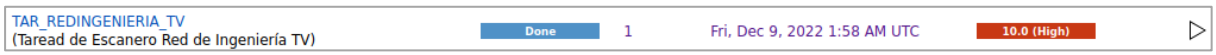


Figura 40. Ejecución de la Tarea

- **Evaluación de vulnerabilidades**

La evaluación de vulnerabilidades detallará reportes como la criticidad de riesgo en los sistemas operativos, un ejemplo de esta evaluación se visualiza en la Figura 41.

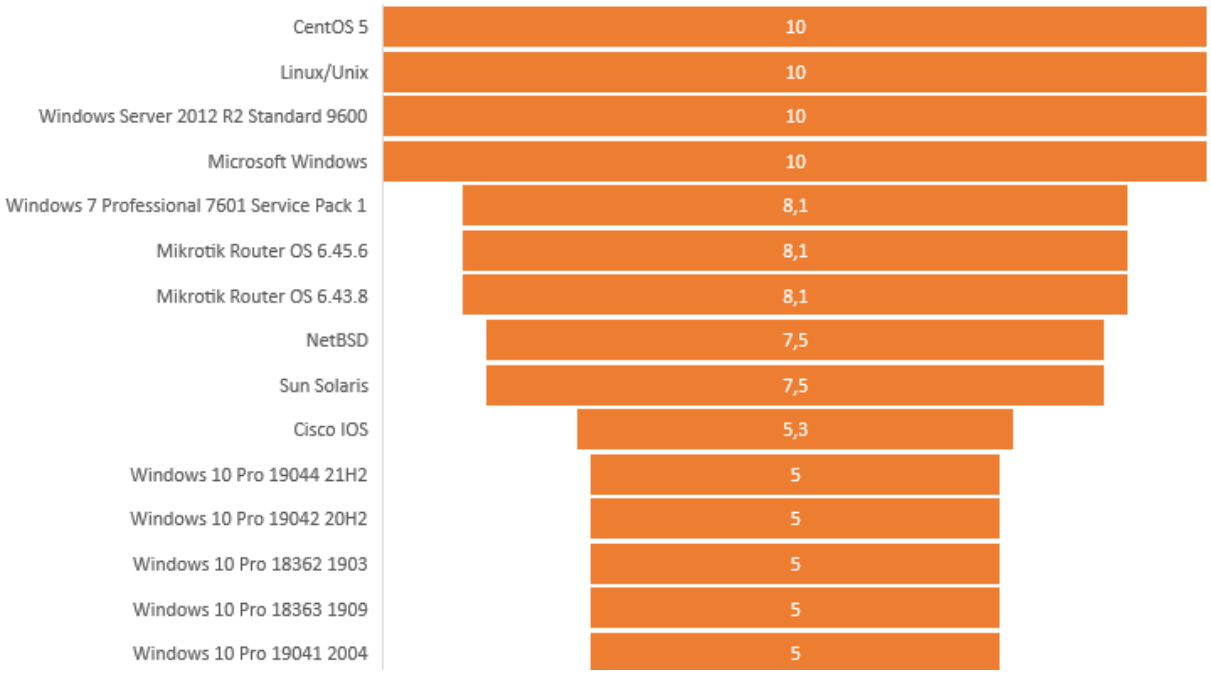


Figura 41. Resultado nivel de riesgo en Sistemas Operativos

Se observa que los equipos con sistemas operativos Linux, Unix, Windows Server 2012 y Microsoft Windows en la red de transmisión del canal de TV tienen el puntaje máximo de riesgo. En el análisis de sensibilidad de información que manejan estos equipos se debe evaluar la solución a las vulnerabilidades encontradas. La Figura 42 muestra los gráficos de la herramienta OPENVAS correspondiente a las vulnerabilidades encontradas en los sistemas operativos.

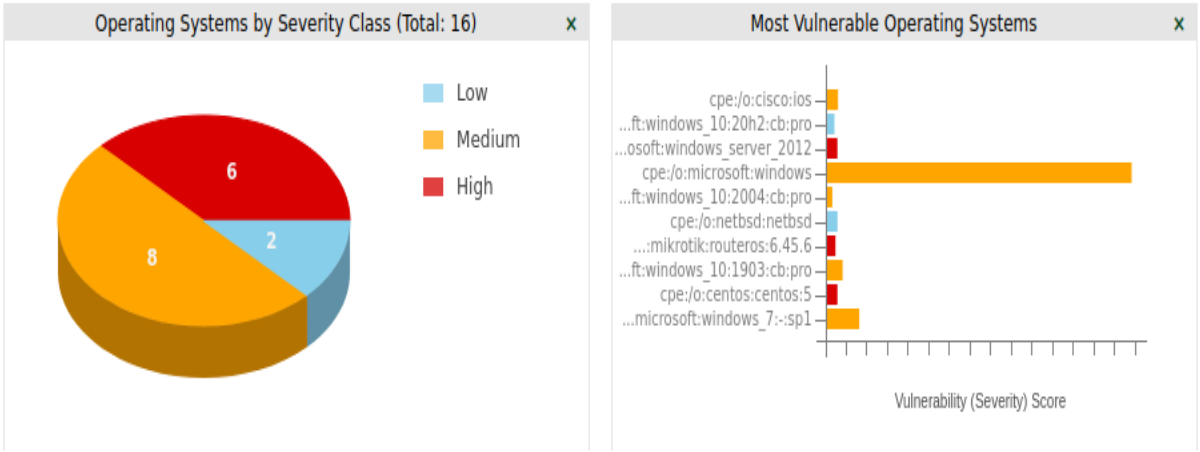


Figura 42.Sistemas Operativos activos encontrados en el escaneo de la herramienta OPENVAS

En el mismo orden se evalúa la criticidad en los equipos escaneados, revelando que el

66% de los equipos de la red de transmisión del canal tienen una vulnerabilidad media, el 22% tiene una calificación baja de riesgo y el 12% una alta vulnerabilidad. Se grafica el resultado en la Figura 43.

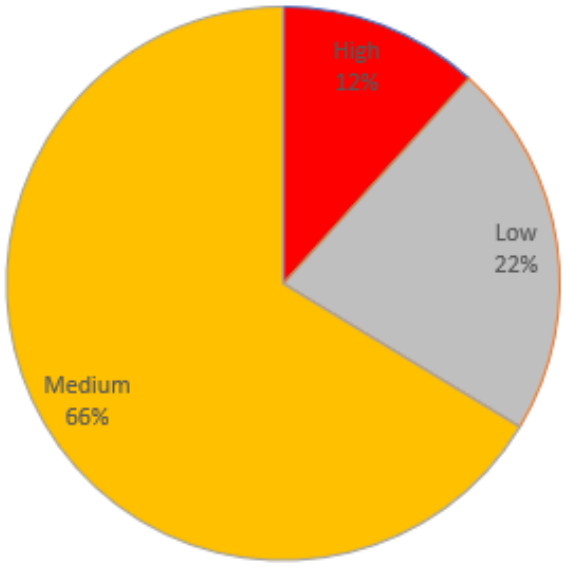


Figura 43. Resultado de calificación de riesgo en los equipos de señal de transmisión de TV

Las vulnerabilidades encontradas en la muestra de equipos indican el tipo de solución: 80% están en mitigación, 13% en VendorFix y el 7% en Workaround, representada en la Figura 44.

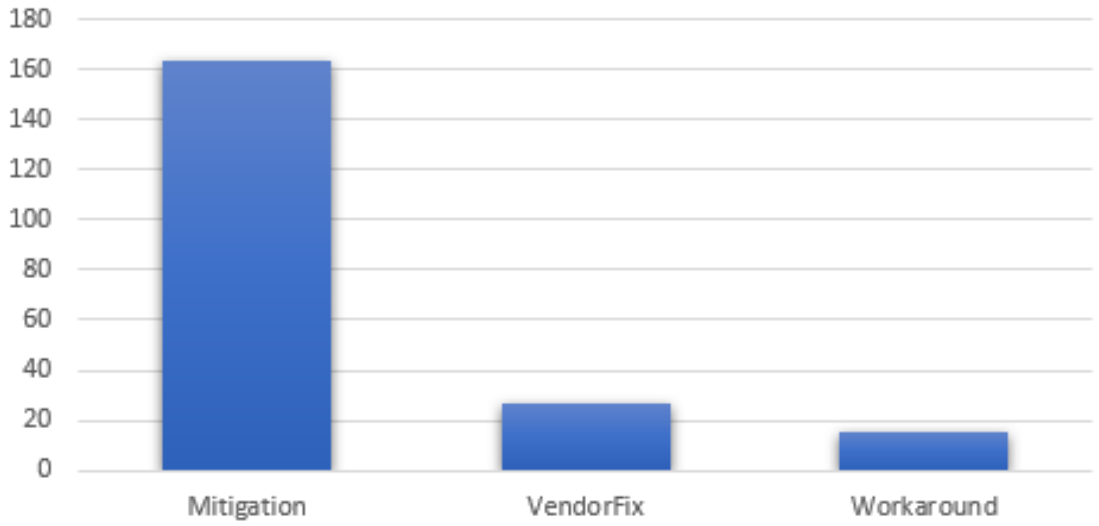


Figura 44. Tipo de soluciones a las vulnerabilidades encontradas en la muestra.

La descripción de las vulnerabilidades encontradas en la nuestra con el tipo de solución

de detallan en la Tabla 16.

Tabla 16.

Descripción de vulnerabilidades con la clasificación de tipo de solución

Solution Type	NVT Name
Mitigation	Anonymous FTP Login Reporting
Mitigation	Check for Chargen Service (TCP)
Mitigation	Check for Chargen Service (UDP)
Mitigation	Check for discard Service
Mitigation	DCE/RPC and MSRPC Services Enumeration Reporting
Mitigation	DNS Cache Snooping Vulnerability (UDP) - Active Check
Mitigation	echo Service Reporting (TCP + UDP)
Mitigation	FTP Unencrypted Cleartext Login
Mitigation	FTP Writeable Directories
Mitigation	HTTP Debugging Methods (TRACE/TRACK) Enabled
Mitigation	ICMP Timestamp Reply Information Disclosure
Mitigation	Operating System (OS) End of Life (EOL) Detection
Mitigation	POP3 Unencrypted Cleartext Login
Mitigation	rsh Unencrypted Cleartext Login

Solution Type	NVT Name
Mitigation	SSL/TLS: Certificate Expired
Mitigation	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
Mitigation	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
Mitigation	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Mitigation	SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection
Mitigation	SSL/TLS: Report Weak Cipher Suites
Mitigation	SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits
Mitigation	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)
Mitigation	TCP timestamps
Mitigation	The rexec service is running
Mitigation	Weak Encryption Algorithm(s) Supported (SSH)
Mitigation	Weak Host Key Algorithm(s) (SSH)
Mitigation	Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Solution Type	NVT Name
Mitigation	Weak MAC Algorithm(s) Supported (SSH)
VendorFix	Apache HTTP Server httpOnly Cookie Information Disclosure Vulnerability
VendorFix	Deprecated SSH-1 Protocol Detection
VendorFix	Microsoft MS03-034 security check
VendorFix	Microsoft SQL Server End Of Life Detection
VendorFix	Microsoft SQL Server Multiple Vulnerabilities (MS15-058)
VendorFix	Microsoft SQL Server Multiple Vulnerabilities (MS16-136)
VendorFix	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
VendorFix	SSL/TLS: RSA Temporary Key Handling RSA_EXPORT Downgrade Issue (FREAK)
Workaround	Check if Mailserver answer to VRFY and EXPN requests
Workaround	Cleartext Transmission of Sensitive Information via HTTP
Workaround	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Fuente: GreenBone (2022)

La herramienta de escaneo ofrece varias alternativas de informes y reportes para mayor usabilidad del responsable de la seguridad, tales como tablas, gráficos circulares, barras e

incluso nube de palabras (Ver Figura 45).

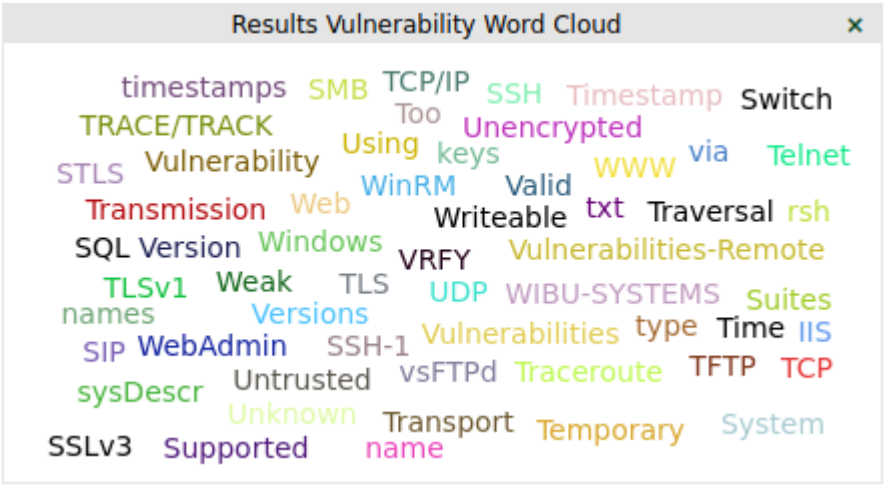


Figura 45. Resultado de escaneo (gráfico de nube de palabras)

- **Evaluación de Impacto y riesgo**

El impacto de cada vulnerabilidad encontrada obtendrá una sugerencia de remediación pero también indicará el impacto de que dicha vulnerabilidad sea explotada. En la Figura 46 se detalla la vulnerabilidad: "Microsoft SQL Server End of Life Detection", detallando en el impacto que al no tener actualizaciones puede quedar comprometida la seguridad del equipo.

Figura 46. Impacto y Solución para una vulnerabilidad encontrada con la herramienta OpenVAS

La herramienta OPENVAS detalla los impactos posibles de las vulnerabilidades

encontradas en cada uno de los hosts. Un resumen de los impactos se muestra en la Tabla 17.

Tabla 17.

Listado de impactos de vulnerabilidades encontradas en el escaneo

Impactos
• A side efect of this feature is that the uptime of the remote host can sometimes be computed
• An attacker can quickly break individual connections
• An attacker can uncover usernames and passwords by sni-ng tra-c to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used
• An attacker could seek to exploit this vulnerability by sending a NetBT Name Service query to the target system and then examine the response to see if it included any random data from that system's memory.
• An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.
• An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords
• An attacker may use this fact to gain more knowledge about the remote host.
• An attacker may use this flaw to trick your legitimate web
• An attacker may use this misconfiguration problem to use the remote FTP server to host arbitrary data, including possibly illegal content
• An attacker might be able to decrypt the SSL/TLS communication offline.
• An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection

Impactos

- An authenticated attacker may have read access to the entire filesystem
- An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network.|solution=- Under Unix systems, comment out the 'chargen' line in /etc/inetd.conf and restart the inetd process
- An end-of-life version of Microsoft SQL Server is not receiving any security updates from the vendor.
- An EOL version of an OS is not receiving any security updates from the vendor
- Attackers can exploit this vulnerability to reset credential storage, which allows them access to the management interface as an administrator without authentication
- Attackers might gain information about cached DNS records
- Based on the files accessible via this anonymous FTP login
- By sending a crafted packet, an authenticated remote user can cause high cpu load, which may make the device respond slowly or unable to respond
- If an attacker is able to guess a PUBLIC community string, they would be able to read SNMP data (depending on which MIBs are installed) from the remote device. This information might include system time, IP addresses, interfaces, processes running, etc.
- Successful exploitation could allow remote attackers to bypass security
- Successful exploitation will allow attackers to obtain sensitive information
- Successful exploitation will allow remote attackers to elevate their privileges or execute arbitrary code
- Successful exploitation will allow remote attackers to gain elevated privileges that could be used to view, change, or delete data, or create new accounts, also can gain additional database and file information and to spoof content, disclose

Impactos
information, or take any action that the user could take on the site on behalf of the targeted user • Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack • The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection • This information might give an attacker information for further reconnaissance and/or attacks (e.g. subnet structure, filter bypass, etc.) • This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration • Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

Fuente: GreenBone (2022)

5.8. Funcionamiento

Para el correcto funcionamiento del análisis de vulnerabilidades debe actualizar la herramienta de escaneo y ejecutarse de forma periódica según la política del sistema de gestión de seguridad. La capacitación al personal encargado de la seguridad de la información es fundamental para su correcto uso.

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

- Con base a los resultados obtenidos de la herramienta OpenVAS los cuales muestran un alto porcentaje de equipos con vulnerabilidad entre media y alta se concluye que el monitoreo de dichas vulnerabilidades en la red del canal de televisión debe ser constante, con actualizaciones periódicas para la temprana detección de las debilidades y fragilidad en su seguridad informática, siendo el tema de ciberseguridad una de las grandes preocupaciones de todo administrador de sistemas informáticos y en el caso del canal de televisión cuyo ente regulador en el otorgamiento de frecuencia exige que tenga todos los mecanismos para proteger la emisión de la señal.
- Luego del análisis con las herramientas propuestas se llegó a la conclusión que no existe un control de las actualizaciones tanto de las aplicaciones como de los equipos. Dentro de las vulnerabilidades encontradas se observa que muchas aplicaciones ya están fuera del tiempo de servicio del vendedor. En este mismo análisis de falta de actualizaciones se concluyó que el canal de televisión no ha actualizado estos componentes debido a la capacidad de su hardware y también a la tecnología con señal análoga que no implicaba tener los equipos conectados a una red. Con el paso a señal digital y los cambios en infraestructura con redes de datos ha provocado que esta vulnerabilidad sea relevante debido su exposición en la red y a que no puede seguir realizando actualizaciones de seguridad para proteger a los sistemas. Esto implica que debe analizarse la obsolescencia no solo de las aplicaciones sino del hardware y toda la infraestructura de red del canal de televisión.
- Se puede concluir que el costo-beneficio, ventajas y desventajas de tener tecnología actualizada con soportes de seguridad versus el mantenimiento de tecnología antigua que no permite seguir creciendo, es de gran impacto, las desventajas son mayores y presenta un riesgo latente, no hay ahorro, el impacto económico puede provocar incluso el cierre de la empresa.
- Se concluye que el uso de herramientas como Kali Linux y OpenVAS que son potentes en las búsquedas de vulnerabilidades y la ventaja de que son de código abierto con una comunidad que realiza grandes aportaciones, son transparentes, no implica costos de licencia, hace que la propuesta de implementación se pueda aplicar a la empresa sin incurrir en grandes costos, teniendo como ventaja el uso de la aplicación en ambiente web sin límites de máquinas.

- Se ha concluido también luego del resultado de las entrevistas que la falta de conocimiento en ciberseguridad en el personal responsable de los equipos que emiten la señal televisiva es un riesgo mayor. Es importante aclarar que el conocimiento en ciberseguridad es muy necesario, una parte que siempre hay mayor riesgo y vulnerabilidad es en la parte humana tanto por desconocimiento como de forma intencional. Se debe implementar capacitaciones no solo al personal especializado sino a todo el personal para que los ciberdelincuentes no vulneren por la parte de del desconocimiento y afecte a la operación de la empresa y en los peores casos al cierre de esta.
- Luego del análisis tanto de la herramienta de escaneo como en las entrevistas al personal se concluye que la propuesta de análisis de vulnerabilidades en el canal de televisión ayudará en grandes rasgos al cumplimiento de las normas de seguridad de las entidades regulatorias. En esta se muestra un detalle de los pasos a seguir según cronograma de trabajo para que la empresa observe su desarrollo y cumplimiento de la proyección, enfatizando que esto es sólo parte del proceso inicial para que la empresa tenga un diagnóstico de su vulnerabilidad.
- Sería interesante en proyectos a futuros consolidar la información del análisis de vulnerabilidad de OpenVAS con otras herramientas de gestión de seguridad tales como OSSIM o Negios para fortalecer la seguridad en el canal de televisión.

6.2. Recomendaciones

- El canal de televisión ha realizado una inversión importante en la adquisición de equipos y servicios para la red de datos en la señal de digital, se recomienda proteger dicha inversión con actualización de los equipos de cómputo de la red del canal tanto en su software como en su hardware para mitigar los problemas de ciberseguridad.
- Uno de los beneficios de la herramienta OPENVAS es que muestra tanto la vulnerabilidad como la acción a ejecutar para que esta se mitigue, por lo que se recomienda que se ejecuten dichas acciones, entre los cuales resaltan:
    - Actualizaciones a los sistemas, ejecutar los parches de seguridad.
    - Actualización o eliminación de protocolos inseguros como SMB 1.0
    - Cambio de metodología de acceso a recursos compartidos
    - Implementar certificados de seguridad SSL/TLS con empresas certificadas.
    - Realizar la tarea de análisis de vulnerabilidades de forma periódica
    - Tener los inventarios de activos al día.

- En relación con el personal es necesario crear periódicamente capacitaciones de análisis de riesgos informáticos y análisis de vulnerabilidades. También se recomienda tener lista de accesos a cada uno de los recursos, así el personal entrenado y con las herramientas disponibles podrá tener mayor capacidad de respuesta contra ataques y mejor protección de los activos de la información.
- Se recomienda que el canal de televisión implemente dentro de sus políticas un marco de seguridad tal como NIST o ISO/IEC 27000 para mitigar los riesgos lo cual beneficiará su control y protección con la orientación a la mejora continua.

Referencias Bibliográficas

Abi-Habib, M. (6 de Octubre de 2022). *The New York Times*. El hackeo del ejército mexicano expone secretos de la institución mas poderosa del país: https://www.nytimes.com/es/2022/10/06/espanol/mexico-sedena-guacamaya-hackeo.html

Aksu, M. U., Bicakci, K., & Altuncu, E. (2019). A First Look at the Usability of OpenVAS. Ankara: TOBB University of Economics and Technology. https://doi.org/10.14722/usec.2019.23026

Almagro, L. (2019). *CIBERSEGURIDAD MARCO NIST.* Un abordaje integral de la Ciberseguridad: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Astakhova, L., & Muravyov, N. (2019). A Data Collection and Analysis System for Managing the Vulnerabilities of Users of an Information System in a Small Business. *2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, (págs. 193-196). https://doi.org/10.1109/USBEREIT.2019.8736583

Bautista, S. (2022). *studocu.* (U. d. Guatemala, Ed.) Vulnerabilidades Web: https://www.studocu.com/gt/document/universidad-de-san-carlos-de-guatemala/financiera/vulnerabilidades-web/21341553

Berrío, J., Montoya Pérez, Y., Pérez Zapata, G., & Jiménez Builes, J. (2016). Modelo para la evaluación de desempeño de los controles de un SGSI badaso en el estándar ISO/IEC 27001. *VIII Congreso Internacional de Computación y Telecomunicaciones*, (pág. 113). Medellín - Colombia.

Chalvatzis, I., Karras, D., & Papademetrio, R. (2019). Evaluation of Security Vulnerability Scanners for Small and Medium Enterprises Business Networks Resilience towards Risk Assessment. *2019 IEEE International Conference on Artificial Intelligence and Computer Applications*, (págs. 52-58). https://doi.org/10.1109/ICAICA.2019.8873438

Chaparro, S., Gonzalez, S., Miranda, N., & Paez, R. (s.f.). Seguridad en la capa de enlace del modelo OSI.

Commnunity-Greenbone. (2022). *Portal de la comunidad Greenbone*. https://community.greenbone.net/

Cordero Vargas, Z. (2009). LA INVESTIGACIÓN APLICADA_ UNA FORMA DE CONOCER LAS REALIDADES CON EVIDENCIA CIENTÍFICA. *33(1)*, 155-165. San PedroCosta Rica, Monte de Oca, Costa Rica: REVISTA EDUCAción. http://www.redalyc.org/articulo.oa?id=44015082010

Gartner. (s.f.). *https://www.gartner.com/.* Enpoint Detection and Response (EDR) Solutions Reviews and Ratings: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

Gorbenko, A., Romanovsky, A., Tarasyuk, O., & Biloborodov, O. (2020). From Analyzing Operating System Vulnerabilities to Designing Multiversion Intrusion-Tolerant Architectures. *IEEE Transactions on Reliability, 69*, págs. 22-39. https://doi.org/10.1109/TR.2019.2897248

GrassVAlley. (s.f.). *GV STRATUS.* grassvalley.com: https://www.grassvalley.com/products/media-asset-management/gv-stratus/

GreenBone. (2022). *https://www.openvas.org/.* History of the OpenVAS project: https://greenbone.github.io/docs/latest/background.html#history-of-the-openvas-project

Hernández, R., & Mendoza, C. (2018). *Metodología de la investigación.* (M.-H. I. C.V., Ed.)

México, México.
Hines, C., & Chowdhury, M. (2022). Uncover Security Weakness Before the Attacker Through Penetration Testing., (págs. 495-497). https://doi.org/10.1109/eIT53891.2022.9813950
INCIBE. (16 de enero de 2017). *¡Fácil y sencillo! Análisis de riesgos en 6 pasos.* https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo
INCIBE CERT_. (Marzo de 2020). *Guía para la gestión de un inventario de activos en sistemas de control industrial.* https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe-cert_guia_inventario_de_activos_2020_v1.pdf
INCIBE. (s.f). *GESTION DE RIESGOS - Una guía de aproximación para el empresario.* https://www.incibe.es/: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf
ISO. (2013). *Information technology — Security techniques — Information security management systems — Requirements.* © ISO/IEC 2013 – All rights reserved: www.iso.org
KALI. (30 de Octubre de 2022). *https://www.kali.org/.* Choose your Kali: https://www.kali.org/images/iso-64-installer.svg
Kaspersky. (16 de Octubre de 2022). *CIBERAMENAZA EN TIEMPO REAL*. https://cybermap.kaspersky.com/es/stats#country=35&type=IDS&period=m
Kim, S., Lee, D., & Hong, C. (2016). Vulnerability detection mechanism based on open API for multi-user's convenience. *International Conference on Information Networking.* https://doi.org/ doi: 10.1109/ICOIN.2016.7427159
MINTEL. (s.f.). *https://www.telecomunicaciones.gob.e.* https://www.telecomunicaciones.gob.ec/television-movil-una-ventaja-mas-la-tdt/
Mitnick, K., & Simon, W. (2021). *The Art of Deception-Controlling the Human Element of Security.*
Monev, V. (2020). "Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002. *2020 International Conference on Information Technologies,* (págs. 1-5). Varna, Bulgaria. https://doi.org/10.1109/InfoTech49733.2020.9211066.
NISCT. (12 de April de 2018). *CiberSecurity Framework.* The Five Functions: https://www.nist.gov/cyberframework/online-learning/five-functions
NIST, N. (s.f.). *NIST NATIONAL VULNERABILITY DATABASE*. SEARCH AND STATISTICS: https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all&isCpeNameSearch=false
normastecnicas.com. (s.f.). *Normas Técnicas ABNT, ISO, NR. IEEE*. SÉRIE ISO 27000: https://www.normastecnicas.com/serie-iso-27000/
RAE. (s.f). *https://dle.rae.es/vulnerar*. https://dle.rae.es/vulnerar
RO #149. (23 de diciembre de 2013). *https://tdtecuador.mintel.gob.ec/.* REGLAMENTO TÉCNICO: https://tdtecuador.mintel.gob.ec/wp-content/uploads/2017/05/Reglamento-T%C3%A9cnico-Ecuatoriano-083_Televisores-con-Sintonizador-Digital.pdf
Serrano, D. (2021 de Julio de 2021). *El Comercio*. CNT dijo que sufrió ataque informático de 'alta sofisticación': https://www.elcomercio.com/actualidad/negocios/cnt-ataque-informativo-hackeo-sofistificacion.html
Silvestra Miraya, I., & Humán Nahula, C. (Marzo de 2019). Pasos para elaborar la investigación y la redacción de la tesis universitaria. Lima, Perú: San Marcos de Aníbal Jesús Paredes Galván.

https://repositorio.utea.edu.pe/bitstream/utea/195/3/Pasos%20para%20elaborar%20la%20investigaci%c3%b3n%20y%20la%20redacci%c3%b3n%20de%20la%20tesis%20universitaria.pdf
Stallman, R. (s.f.). El software Libre y la Educación. https://www.gnu.org/education/rms-education-es.es.ogv
THOMSON. (s.f.). RD4000 Distribution Receiver Decoder. *PRODUCT DATA SHEET*.
THOMSON. (s.f.). ViBE CP6000 Contribution Platform. *Product Data Sheet*.
Torres, M., Paz, K., & Galazar, F. (s.f.). ´METODOS DE RECOLECCIÓN DE DATOS PARA UNA INVESTIGACIÓN. *Boletín Electrónicoi No. 03*. Universidad Rafael Landívar. Retrieved 13 de Noviembre de 2022, from http://148.202.167.116:8080/jspui/bitstream/123456789/2817/1/M%c3%a9todos%20de%20recolecci%c3%b3n%20de%20datos%20para%20una%20investigaci%c3%b3n.pdf
Vimala, K., & Fugkeaw, S. (2022). VAPE-BRIDGE: Bridging OpenVAS Results for Automating Metasploit Framework. *2022 14th International Conference on Knowledge and Smart Technology* , (págs. 69-74). https://doi.org/10.1109/KST53302.2022.9729085
Wang, Y., Bai, Y., LI, L., Chen, X., & Chen, A. (2020). Design of Network Vulnerability Scanning System Based on NVTs. *2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)*, (págs. 1774-1777). Chongqing, China. https://doi.org/10.1109/ITOEC49072.2020.9141812.
WEF, & Accenture. (Enero de 2022). https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf
Yosifova, V., Tasheva, A., & R. Trifonov. (2021). Predicting Vulnerability Type in Common Vulnerabilities and Exposures (CVE) Database with Machine Learning Classifiers. *2021 12th National Conference with International Participation (ELECTRONICA)*, (págs. 1-6). https://doi.org/10.1109/ELECTRONICA52725.2021.9513723

ANEXOS

Anexo 1

Instalación de OpenVAS.

La herramienta OpenVAS/GVM debe ser instalada desde la consola de Kali-Linux, este sistema operativo es open source, diseñado para la seguridad informática, es mayormente usado por profesionales para el pentesting usando pruebas de penetración avanzadas, informática forense, ingeniería inversa e investigación de seguridad, es una distribución del sistema operativo Linux basado en Debian. Se lo puede descargar desde el siguiente enlace: https://www.kali.org/get-kali/#kali-installer-images en versiones de 32 bits y 64 bits e instalarlo sobre una máquina virtual.

Los pasos para la instalación de OPENVAS/GVM son los siguientes:

1. Desde la consola de comando de Kali-Linux se debe actualizar el sistema operativo con el comando:

```
sudo apt-get update
sudo apt-get upgrade
```

2. Se debe seguir el proceso de instalación de GVM con los siguientes comandos:

```
sudo apt-get install gvm*
```

3. Los siguientes comandos instalan el firewall o cortafuego, lo habilita y permite el paso del puerto 80 y 9392 para acceso web:

```
sudo apt-get install ufw
sudo ufw enable
sudo ufw allow 80
sudo ufw allow 9392
```

4. Se continúa con la instalación del Asistente de Seguridad de GreenBone, certificados y agente de mensajes:

```
sudo apt-get install -y greenbone-security-assistant
sudo runuser -u _gvm -- gvm-manage-certs -a -f
sudo apt-get install redis
systemctl start redis-server@openvas.service
```

5. Se habilita la sincronización con las bases de vulnerabilidades NVT SCAP, se crea la

base de datos, se crea el usuario administrador de la herramienta.

```
sudo runuser -u _gvm -- greenbone-nvt-sync
sudo runuser -u _gvm -- greenbone-feed-sync --type SCAP
sudo runuser -u _gvm -- greenbone-feed-sync --type CERT
sudo runuser -u postgres -- /usr/share/gvm/create-postgresql-database
sudo runuser -u _gvm -- gvmd –create-user=<user> --password=<password>
```

6. Se establece permisos al archivo de log, se verifica la instalación que debe indicar que el proceso está funcionando correcto y finalmente se inicia la ejecución de la herramienta.

```
sudo chmod 666 /var/log/gvm/openvas.log
sudo gvm-check-setup
sudo gvm-start
```

7. Se muestra la pantalla de inicio para ingreso a la herramienta OPENVAS/GVM (Ver Figura 47).

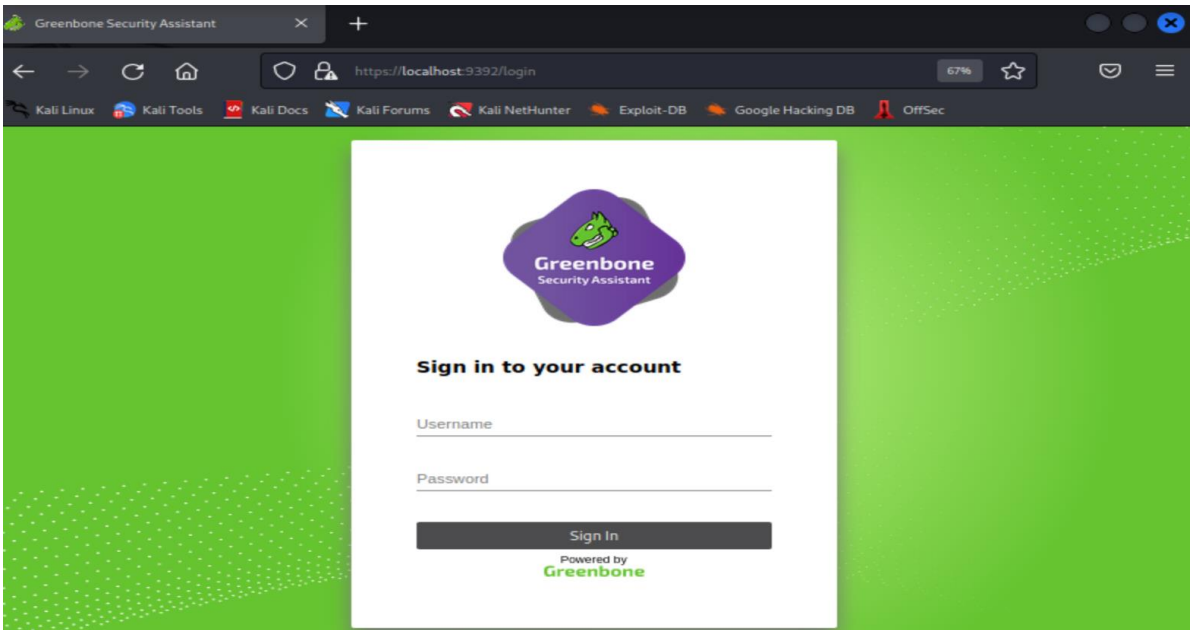


Figura 47. Ingreso a la herramienta OPENVAS en ambiente web

Una de las funcionales de OPENVAS es el uso de wizard para usuarios que aún no están familiarizados con la herramienta permitiendo mayor usabilidad. La Figura 48 muestra esta opción.

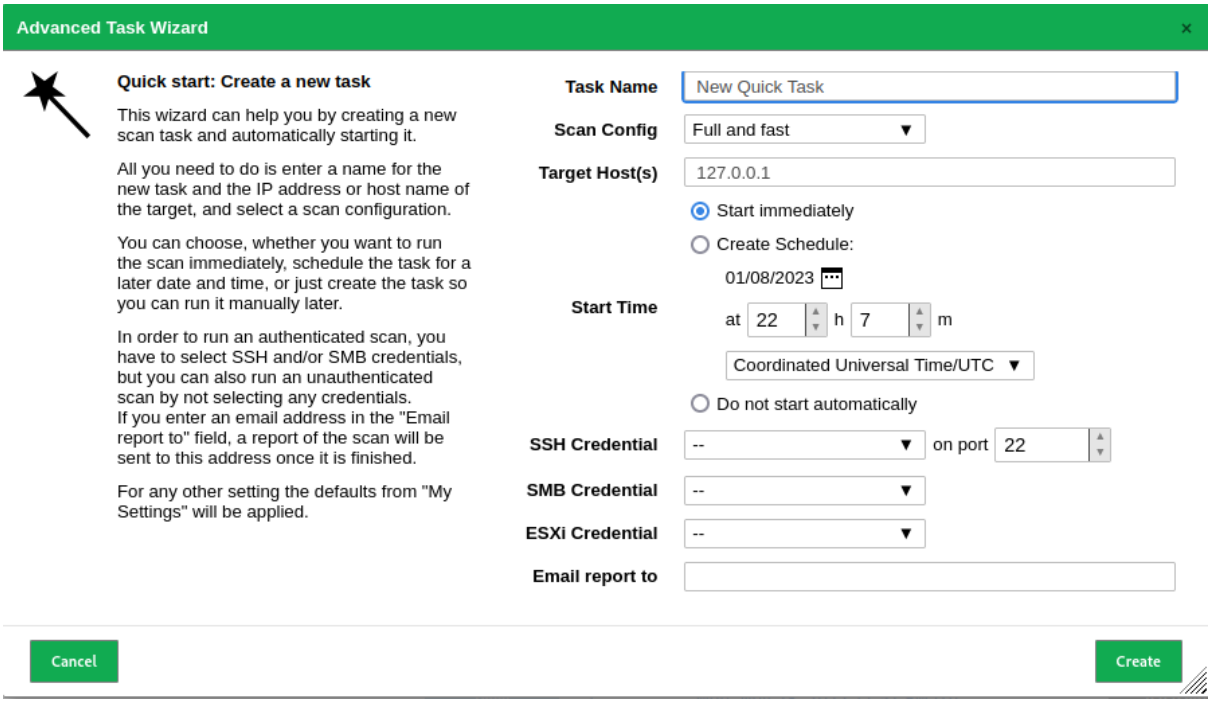


Figura 48 Creación de una tarea utilizando el Wizard de OpenVAS

Anexo 2

LISTADO DE ACTIVOS DEL ÁREA DE INGENIERÍA

A continuación se muestra en la Tabla 18 el listado de equipos informáticos seleccionados según la identificación de muestreo. El campo ID es el indicador con el cual el equipo fue seleccionado, quedando un estudio de 114 activos para este fin.

Tabla 18

Activos de muestreo del área de Ingeniería para transmisión aire

SECUENCIA	ID	DESCRIPCION	TIPO
1	1	FIREWALL IT	RED
2	2	ETHERNET MODEM, SISTEMA BRANDING INCLUYE CARGADOR ADAPTER, CARGADOR ZYPCOM	HARDWARE
3	5	SWITCH GIGABIT ETHERNET DE 24 PUERTOS	RED
4	6	SWITCH ADMINISTRABLE DE 24 PUERTOS CON RANGO DE FRECUENCIA DE 50/60HZ, GIGABIT ETHERNET MULTIMODE DE FIBRA OPTICA 500MHZ, AC POWER 127/200-240 VOLTS	RED
5	7	20 PORT FIBER CHANNEL SWITCH 5602Q (SB5602Q-8A)	RED
6	9	SWITCHER DE 24 PUERTOS	RED

SECUENCIA	ID	DESCRIPCION	TIPO
7	10	SWITCHER 8 PUERTOS	RED
8	11	SWITCHER SUPERSTACK 3	RED
9	12	SWITCHER DE 16 PUERTOS 2 CAPAS	RED
10	14	SWITCH 24PTOS. SUBREDES VIDEO	RED
11	15	SWITCH 48 PUERTOS	RED
12	16	SWITCH 48 PUERTOS	RED
13	17	SWITCHER 48PTOS. NOTICIAS	RED
14	18	SWITCHER 48PTOS. NOTICIAS	RED
15	20	CPU	HARDWARE
16	21	CPU	HARDWARE
17	22	EST. TRABAJO CONSISTE EN TARJETA INTEL S5000XVNSAS, CHASSIS INTEL SC5299WS, PROCESADOR DUAL-CORE INTEL 3GHZ 2X2MB,2 FULLY BUFFERED DIMM 1GB, HDD 320GB 16MB SATA2, TARJETA DE SONIDO Y VIDEO, DVD WRITER	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
18	23	CPU SCORPION "CLON”.	HARDWARE
19	25	PROCESADOR INTEL CORE I7 3.40GHZ, DISCO DURO WD SATA, DVD WRITER INTERNO SATA, CASE SUPER POWER 3340-A11 ATX 550W, MOTHER BOARD INTEL DH61WW, MEMORIA DDR3 1333, TECLADO, MOUSE GENIUS KMS	HARDWARE
20	26	DISCO DURO EXTERNO DE 60GB CON USB 2.0 ADICIONAL INCLUYE TARJETA DE MEMORIA PANASONIC P2 DE 8 GB, MODELO AJ-P2C008HG, SERIE ABD07A1415	HARDWARE
21	28	MODELO 14-AL007LA NOT 14"INTI 7/4GB/ITB/W10/DVD-DR/R. DUNN	HARDWARE
22	29	ZENBOOK UX301LA-XH72T 13.3 QUAD-HD DISPLAY	HARDWARE
23	30	ELITEBOOK 8440P NOTEBOOK PC (XV041LA) CON MEMORIA DE 4 GB	HARDWARE
24	31	ULTRABOOK Z835 CORE I5 6GB 128GB+MSE. HDF TOSHIBA SPA 13.3". CI5-2467	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
25	32	EDIT MACBOOK PRO	HARDWARE
26	33	GENERADOR GRAFICO MULTIKEYERS PARA USO EN BRANDING DE 160G MEMORIA RAM DE256MB, CAPACIDAD PARA REPRODUCIR VIDEOS, GYF, MOV, SALIDA FIL Y KID DIGITAL, SALIDA DE AUDIO DIGITAL	HARDWARE
27	34	GENERADOR GRAFICO MULTIKEYERS PARA USO EN BRANDING DE 160G MEMORIA RAM DE256MB, CAPACIDAD PARA REPRODUCIR VIDEOS, GYF, MOV, SALIDA FIL Y KID DIGITAL, SALIDA DE AUDIO DIGITAL	HARDWARE
28	35	GENERADOR GRAFICO MULTIKEYERS PARA USO EN BRANDING DE 160G MEMORIA RAM DE256MB, CAPACIDAD PARA REPRODUCIR VIDEOS, GYF, MOV, SALIDA FIL Y KID DIGITAL, SALIDA DE AUDIO DIGITAL	HARDWARE
29	36	BRANDING INTUITION TCR UIO	HARDWARE
30	37	BRANDING INTUITION-XG-3U-e	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
31	38	RF SWITCH PARA CAMBIAR LA POLIRIDAD DEL LNB PARA BANDA KU	RED
32	39	SWITCH CHANGEOVER CON 8 CANALES INPUT 110-120V 200-240V 50/60HZ INCLUYE FUENTE DE PODER SERIE 01945	RED
33	40	SWITCH CH_ OVER C. PICHINCHA	RED
34	41	SWITCH CH_ OVER UIO- C_PICHINCHA	RED
35	42	SWITCH CH_ OVER C. PICHINCHA	RED
36	43	GENERADOR GRAFICO MULTIKEYERS PARA USO EN BRANDING DE 160G MEMORIA RAM DE256MB, CAPACIDAD PARA REPRODUCIR VIDEOS, GYF, MOV, SALIDA FIL Y KID DIGITAL, SALIDA DE AUDIO DIGITAL	HARDWARE
37	44	GENERADOR GRAFICO MULTIKEYERS PARA USO EN BRANDING DE 160G MEMORIA RAM DE256MB, CAPACIDAD PARA REPRODUCIR VIDEOS, GYF, MOV, SALIDA FIL Y KID DIGITAL, SALIDA DE AUDIO DIGITAL	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
38	45	GENERADOR GRAFICO MULTIKEYERS PARA USO EN BRANDING DE 160G MEMORIA RAM DE256MB, CAPACIDAD PARA REPRODUCIR VIDEOS, GYF, MOV, SALIDA FIL Y KID DIGITAL, SALIDA DE AUDIO DIGITAL	HARDWARE
39	46	CASE ATX MAINBOARD INTEL DH61W. PROCESADOR INTEL CORE I3-2120 3.3GHZ. DISCO DURO DE 1TB SATA SEAGATE. MEMORIA DE 4GB DDR3. TARJETA DE VIDEO ZOGIS 1GB.	HARDWARE
40	47	CASE ATX. MAINBOARD INTEL DH61W. PROCESADOR INTEL DUAL CORE G630 2.7GHZ. DISCO DURO DE 500GB SATA SEAGATE.	HARDWARE
41	49	LAPTOP PARA SER USADA COMO EDITORA FINAL CUT	HARDWARE
42	50	MAC PRO (2.8GHZ PROCESADOR QUAD-CORE INTEL XEON NEHALEM/8GB (4X2GB) DDR3 ECC SDRAM/DISCO DURO DE 1TB 7200-RPM SERIAL ATA 3GB/S/TARJETA GRAFICA ATI RADEON HD 5770 DE 1GB GDDR5/SUPERDRIVE/BLUETOOTH 2	HARDWARE
43	53	SIST. ED. NO LINEAL APPLE: MAC PRO-DUAL 2.66GHZ DUAL-CORE INTEL XEON/1GB/250GB, MEMORIA RAM 1GB, SOFTWARE	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
		FINALCUT STUDIO 5.1, TARJETA DE RED DE FIBRE, TARJ. VIDEO BREAKOUT BOX, SOFTWARE DE TRANSCORDER	
44	55	EDITORA VELOCITY LINEAL EN TIEMPO REAL SOFTWARE VELOCITY Q VERSION 8.2, TARJETA VIDEO VELOCITY REALLITY QUATRUS BASADA EN UN PC IBM, DOBLE PROCEADOR XEON, RAM 1MB, HD AUDIO, DISCO EXTERNO 2 X 72GB	HARDWARE
45	58	EDITORA NEWSEDIT SC NO LINEAL SOFTWARE COSEC PARA DV25 (DV, DVCAM, DVCPRO) CON 2 HD SCSI 36 GB TARJETAS, RED ETHERNET 10/100 BT Y FIBRE CHENNEL 26B, INCLUYE MONITOR Y TECLADO	HARDWARE
46	60	EDITORA VELOCITY LINEAL EN TIEMPO REAL SOFTWARE VELOCITY Q VERSION 8.2, TARJETA VIDEO VELOCITY REALLITY QUATRUS BASADA EN UN PC IBM, DOBLE PROCEADOR XEON, RAM 1MB, HD AUDIO, DISCO EXTERNO 2 X 72GB	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
47	62	MAC PRO (2.8GHZ PROCESADOR QUAD-CORE INTEL XEON "NEHALEM"/3GB (4X2GB) DDR3 ECC SDRAM/DISCO DURO DE 1 TB 7200) TARJETA GRAFICA ATI RADEON HD 5770 DE 1GB	HARDWARE
48	63	Z440 WORKSTATION INTEL XEON E5-1603V3. SIX CORE 3.5GHZ, 15MB CACHE, DDR4-2133 MEMORY, 140W, HT, TURBOBOOST (3.8GHZ). 16GB (2X8GB), MX. 128GB DDR4-2133 REG RAM. 1TB SATA 6GB/S 72200	HARDWARE
49	64	Z230 WORKSTATION SFF SMART BUY INTEL CORE I5-4690 QUAD CORE (3.50GHZ 6MB) AMD FIREPRO W2100 (2GB) GRAPHICS 8GB (2X4GB) DDR3 1600MHZ NECC 1TB DVD-RW W7 PRO 64BITS	HARDWARE
50	65	Z230 WORKSTATION SFF SMART BUY INTEL CORE I5-4690 QUAD CORE (3.50GHZ 6MB) AMD FIREPRO W2100 (2GB) GRAPHICS 8GB (2X4GB) DDR3 1600MHZ NECC 1TB DVD-RW W7 PRO 64BITS	HARDWARE
51	66	Z230 WORKSTATION SFF SMART BUY INTEL CORE I5-4690 QUAD CORE (3.50GHZ 6MB) AMD FIREPRO W2100 (2GB) GRAPHICS 8GB (2X4GB) DDR3 1600MHZ NECC 1TB DVD-RW W7 PRO 64BITS	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
52	67	Z230 WORKSTATION SFF SMART BUY INTEL CORE I5-4690 QUAD CORE (3.50GHZ 6MB) AMD FIREPRO W2100 (2GB) GRAPHICS 8GB (2X4GB) DDR3 1600MHZ NECC 1TB DVD-RW W7 PRO 64BITS	HARDWARE
53	69	Z230 WORKSTATION SFF SMART BUY INTEL CORE I5-4690 QUAD CORE (3.50GHZ 6MB) AMD FIREPRO W2100 (2GB) GRAPHICS 8GB (2X4GB) DDR3 1600MHZ NECC 1TB DVD-RW W7 PRO 64BITS	HARDWARE
54	70	Z230 WORKSTATION SFF SMART BUY INTEL CORE I5-4690 QUAD CORE (3.50GHZ 6MB) AMD FIREPRO W2100 (2GB) GRAPHICS 8GB (2X4GB) DDR3 1600MHZ NECC 1TB DVD-RW W7 PRO 64BITS	HARDWARE
55	71	Z230 WORKSTATION SFF SMART BUY INTEL CORE I5-4690 QUAD CORE (3.50GHZ 6MB) AMD FIREPRO W2100 (2GB) GRAPHICS 8GB (2X4GB) DDR3 1600MHZ NECC 1TB DVD-RW W7 PRO 64BITS	HARDWARE
56	72	Z230 WORKSTATION SFF SMART BUY INTEL CORE I5-4690 QUAD CORE (3.50GHZ 6MB) AMD FIREPRO W2100 (2GB) GRAPHICS 8GB (2X4GB) DDR3 1600MHZ NECC 1TB DVD-RW W7 PRO 64BITS	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
57	74	Z840 WORKSTATION. INTEL XEON E5-2630 V3 8-CORE (2.40GHZ 20 MB) NVIDIA QUADRO K4200 (4GB) GRAPHICS 16GB. DDR4 2133MHZ. DVD-RW W8.1 PRO 64BITS	HARDWARE
58	75	Z840 WORKSTATION. INTEL XEON E5-2630 V3 8-CORE (2.40GHZ 20 MB) NVIDIA QUADRO K4200 (4GB) GRAPHICS 16GB. DDR4 2133MHZ. DVD-RW W8.1 PRO 64BITS	HARDWARE
59	76	EDIT. MACPRO DISEÑ#O GRAF.	HARDWARE
60	77	EDITORA MAC PRO EDIT. #9	HARDWARE
61	78	REVISORA CONTENIDOS EN BAJA RESOLUCIÓN 2	HARDWARE
62	79	REVISORA DE CONTENIDOS EN BAJA RESOLUCIÓN 1	HARDWARE
63	80	REVISORA DE CONTENIDOS EN BAJA RESOLUCIÓN 5	HARDWARE
64	81	SAN STORAGE EXPANSION_1 NOT	HARDWARE
65	82	SAN STORAGE EXPANSION_2 NOT	HARDWARE
66	84	SAN STORAGE PRINCIPAL NOT	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
67	85	NAS DE PRODUCCIÓN, SERVIDOR CON TARJETA INTEL XEON 2 GHZ DUAL CORE 5503 CON ALMACENAMIENTO DE 16 DISCOS DUROS DE 2TB SEAGATE.	HARDWARE/INFORMACIÓN
68	86	NAS SERVER DE CONTENIDOS CON CAPACIDAD 1.5TB INCLUYE LTO (MEDIA ARCHIVE LIBRARY)	HARDWARE/INFORMACIÓN
69	88	ARREGLO PARA RED DE ALMACENAMIENTO 1	HARDWARE/INFORMACIÓN
70	90	NAS TOLEDO TCR	HARDWARE/INFORMACIÓN
71	91	COMPUTADOR CORE 2 QUAD MAINBOARD DG41 INCLUYE 2 TARJETASDE RED 10/100/1000, DISCO DURO 500GB & 2TB, MEMORIA 3GB, UNIDAD DVD	HARDWARE
72	92	CPU INTEL CORE 2 DUO 2.8GHZ, CASE TIPO TORRE, MAINBOARD INTEL DG35EC, MEMORIA 4GB DDR2,1 DISCO DURO 320GB ATA, DVD-RW, LECTOR DE TARJETAS INCLUYE LICENCIA WINDOWS XP PRO-OEM	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
73	93	CPU INTEL CORE 2 DUO 2.66GHZ, MAINBOARD INTEL DG31PR, DISCO DURO SAMSUNG 160GB SATA, MEMORIA 2GB DDR2 800, DVD WRITER, FUENTE DE PODER 500W	HARDWARE
74	95	KVM EXTENDER SERV. COMERCIALES KUM-EXTENDER SERV. COMERCIALES.TRIP-LITTE, CREMA, CARGADOR.AC ADAPTADOR.OEM	HARDWARE
75	96	INGESTA DE COMERCIALES, PROGRAMACION Y PROMOCIONES USANDO SOFTWARE DE HARDATA HDX VIDEO OFFICEE INSTALADO EN PC Q INCLUYE: MICROPROCESADOR CORE I7 2,93GHZ, MEMORIA 2GB DDR3, DISCO DURO 1,5TERAS SATA,	HARDWARE/SOFTWARE
76	97	NEWS BROWSE SEQUENTIAL ENCODER PARA BAJA RESOLUCIÓN	HARDWARE
77	98	SISTEMA PLAYOUT PARA PROFILE CON CONTROL DE HASTA 6 CANALES INDEPENDIENTES O 4 ESPEJOS CON MOUSE Y TECLADO	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
78	99	INCEPTION SYSTEM BUNDLE SINGLE SERVER INCLUYE: SOFTWARE Y HARDWARE. PLUG IN-PLAYLIST, ADDITIONAL USER, POLLS Y XPRESSION CONNECT.	HARDWARE
79	100	SERVIDOR DE VIDEO	HARDWARE/INFORMACIÓN
80	101	NEWS BROWSE SERVER FOR NEW SEDIT SESSION LICENCE CON FLAT PANEL VGA 15" Y TECLADO MARCA DELL Y SELETOR CON 8. NOMBRE CORTO (WEB/DA	HARDWARE/INFORMACIÓN
81	102	SERVIDOR BASADO EN PC PROCESADOR INTEL XEON E5630 2.53GHZ,8GB MEMORIA (4X2GB),2 DISCOS DUROS SATA 250GB INCLUYE LICENCIA WINDOWS STORENEXT 2.0 Y ADAPTADOR DELL SINGLE CHANNEL ULTRA 320 SCSI PCIE	HARDWARE/INFORMACIÓN
82	103	SERVIDOR DE VIDEO PARA COMERCIALES Y PROGRAMACIÓN CON CAPACIDAD 70H DE GRABACIÓN DV25 DE 146GB	HARDWARE/INFORMACIÓN
83	105	APLICATIVO PARA TRANSFERENCIA DE CONTENIDO	SOFTWARE
84	106	DE 4 CANALES DE GRABACION Y 1 CANAL DE REPRODUCCION. 40 HORAS DE ALMACENAMIENTO EN HD	INFORMACION

SECUENCIA	ID	DESCRIPCION	TIPO
85	107	FAZZT UPLOAD/DOWNLOAD MANAGER, IP INPUT. 2U, DUAL 1TB HDD CONFIGURED WITH RAID, DUAL NICS, ADDITIONAL DUAL NIC INTERFACE.	HARDWARE/SOFTWARE
86	109	CLIENTE SERVIDOR K2 (PC WINDOWS XP MONTAJE EN BASTIDOR) CON 4CH BIDIRECCIONALES DE VIDEO INCLUYE: LICENCIA DE SOFTWARE SNMP PARA CLIENTE SERVIDOR Y SERVIDOR DE MEDIA K2 CON PURTO USB	HARDWARE/SOFTWARE
87	110	SERVIDOR DE CONVERSIÓN DE VIDEO DE BAJA A ALTA RESOLUCIÓN PARA PROFILE CON MOUSE Y TECLADO MARCA DELL INCLUYE RACKMOUNTING S/N GFRBY41.	HARDWARE
88	111	NEXIO AMP 3RU shared storage video server. 3 channel SD/HD, 4 input and 4 output SDI/HD-SDI interface card. INCLUYE: USB powered House Timecode Input to NEXIO, Ethernet switch for Media Host & VLAN	HARDWARE/SOFTWARE
89	112	SERVIDOR	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
90	113	SERVIDOR DE THUMBNAIL Y CREACION DE STORY BAORD PARA SISTEMA DE EDICION NEWSTROWSE (DA) (N. CORT.CLIPS SERVER)	HARDWARE
91	114	NEXIO AMP 3RU shared storage video server. 3 channel SD/HD, 4 input and 4 output SDI/HD-SDI interface card. INCLUYE: USB powered House Timecode Input to NEXIO, Ethernet switch for Media Host & VLAN	HARDWARE/SOFTWARE
92	115	NEW BROWSE ENCODER PARA BAJA RESOLUCIÓN 1 CH.	HARDWARE
93	116	MODELO: FUSION D800TBR5 16TB. 8 DRIVE RAID 5 DESKTOP STORAGE SYSTEM. SAS BOARD PCI EXPRESS, MODELO: ESAS-H680, MARCA: ATTO. LTO5 EXTERNAL DRIVE, MODELO: EH958A, MARCA: HP	HARDWARE
94	117	SIST. /ALMACENAMIENTO REDUNDANTE K2 NIVEL 10. INCLUYE 2 SERVID. DE MEDIA K2 (PC WINDOWS XP MONTAJE EN BASTIDOR), UNA BANDEJA EXTERNA PARA MONTAJE DE DISCOS CON 2 CONTROLADORES RAID Y 2 FUENTES DE PODER	HARDWARE/INFORMACIÓN
95	121	CONTROLADOR DE PB PRODUCCIÓN	HARDWARE/INFORMACIÓN

SECUENCIA	ID	DESCRIPCION	TIPO
96	122	EDIT. MACPRO EDIT. #12	HARDWARE
97	127	METADATA CONTROLLER BACKUP SERVER	HARDWARE
98	128	METADATA CONTROLLER SERVER	HARDWARE/INFORMACIÓN
99	130	MONITOREO DE CONTENIDOS	HARDWARE/INFORMACIÓN
100	132	ORGANIZADOR DE CONTENIDOS	HARDWARE
101	133	PLAYOUT SERVER MASTER 1	HARDWARE
102	140	SERV. INGESTA 2CH NOT_1	HARDWARE
103	141	SERV. INGESTA 2CH NOT_2	HARDWARE
104	143	SERV. PROXY ENCODER NOTICIAS	HARDWARE
105	144	SERV. DE VIDEO UIO	HARDWARE/INFORMACIÓN
106	148	SERVIDOR DE ARCHIVO 2	HARDWARE/INFORMACIÓN
107	151	SERVIDOR PLAYBACK K2 TCR UIO	HARDWARE/INFORMACIÓN

SECUENCIA	ID	DESCRIPCION	TIPO
108	153	SWITCH FIBRA RED DE EDIC. #1 CTO. RACK	RED
109	155	SWITCH 48PTOS. XSAN CTO. RACK EQP	RED
110	156	SWITCH 48PTOS.PRIVATE CTO. RACK EQP	RED
111	158	CPU INTEL CORE 2 QUAD 2.66GHZ Q9400, MAINBOARD INTEL DG35EG, DVD WRITER, FUENTE DE PODER 500W, LECTOR DE MEMORIAS, TARJETA DE VIDEO 1GB NVIDIA GFORCE 9400GT,2 DISCO DUROS SATA 250GB,2 MEMORIAS 2GB DDR2.	HARDWARE
112	159	CPU PARA PROGRAMA. APPCENTER Q' MANEJA EL PLAYLIST DEL SERVIDOR K2, INCLUYE: MAINBOARD INTEL 945GCNL, MICROPROCESADOR. INTEL CORE 2DUO 2.2GHZ, MEMORIA RAM 2GB, DISCO DURO 250GB, TARJETA/VIDEO 256MB	HARDWARE
113	160	HELM PENTIUM 4 DE 3.07 MEMORIA DE 1GB DISCO DURO 160GB TARJETA GRAFICA 256MB,	HARDWARE
114	163	ADMINISTRADOR DE ENCODER INCLUYE XMU BASADO EN UN PC HPHARDWARD Y SOFTWARE NUMERO N360C000AAM, XMS	HARDWARE

SECUENCIA	ID	DESCRIPCION	TIPO
		SISTEMA ADICIONAL DE ADMINISTRADOR N360SCL3AA LICENCIA DE EDICION SIMPLE N3500201AA	

Anexo 3

LISTADO DE NÚMEROS ALEATORIOS PARA LA MUESTRA DE EQUIPOS

En el uso de la herramienta STATS se generan números aleatorios con el rango de ID de equipos, en la Tabla 19 se lista la generación de los números generados por dicha herramienta para toma de la muestra de hosts.

Tabla 19

Generación de números de aleatorios de la Muestra

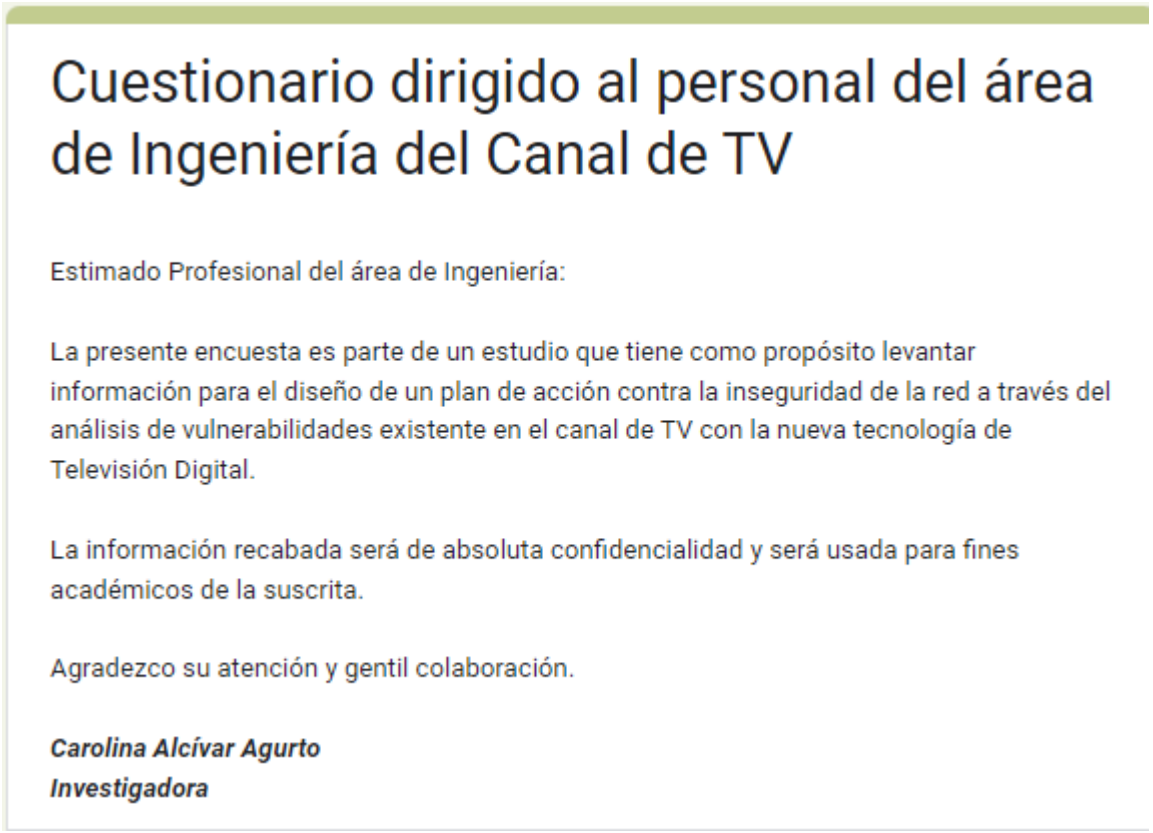
NÚMERO ALEATORIOS DE ID EN ACTIVOS							
1	21	38	60	78	97	114	148
2	22	39	62	79	98	115	151
5	23	40	63	80	99	116	153
6	25	41	64	81	100	117	155
7	26	42	65	82	101	121	156
9	28	43	66	84	102	122	158
10	29	44	67	85	103	127	159
11	30	45	69	86	105	128	160
12	31	46	70	88	106	130	163
14	32	47	71	90	107	132	
15	33	49	72	91	109	133	
16	34	50	74	92	110	140	
17	35	53	75	93	111	141	
18	36	55	76	95	112	143	
20	37	58	77	96	113	144	

Anexo 4

Instrumento aplicado al personal.

Encuesta dirigida al personal de Ingeniería del canal de televisión

La presente encuesta es parte de un estudio que tiene como propósito levantar información para el diseño de un plan de acción contra la inseguridad de la red a través del análisis de vulnerabilidades existentes en el canal de TV con la nueva tecnología de Televisión Digital



Cuestionario dirigido al personal del área de Ingeniería del Canal de TV

Estimado Profesional del área de Ingeniería:

La presente encuesta es parte de un estudio que tiene como propósito levantar información para el diseño de un plan de acción contra la inseguridad de la red a través del análisis de vulnerabilidades existente en el canal de TV con la nueva tecnología de Televisión Digital.

La información recabada será de absoluta confidencialidad y será usada para fines académicos de la suscrita.

Agradezco su atención y gentil colaboración.

Carolina Alcívar Agurto
Investigadora

¿Existen seguridad perimetral? *

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Está la Alta Gerencia involucrada en la gestión y procedimientos de seguridad de la Información? *

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Existen procedimientos para continuidad de negocio?

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Existen servicios de archivos compartidos con políticas acceso de Directorio Activo u otro control de acceso? *

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿La información entre los enlaces viaja de forma encriptada o cifrada? *

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Existe un sistema de registro de incidentes?

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Se tienen herramientas para controlar posibles amenazas en la seguridad de la información? *

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Están los activos debidamente etiquetados? *

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Tiene la empresa un Sistema de Gestión de la Seguridad de la Información (SGSI)? *

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Existe monitoreo de las actividades de los enlaces de Transmisión en TV? *

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Tienen un listado de los activos de Información del área de Ingeniería? *

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Existen políticas de respaldo de la información?, ¿Qué tipo de respaldo?

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Existen políticas de Seguridad de la Información? *

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Las aplicaciones y desarrollos implementados se cuentan con procesos de seguridad? *

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

¿Existen dispositivos móviles o equipos en ambientes remotos? *

- ◯ Muy de acuerdo
- ◯ De acuerdo
- ◯ Ni de acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ Muy en desacuerdo

Enviar Página 1 de 1 Borrar formulario

Anexo 5

Alerta de incidentes de ECUCERT.

Los incidentes que reporta el ECUCERT están clasificados como ALERTAS DE SEGURIDAD debidamente identificadas con su respectivo CVE. La Tabla 20 detalla este tipo de clasificación que es actualizado según los tiempos que defina el ECUCERT

Tabla 20.

Listado de Alertas de Seguridad identificadas por ECUCERT

CENTRO DE RESPUESTA A INCIDENTES INFORMATICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**		
ID de CVE	Descripción	Fecha límite del parche
CVE-2021-36934	Vulnerabilidad de escalada de privilegios locales SAM de Microsoft Windows	2/24/2022
CVE-2020-0796	Vulnerabilidad de ejecución remota de código de Microsoft SMBv3	8/10/2022
CVE-2018-1000861	Jenkins Stapler Web Framework Deserialización de datos no confiables	8/10/2022
CVE-2017-9791	Vulnerabilidad de validación de entrada incorrecta de Apache Struts 1	8/10/2022
CVE-2017-8464	Ejecución remota de código de Microsoft Windows Shell (.lnk)	8/10/2022
CVE-2017-10271	Oracle Corporation WebLogic Server Ejecución remota de código	8/10/2022
CVE-2017-0263	Vulnerabilidad de escalada de privilegios de Microsoft Win32k	8/10/2022
CVE-2017-0262	Vulnerabilidad de ejecución remota de código de Microsoft Office	8/10/2022

CVE-2017-0145	Vulnerabilidad de ejecución remota de código de Microsoft SMBv1	8/10/2022
CVE-2017-0144	Vulnerabilidad de ejecución remota de código de Microsoft SMBv1	8/10/2022
CVE-2016-3088	Vulnerabilidad de validación de entrada incorrecta de Apache ActiveMQ	8/10/2022
CVE-2015-2051	Ejecución remota de código del enrutador D-Link DIR-645	8/10/2022
CVE-2015-1635	Vulnerabilidad de ejecución remota de código de Microsoft HTTP –sys	8/10/2022
CVE-2015-1130	Vulnerabilidad de omisión de autenticación de Apple OS X	8/10/2022
CVE-2014-4404	Vulnerabilidad de desbordamiento de búfer basado en almacenamiento dinámico de Apple OS X	8/10/2022