Institución Universitaria

Metodología de detección de intrusos para radios que utilizan protocolo radio móvil digital (DMR), que permitirá identificar ataques de denegación de servicios que afectan la disponibilidad en la transmisión de datos para empresas de seguridad privada.

Sergio Andrés Álvarez Gaviria
Oscar David Urrea Ernotte

Instituto Tecnológico Metropolitano
Facultad de ingenierías
Medellín, Colombia
2019

Metodología de detección de intrusos para radios que utilizan protocolo radio móvil digital (DMR), que permitirá identificar ataques de denegación de servicios que afectan la disponibilidad en la transmisión de datos para empresas de seguridad privada.

Sergio Andrés Álvarez Gaviria
Oscar David Urrea Ernotte

Tesis o trabajo de investigación presentado como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director:
Msc. Andrés Felipe Ramírez Barrera
Codirector:
Msc. Leonel Marín Ramírez

Línea de Investigación:
Ciencias Ingenieriles Biomédicas
Grupo de Investigación:
Investigación e innovación biomédica

Línea de Investigación
Ciencias Computacionales
Grupo de Investigación
Automática, Electrónica y Ciencias Computaciones

Instituto Tecnológico Metropolitano
Facultad de ingenierías
Medellín, Colombia
2019

Esta tesis está dedicada:

A toda la comunidad universitaria del país, en pro de fortalecer el área del conocimiento y así lograr demostrar que nuestra sociedad desde las aulas; puede lograr grandes contribuciones en el área técnica y tecnológica.

Agradecimientos

Aprovechamos este espacio para agradecer a la institución, a toda la cadena de recursos que hacen posible el desarrollo de la maestría, destacando entre ellos: Profesorado, directores y compañeros de curso. Sus acertados comentarios ayudaron y fomentaron el desarrollo del presente trabajo, a ellos muchísimas gracias.

Resumen

En los diferentes sectores empresariales tanto privados como públicos se deben escoger plataformas de comunicación que soporten las necesidades del medio, no sin antes priorizar y evaluar variables de suma relevancia en la parte técnica, gerencial y económica. Factores tales como el costo, respaldo de marca, disponibilidad del servicio y monitoreo se vuelven fundamentales a la hora de escoger la plataforma de comunicación. Luego de ser evaluadas estas variables en algunos casos son elegidas las tecnologías análogas ya que tienen ventajas de disponibilidad para el uso en infraestructuras críticas o son usadas en forma común las tecnologías más propagadas u económicas como la telefonía celular GSM, sin considerar que estas últimas pueden colapsar ante eventos naturales o incidentes por saturación. Específicamente los sectores críticos de seguridad privada y pública se apropian de las tecnologías análogas por radio frecuencia conocidas como las comunicaciones por RF; las cuales tienen un índice muy alto de consumo e implementación en el mercado por la alta disponibilidad que ofrecen sobre diferentes agentes externos adversos. Cabe decir que este tipo de tecnologías están limitadas (en la mayoría de los casos) a solo recibir y entregar mensajes de voz. Dentro de la tecnología RF existen muchos estándares los cuales vienen tomando fuerza para los radios digitales que son tendencia en la actualidad y que permiten soportar gran cantidad de servicios adicionales que aumentan la productividad, divididos en una capa de voz y otra capa de datos sobre la misma infraestructura y transmitidas por una sola cadena de conexión. Uno de los estándares que toma importancia y toma los principios mencionados es el protocolo Radio Móvil Digital DMR, diseñado por la ETSI en 2005. Las comunicaciones por DMR admiten el envío de datos heredando las vulnerabilidades conocidas del espacio radioeléctrico y de TCP/IP que pueden ser atacados, vulnerados y explotados afectando la disponibilidad de estos servicios complementarios. La investigación está estructurada por capítulos, primero se abordará el contexto de la tesis, luego el estado del arte, seguidamente un marco teórico, luego la caracterización de servicios y tecnologías implicadas dentro del protocolo, después se realizará un análisis de riesgos sobre los servicios/tecnologías previamente listadas y por último se expondrá la metodología orientada a la detección de DoS sobre comunicaciones DMR. Siguiendo los pasos

de la metodología se podrá detectar intrusos y tratar ataques tipo DoS que afecten la disponibilidad dentro de la cadena de conexión del protocolo DMR.

Palabras clave: DMR, DoS, detección de intrusos, disponibilidad dato, IDS

Abstract

In the different business sectors, both private and public, communication platforms must be chosen that support the needs of the medium, but not before prioritizing and evaluating highly relevant variables in the technical, managerial and economic areas. Factors such as cost, brand support, service availability and monitoring become fundamental when choosing the communication platform. After evaluating these variables, in some cases analogous technologies are chosen because they have availability advantages for use in critical infrastructures or the most widespread or economic technologies such as GSM cellular telephony are used in common, without considering that the latter can collapse before natural events or saturation incidents. Specifically, the critical sectors of private and public security appropriate the analogous radio frequency technologies known as RF communications; which have a very high rate of consumption and implementation in the market due to the high availability they offer on different adverse external agents. It should be noted that this type of technology is limited (in most cases) to only receive and deliver voice messages. Within RF technology there are many standards which are gaining strength for digital radios that are currently trending and that allow to support a large number of additional services that increase productivity, divided into a layer of voice and another layer of data on the same infrastructure and transmitted by a single connection string. One of the standards that takes importance and takes the mentioned principles is the Mobile Digital DMR protocol, designed by the ETSI in 2005. The DMR communications support the sending of data inheriting the known vulnerabilities of the radioelectric space and TCP / IP that can be attacked, violated and exploited affecting the availability of these complementary services. The research is structured by chapters, first the context of the thesis will be addressed, then the state of the art, then a theoretical framework, then the characterization of services and technologies involved in the protocol, then a risk analysis will be performed on the services / previously listed technologies and finally the methodology aimed at detecting DoS over DMR communications. Following the steps of the methodology, it will be possible to detect intruders and to deal with DoS attacks that affect availability within the DMR protocol connection chain.

Keywords: DMR, DoS, intrusion detection, data availability, IDS

Contenido

Pág.

Lista de figuras

Pág.

Lista de tablas

Pág.

Lista de Símbolos y abreviaturas

Abreviaturas

Abreviatura	Término
SLOT	*Ranura de expansión*
SCADA	*Software de control en procesos industriales*
IDS	*Sistema de detección de intrusos*
CAPEX	*Gasto de una empresa en bienes*
IPS	*Sistema de prevención de intrusos*
BD	*Base de datos*
GNU	*Comunidad de sistemas operativos libres*
DMR	*Radio móvil digital*
DLL	*Biblioteca de enlace dinámico*
DoS	*Denegación de servicios*
OTA	*Programación por aire*
UDP	*Protocolo de datagramas*
IPv4	*Protocolo de internet versión 4*
PDP	*Protocolo de trasferencias de datos*
RAW	*Formato de imágenes en crudo*
RF	*Radio frecuencia*
ETSI	*Instituto europeo de normas de telecomunicaciones*

OSI	*Modelo de interconexión de sistemas abiertos*
CSAE	*Consejo superior de administración electrónica*
MAP	*Ministerio de administraciones públicas*
IDS	*Sistema de detección de intrusos*
VHF	*Banda del espectro electromagnético frecuencias de 30MHz a 300MHz*
UHF	*Banda del espectro electromagnético frecuencias de 300MHz a 3GHz*
SIRDEE	*Sistema de radiocomunicaciones digitales de emergencia del estado*
TETRAPOL	*Estándar de radiocomunicaciones digitales profesional*
TETRA	*Empresa de fabricación de equipos de telecomunicaciones*
OSINT	*Inteligencia de fuentes abiertas*
WLAN	*Red de área local inalámbrica*
GPS	*Sistema de geoposicionamiento global*
SMS	*Servicios de mensajes cortos*
SCOPUS	*Base de datos bibliográficas digitales*
TDMA	*Acceso múltiple por división de tiempo*
SMURF	*Ataque pitufo tipo Dos*
ICMP	*Protocolo de control de mensajes de Internet*
IP	*Número de identificación única de red*
SYN	*Solicitud de conexión*
ACK	*Validación de una conexión*
BGP	*Protocolo de puerta de enlace*

SNIFFER	*Software analizador de paquetes*
SDR	*Radio definida por software*
UIT	*Unión internacional de telecomunicaciones*
TCP/IP	*Familia de protocolos de internet*
NIDS	*Sistema de detección de intrusos de red*
HIDS	*Sistema de detección de intrusos de host*
HOST	*Dispositivo de red*
TIER	*Nivel*
CODEPLUG	*Firmware de radios DMR*
AES	*Estándar avanzado de cifrado*
DPI	*Inspección profunda de paquetes*
ROOTKITS	*Aplicación para escalar privilegios en un sistema*
OSSEC	*Sistema gratuito de detección de intrusos basado en host*
OSSIM	*Sistema gratuito para detección y prevención de intrusos de red*
DDoS	*Denegación de servicios distribuido*
KHz	*Kilo, unidad de frecuencia*
MHz	*Kilo, unidad de frecuencia*
SYSLOG	*Estándar para enviar mensajes de registro de red*
MULTICAST	*Multidifusión*

Introducción

Las comunicaciones en los diferentes sectores industriales se vuelven fundamentales para ejecutar labores rutinarias, acortar distancias y aumentar la productividad. En la actualidad existen diferentes medios de trasmisión que permiten la comunicación que de alguna manera cumplen con las exigencias mínimas requeridas. En muchos casos estas comunicaciones no soportan a cabalidad las necesidades reales de la industria. Estas necesidades en escenarios normales pueden ser acotadas a los siguientes pilares: la disponibilidad, la confidencialidad e integridad. Esta caracterización de pilares debería ser valorada antes de tomar una decisión sobre que tecnologías soportaran las comunicaciones de las industrias. Apadrinar una tecnología de comunicación es una tarea confusa, costosa y abstracta; pero a la vez prioritaria y relevante. En los sectores primarios de la industria que se enfocan en la seguridad física: policía, bomberos, ejercito, defensa civil y vigilancia privada se ha notado que han apadrinado las tecnologías por radio frecuencia RF por que ofrecen alta disponibilidad y mayor alcance. En el mercado existen diferentes estándares de comunicación por radio frecuencia RF tanto en tecnologías análogas como digitales. Las análogas son implementadas en sectores prioritarios, pero subutilizando el medio de trasmisión (el espectro). Es acá donde cobra importancia tener comunicaciones por radio frecuencia que permitan explotar el uso de los canales de comunicación para ampliar el abanico de servicios y aplicaciones. Una de las tecnologías que da la aplicabilidad de combinar voz y datos es DMR. Estándar desarrollado por la ETSI que viene cogiendo fuerza en los sectores primarios industriales en la región europea y viene ampliando campo en la industria latinoamericana. El protocolo DMR está dividido en dos mundos: voz y datos. Este documento ahondara en explicar cómo se puede mitigar la denegación de servicios DoS para tratar de evitar una interrupción del estándar DMR enfocado a la disponibilidad del servicio. La parte de voz en el estándar DMR esta soportada por tecnologías tradicionales análogas, aprovechando lo establecido en la cadena de conexión tradicional y aumentando los servicios de datos (parte digital) sobre la misma cadena de conexión. Esto permite a DMR soportar datos y voz por medio de dos ranuras SLOTS en las repetidoras una para voz y otra para datos, para así no solo tener comunicaciones por voz en la radio frecuencia, si no también servicios de datos en los que se destacan: ubicación por GPS, botones de pánico, mensajes tipo SMS, monitoreo desde

una central, respaldo de mensajes de voz, entre otros. En este documento se propone escribir una metodología para detectar intrusos en la cadena de conexión del estándar DMR y que pueda afectar la disponibilidad del servicio enfocado a prevenir un ataque tipo DoS en la capa de datos del protocolo.

1.Capítulo 1: Contexto de la tesis

Este capítulo se orientó hacia la importancia que tiene para el desarrollo de la tesis; los posibles fallos de seguridad en las comunicaciones con tecnologías RF (Ramos, 2015) derivando en la problemática específica del protocolo DMR (Blanco, 2016), orientado a la capa de datos.

1.1 Planteamiento del problema

La industria bajo la necesidad de tener comunicaciones eficientes y por sus procesos misionales, ven la opción de soportar sus comunicaciones aprovechando el espacio radioeléctrico con las comunicaciones de tipo RF implementadas en redes sensibles, criticas y prioritarias. En muchos ámbitos tecnológicos, soportar las comunicaciones por RF es garantía de alta disponibilidad y eficacia (Ramos, 2015) por lo que actualmente y con el desarrollo de tecnologías de comunicación, el aprovechamiento del RF ha evolucionado en forma acelerada y no ha perdido importancia al ser usado por sectores públicos y privados como la defensa civil, policía, ejercito, vigilancia privada, cruz roja, entre otros (DMR Movil Association, 2019).

Al mismo tiempo, las empresas de diferentes sectores necesitan acceso al espectro para satisfacer las crecientes demandas de sus redes, en donde también deben aumentar la seguridad de su infraestructura ante amenazas físicas y de seguridad cibernética. Hoy en día, los activos críticos de servicios públicos están cada vez más interconectados entre sí y son cada vez más sofisticados y coordinados, incluidos los ataques cibernéticos. Si bien es imposible evitar en su totalidad que ocurran ataques, los riesgos se pueden mitigar a través de herramientas técnicas y soluciones basadas en procesos, que incluyen mejorar la confiabilidad y la capacidad de recuperación de las redes de comunicaciones subyacentes que admiten aplicaciones de datos.

En el caso específico del estándar DMR muy usado en la unión europea y que se viene desplegando por Latinoamérica por su bajo coste y reutilización de las comunicaciones tradicionales (DMR Association, 2019), se observa una creciente evolución al permitir la adición de funcionalidades como mensajes de texto, GPS, telemetría y alertas de estado

en una capa de datos que convive con tecnologías y protocolos ya conocidos como TCP/IP o UDP que poseen vulnerabilidades; lo cual manifiesta una amenaza en situaciones extremas de servicio como: eventos públicos, desastres naturales, atentados terroristas, desórdenes públicos, guerras y epidemias en donde la disponibilidad de las radiocomunicaciones es fundamental (DMR Association, 2017).

Dado lo anterior el uso de las comunicaciones DMR, apoya en gran medida la gestión operativa de las organizaciones usando servicios adicionales de datos que permiten responder ante eventos o maximizar la gestión de las personas mediante el uso de indicadores que proporcionan los datos recibidos. Pero se encuentra que en la actualidad no se cuenta con estrategias de detección de intrusiones para este tipo de comunicaciones que permitan alertar sobre posibles intrusiones o ataques que pueden afectar el real potencial del estándar al enviar paquetes de datos por una cadena de conexión. Esto aumenta la importancia que deben tener estrategias de control como la detección de intrusos en estas comunicaciones ante los ataques informáticos y en especial a la denegación de servicio DoS. (Ramos, 2015).

1.2 Antecedentes y justificación.

En años anteriores interceptar comunicaciones por RF era relativamente fácil, bastaba con tener un receptor tipo escáner VHF/UHF (Ramos, 2015) y con solo ajustar unos rangos de frecuencia se podían interceptar comunicaciones de la policía. Por ejemplo, en España la protección de estas comunicaciones no ha variado sustancialmente y las comunicaciones criticas pasaron a soportarse por la SIRDEE (Baldini, 2010) que usa el estándar TETRAPOL (Tetrapol Forum, 2018) que hasta el momento han dado respuestas positivas. En muchos casos las entidades gubernamentales que tienen comunicaciones criticas están haciendo uso de bandas abiertas a bajo costo y que son de radio frecuencias digitales, entre ellas: DMR y TETRA. Hacer una recopilación de información con técnicas como OSINT y aplicadas al Google Hacking se pueden obtener datos sensibles públicos referentes a las comunicaciones criticas validando las frecuencias normalmente usadas. Así un atacante podrá tener la información suficiente para usar un frecuencímetro oculto y así acceder a la RF objetivo para realizar un ataque tipo “off-line” síntoma básico de un ataque tipo DoS. En DMR existen varios mecanismos de seguridad con algunas diferencias entre fabricantes, pero se han detectado fallos que permiten ataques de fuerza bruta, previniéndose en si con cifrados tipo AES o controles de acceso con RAS para evitar intrusos en la red. Otro de los casos relevantes son hallazgos en vulnerabilidades en el firmware de fabricantes en algunos modelos de radio móviles. Un atacante si logra ingresar a la red podrá hacer operaciones tipo OTA que pueden desactivar ciertos terminales. Otra técnica efectiva es la clonación de terminales DMR con los parámetros de red mínimos con información obtenida en un SDR. Otra técnica muy efectiva es el radio Jamming (Kumar, 2017); La técnica Jamming en realidad son interferencias intencionadas para la bifurcación de la radio señal con el fin de colapsar o tumbar la red de radio frecuencia, esta técnica es sencilla de aplicar, pero difíciles de mitigar. Dentro de las consultas realizadas en las bases de datos científicas se realizó una exploración sobre la existencia de metodologías que protejan los datos en el estándar DMR enfocados a los ataques de denegación de servicios DoS, evidenciando que la generación de conocimiento en revistas científicas en esta área es casi nula, por lo que se procedió a realizar búsquedas en blogs de expertos en radio frecuencia, foros de RF con resultados más positivos. Se encontró material referente a experimentaciones y laboratorios sobre ataques que afecten la disponibilidad sobre el

estándar DMR. En algunos casos se encontró información de algunos fabricantes que expresan que el modelo DMR es afectado por variables externas al protocolo y que en algunos países el estándar DMR ha tenido afectación en la disponibilidad tanto en voz como para datos. De manera consecuente, se procedió a realizar búsquedas que pongan en riesgo algún otro pilar de la seguridad informática; desafortunadamente los resultados fueron negativos: no se pudo encontrar documentación relevante. Se encontró información de personas con experimentos, pero efectivos hacia las afectaciones sobre el estándar DMR. Las comunicaciones digitales toman fuerza por todos los beneficios que brindan en cuanto a calidad, rendimiento y seguridad. Es por esto por lo que las empresas del sector de la seguridad y vigilancia privada para estar a la vanguardia de las comunicaciones están migrando a radios con protocolo DMR. Con la experiencia profesional y académica; las exploraciones iniciales avalan la pertinencia de la presente investigación al notar la ausencia de metodologías claras sobre las medidas de aseguramiento sobre posibles ataques que pueden alterar el funcionamiento de la cadena de conexión del protocolo DMR. (Stahlberg, 2000) Realiza un análisis acerca de interceptación en tipos de redes GSM y WLAN que por diferentes causas se encuentran inherentemente expuestas a varios ataques de denegación de servicio y realiza un análisis sobre contramedidas que impedirían que se materialicen ente tipo de amenazas. (Verisign, 2015) empresa reconocida por proveer servicios de internet y de seguridad informática a nivel mundial en su reporte anual, evidencia un notable crecimiento de ataques de denegación de servicio; siendo las redes empresariales con constante tráfico las más afectadas. (Utilities Telecom Council, 2014) realiza una revisión general de tecnologías de radio comunicación digital existente para ser usadas en infraestructuras críticas. Se aprecia que no hay una definición sobre el tipo de seguridad informática y de información que se deba implementar en el protocolo radio móvil digital o las condiciones generales de los actores físicos y lógicos que se usan para el trasporte de datos. La super intendencia de vigilancia publicó una restricción sobre equipos de interceptación y del uso de estos equipos por parte de empresas de vigilancia y seguridad privada debido posibles aplicaciones de hardware para este tipo de actividades (Super Vigilancia, 2009). Este antecedente es crítico, debido a que este tipo de empresas se encuentran reguladas por la superintendencia de vigilancia y seguridad que prohíbe este tipo de prácticas y genera fuertes sanciones (Super Vigilancia, 2009), así como retiro de licencias de funcionamiento a este tipo de empresas. La

conciencia sobre la necesidad de comenzar a utilizar cada vez más la seguridad en las comunicaciones es algo que se ha introducido muy poco en la sociedad, los administradores de redes, diseñadores de aplicaciones y protocolos. La realización y aplicación de una metodología de mejoramiento de la disponibilidad por medio de la detección de intrusos ajustada al estándar; mejoraría porcentualmente en la estabilidad y calidad del servicio de radio móvil digital DMR. Obteniendo beneficios en el sector privado y amateur; este último con un auge importante en Europa (Burningham, 2015).

1.3 Objetivos

1.3.1. General

Elaborar una metodología de detección de intrusos para radios que utilizan protocolo DMR, que permitirá identificar y tratar ataques de denegación de servicios que afectan la disponibilidad en la transmisión de datos para empresas de seguridad privada a fin de reducir los riesgos de perdida de paquetes de datos en la cadena de conexión.

1.3.2. Específicos

- Identificar servicios y tecnologías implicadas en las comunicaciones a través del protocolo radio digital móvil DMR.
- Realizar un análisis de riesgos para determinar posibles impactos negativos ocasionados por diferentes ataques informáticos que generen denegación de servicio.
- Proponer una metodología orientada a la detección de DoS en las comunicaciones basadas en el estándar DMR que contenga las posibles alternativas de protección y respuesta.

2.Capítulo 2: Estado del Arte

Para encontrar el foco real de la investigación, se validaron los estados documentales de las bases de datos indexadas para así buscar la posible actividad científica o investigación sobre las metodologías existentes en el estándar DMR. El resultado de la búsqueda no arrojo información concreta, precisa y relevante de metodologías que se adapten al estándar DMR. Cabe aclarar que la información encontrada hace referencia a la comunidad radio aficionada “amateur” que en sus blogs personales documentan algo de información del estándar DMR. Por esto se recurre al insumo de un análisis bibliométrico para posicionar y aumentar la importancia de la metodología de detección de intrusos para el estándar. La bibliometría como método estadístico (Piñero, 1992) permitió realizar un análisis más profundo del estado actual de las investigaciones vecinas e influyentes a la metodología propuesta. La bibliometría como fundamento estadístico y matemático permitió analizar la actividad científica y producción de literatura ligados al estándar DMR. A su vez permitió posicionar tendencias sobre las condiciones actuales de la literatura en sí. Los indicadores obtenidos en el análisis bibliométrico suministraron información de los procesos investigativos relacionados directa e indirectamente con el estándar. Para la realización de este análisis se tuvo en cuenta aspectos como: Detección de intrusos IDS, denegación de servicios DoS y la incidencia en la transmisión de datos en radio DMR.

2.1 Análisis bibliométrico en DMR

En la búsqueda de información referenciada a las posibles metodologías sobre el estándar DMR; no se lo gro encontrar información científica asociada algún pilar de la seguridad informática. Por ende, se soportó el estado del arte con un análisis bibliométrico para lograr cuantificar con la base de datos SCOPUS para obtener documentación científica del estándar DMR y potencializar la búsqueda con las herramientas avanzadas de esta plataforma.

En el Anexo A se puede observar un vacío en la literatura en la documentación técnica de las cuales se puede obtener información detallada de los avances tecnológicos en esta rama de la ciencia. Esto aumenta la importancia de la metodología propuesta ya que no existe documentación o actividad científica que pueda soportar el inicio de unas reglas protocolarias del estándar. El filtrado de búsqueda está relacionado en todos los periodos anuales y tipos de documentos.

2.2 Análisis sobre detección de intrusos (IDS)

Se realizo una búsqueda de la actividad científica enfocada a la detección de intrusos en las diferentes ramas de la ciencia de la computación en los últimos tres años. La ventana de búsqueda de todas las figuras de este sub capitulo está ligada a la base de datos SCOPUS con la sintaxis: TITLE-ABS-KEY (intrusion AND detection AND data limited 2017-2019).

En el Anexo B se puede observar alta actividad científica en los últimos años, enfocada al aumento y el desarrollo tecnológico que existe con respecto a técnicas de detección de intrusos. (Chang y Dillon, 2019). Se hizo referencia a las ciencias de la computación porque propiamente para el estándar DMR no hay actividad científica publicada.

Luego se realizó una búsqueda de la actividad científica por autores, enfocada a la detección de intrusos en las diferentes ramas de la ciencia de la computación, se aclara que se tomaron los últimos tres años como referencia.

En el Anexo C se puede observar actividad científica de los autores que más escriben de la temática de detección de intrusos. Esto denota que los sistemas de detección están

siendo explotados, desarrollados e implementados en los diferentes sectores. Detectar intrusos permitirá tener un control sobre las infraestructuras digitales. Esto impacta a gran escala la importancia de tener un sistema de detecciones en las topologías computacionales para así mitigar las intrusiones a los sistemas que deben protegerse.

Luego se realizó una búsqueda sobre la actividad científica por países, enfocada a la detección de intrusos en las diferentes ramas de la ciencia de la computación, se aclara que se toman los últimos tres años como referencia.

En el Anexo D se puede observar que los países con más actividad científica enfocada a la detección de intrusos; son las grandes potencias desarrolladoras de tecnología. Esto indica un alto crecimiento y cohesión entre los ciberataques vs ciberdefensa. Se resalta el vacío documental en países latinoamericanos, es claro la importancia y la necesidad de la actividad científica que supla la necesidad del entorno de la industria.

2.3 Análisis sobre denegación de servicios (DoS)

Se realizó una búsqueda de la actividad científica por año enfocada a la denegación de servicios DoS en las diferentes ramas de la ciencia de la computación en los últimos tres años. La ventana de búsqueda de todas las figuras de este sub capitulo está ligada y limitada en la base de datos SCOPUS con la siguiente sintaxis: TITLE-ABS-KEY (denail AND of AND services AND data limited 2017-2019).

En el Anexo E se puede observar poca actividad científica en la detección de intrusos, se destaca que en el año 2019 no hay actividad o documentación científica. Aunque existen muchos ataques de denegación de servicios en el sector industrial (Srinivas, 2019), debería existir más documentación sobre esta técnica ya que atenta contra la seguridad informática y sea uno de los puntos de inflexión a explotar para documentar (Wankhede, 2019). Luego se realizó una búsqueda de la actividad científica por autores enfocada a la denegación de servicios en las diferentes ramas de la ciencia de la computación, se aclara que se toman los últimos tres años como referencia. En el Anexo F se puede notar que existe algo de documentación científica de DoS enfocada a las ciencias de la computación.

Se reitera que existe documentación, pero no existe una actividad importante e imponente que cumpla con las necesidades del mercado.
Posteriormente se realizó una búsqueda de actividad científica por países enfocada a la denegación de servicios en las diferentes ramas de la ciencia de la computación se aclara que se toman los últimos tres años como referencia. En el Anexo G se puede observar poca actividad, se destaca que los países con más desarrollo tecnológico estarán ligados o comprometidos ante los ataques tipo DoS, esto los etiqueta como objetivo militar. Si se desarrolla tecnología es claro que se desarrolla o se documenta su respectiva ciberdefensa. Es claro que todos los desarrolladores en una minoría no lo hacen, pero los que están en vanguardia respetan la relación ciberataque vs ciberdefensa.

2.4 Análisis sobre problemas en la trasmisión de datos en radios

A la existencia de los diferentes protocolos, estándares y tecnologías que se asocian con la radio frecuencia; existe amplia documentación científica de las afectaciones, problemas y optimizaciones de la trasmisión de datos en esta tecnología. La trasmisión de datos por este medio ha venido tomando una fuerza importante en topologías de todos los sectores de la industria. La ventana de búsqueda de todas las figuras de este sub capitulo está ligada y limitada en la base de datos SCOPUS con la siguiente sintaxis: TITLE-ABS-KEY (transmission AND radio AND data limited 2017-2019).

Por esto se realizó una búsqueda de la actividad científica por año sobre la trasmisión de datos en radios se aclara que se toman los últimos tres años como referencia. En el Anexo H se puede observar la actividad científica en cuanto a los problemas que existen en las diferentes tecnologías y estándares adaptan la radiofrecuencia para soportar la trasmisión de datos en sus infraestructuras o topologías. A causa de esto existe una amplia actividad científica en: radio aficionados, fabricantes e investigadores. Luego se realizó una búsqueda de la actividad científica por autores sobre la trasmisión de datos en radios, se aclara que se toman los últimos tres años como referencia. En el Anexo I se puede ver que los autores con más actividad científicamente sobre la trasmisión de datos en radiofrecuencia. Se destaca que existe documentación, pero se nota un pequeño vacío en la exploración y documentación porque no hay la gráfica no representa un número importante. El resumen de la documentación encontrada muestra el top de los autores que

más escriben sobre la trasmisión de datos en toda el área de la radiofrecuencia. Cabe notar que dentro de la exploración realizada no se encontró bibliografía relacionada al estándar DMR, pero se trató de consolidar por medio del Anexo I que se documenta sobre el RF y la trasmisión de datos. Luego se realizó una búsqueda de la actividad científica por país enfocada a la trasmisión de datos en radio, se aclara que se toman los últimos tres años como referencia. En el Anexo J se muestran los países que más documentan y publican sobre los posibles problemas que existen en la trasmisión de datos sobre la radio frecuencia y que de alguna manera aprovechan el espectro como ducto o medio de trasmisión. Cabe notar el patrón de resultados que se perfila en la exploración, ya que son los mismos países potencia los fabricantes de tecnologías que regularmente están en el mercado de los radios móviles.

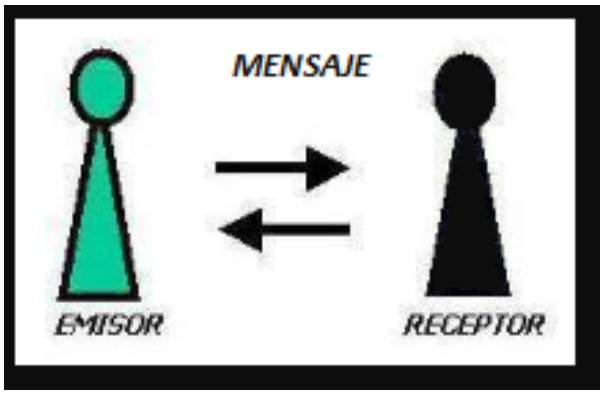
3.Capítulo 3: Marco teórico

En este capítulo se analizó el funcionamiento de la tecnología radio móvil digital DMR. Se tuvieron en cuenta aspectos relevantes por los cuales los grandes fabricantes de radiocomunicaciones adoptaron el estándar para la fabricación de sus equipos, escenarios de implementación, herramientas usadas para la administración de plataformas, ventajas con desventajas y la actualidad en escenarios productivos en empresas de vigilancia privada. También se describieron antecedentes de afectación en radio comunicaciones por ataques que ponen en riesgo la disponibilidad para realizar propuestas preventivas para mejorar el funcionamiento de los servicios incluidos en el estándar. Luego se tuvo en cuenta herramientas libres OPEN SOURCE como propuesta contributiva a la generación de estrategias de control y protección en toda la cadena de conexión de la tecnología DMR. Seguidamente se analizó los sistemas de detección de intrusos, los tipos de usos en el espacio radioeléctrico, la aplicabilidad en la detección de ataques de denegación de servicios DoS; así como las ventajas y desventajas al implementar este tipo de control técnico de prevención. Igualmente se describe la pertinencia del IDS orientado a escenarios complejos de seguridad publica asociados al espacio radio eléctrico, que exigen alta disponibilidad de servicios de comunicación de datos. Y ya finalmente se plasma un análisis de riesgos de los activos que componen la cadena de conexión del estándar.

3.1 El estándar Radio Móvil Digital DMR

“Los sistemas de radiocomunicaciones móviles permiten el intercambio de información entre estaciones fijas o móviles utilizando como medio de transmisión el espectro radioeléctrico. (Perez, 2013) La manera más coherente de entender cómo funciona un protocolo de radio frecuencia es utilizar los conceptos básicos de la comunicación:

Figura 3-1: Teoría básica de la comunicación



Fuente: Construcción propia

La figura 3-1 describe la teoría de las comunicaciones y sus agentes que intervienen en la cadena, en la cual se destacan: El emisor del mensaje, el medio de trasmisión y el receptor del mensaje. DMR al ser un protocolo que depende de la radiocomunicación (DMR Association, 2017) respeta y aprovecha cada una de las fases de las comunicaciones RF tradicionales, en las que se destacan: Radios móviles, espectro, antena y repetidora.

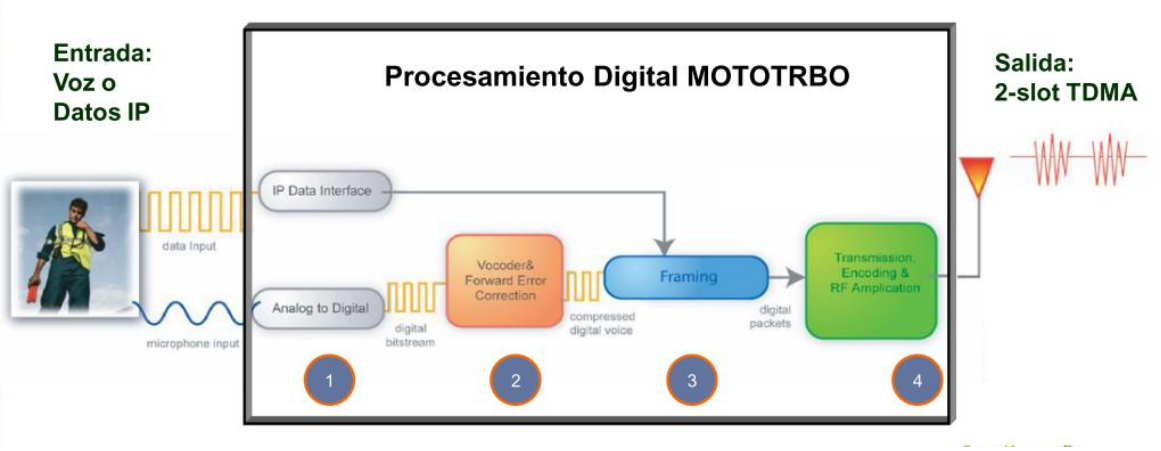
A continuación, se ilustrará los agentes que interviene en una cadena de comunicación RF clásica comparada con la cadena de comunicación DMR básica, ver tabla 3-1:

Tabla 3-1: Agentes en la cadena de conexión

AGENTES	RF	DMR
Radios móviles	Aplica	Aplica
Espectro	Aplica	Aplica
Antena	Aplica	Aplica
Repetidora	Aplica	Aplica

Fuente: (DMR Association, 2017)

Figura 3-2: Cadena de conexión básica en RF



Fuente: (Hernandez, 2017)

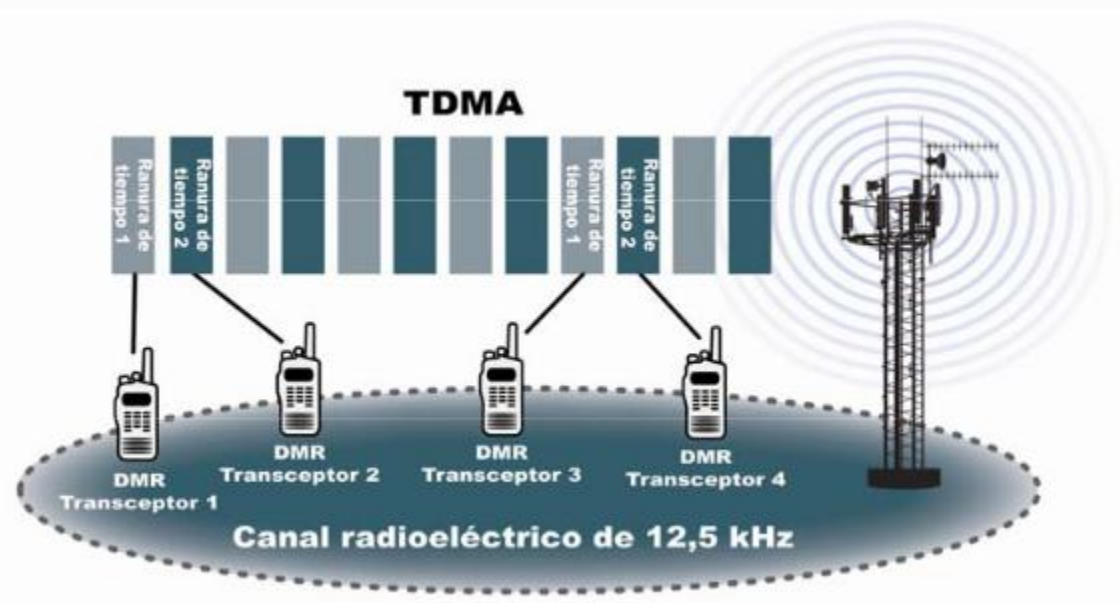
La figura 3-2 muestra los pasos de la cadena de conexión en DMR. El paso 1 muestra él envió de señales análogas o digitales, el paso 2 muestra la conversión de paquetes de voz con el codificador a señal digital, el paso 3 muestra la fase ajuste o de empaquetamiento de la trama PDP y la fase 4 organiza el canal de transmisión en TDMA para el transporte de paquetes. DMR es un protocolo de radio digital de banda estrecha con el objetivo de mejorar el espectro sobre la radio analógica tradicional PMR, (DMR Association, 2017) aprovechar el espacio de canales en 12.5 KHz existentes en frecuencias ya autorizadas y así adaptar comunicaciones en ambas direcciones sobre la radio digital explotando tanto servicios de voz como los servicios de datos.

3.1.1 Transmisión de datos bajo el estándar DMR

La transmisión de datos bajo el protocolo DMR se focaliza en el medio de trasmisión y la tecnología que lo soporta; TDMA es la tecnología utilizada por DMR, la cual proporciona dos canales individuales de 12.5 KHz aumentando la capacidad al doble con respecto a las otras tecnologías. Esto permite compatibilidad entre fabricantes cumpliendo con la filosofía y propiedades de un sistema abierto. Una de las funcionalidades de DMR son trasmitir datos a servicios adicionales como:

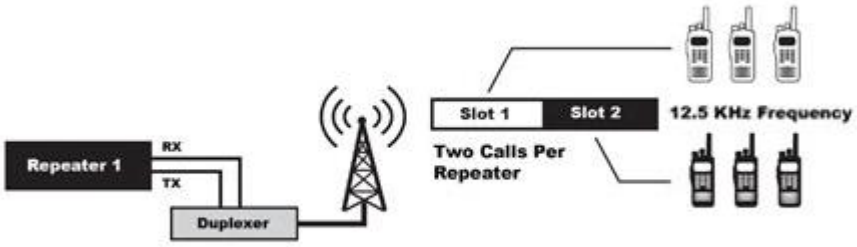
- Telemetría
- Mensajes de texto
- Coordenadas GPS
- Datos IP

Figura 3-3: Topología de onda TDMA con DMR



Fuente: (DMR Association, 2017)

Figura 3-4: Topología RF convencional



Fuente: (DMR Association, 2017)

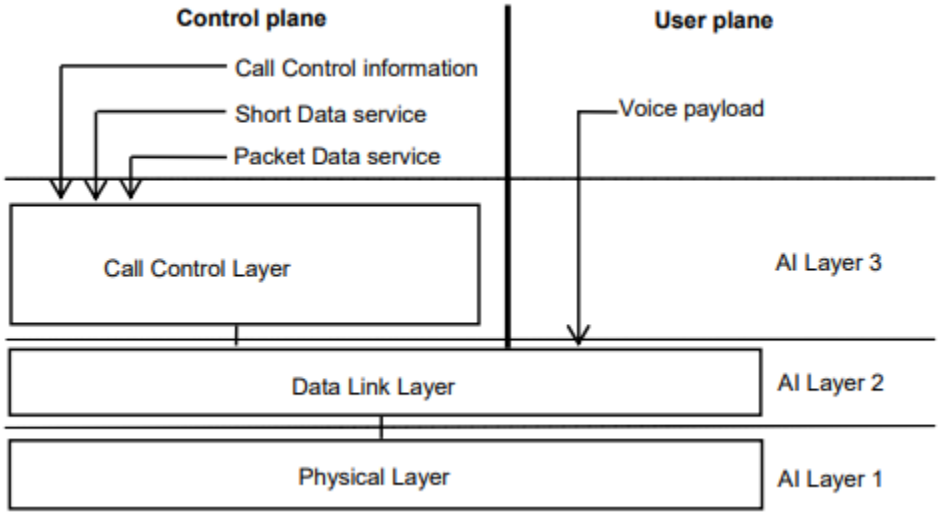
En las figuras 3-3 y 3-4 se puede observar una topología para que exista una transmisión de datos efectiva en la cadena de conexión del estándar, se debe entender primeramente la arquitectura del protocolo que se rige a tres capas o LAYERS:

Capa 1 "Air Interface Physical Layer". Es la interface física encargada de enviar/recibir físicamente los bits que contiene las siguientes funciones:

Capa 2 "Air Interface Data Link Layer". Capa encargada de las conexiones lógicas ocultando el medio físico de las capas superiores, se listan las principales funciones:

Capa 3 "Air Interface Call Control Layer". Capa encargada del panel de control, de los servicios y características soportadas por DMR, aprovisiona las siguientes funciones:

Figura 3-5: Arquitectura de las capas



Fuente: (DMR Association, 2017)

En la figura 3-5 se muestran las capas de la arquitectura donde hace presencia el protocolo PDP, que es el encargado de realizar todos los procedimientos de transmisión de paquetes de datos como por ejemplo datos no confirmados, datos confirmados, respuesta de datos confirmados, etc.

El protocolo PDP en DMR contiene los siguientes tipos de transmisiones de la capa 2:

- Transmisión de datos del servicio portador
- Transmisión de datos no confirmado
- Datos confirmados en transmisión de datos y transmisión de respuesta

También soporta la transmisión de la capa 3 en los siguientes aspectos:

- Protocolo de internet
- Dato RAW
- Estados de datos precodificados
- Datos definidos

Y a su vez es soportado por el protocolo clásico de internet IPv4:

- Direccionamiento IP
- Direccionamiento IP neutral
- Error en los mensajes IP
- Datos no confirmados en la capa 2
- Datos confirmados en la capa 2
- Datos UDP/IPv4
- Encabezados comprimidos UDP/IPv4
- Datos de aplicación sobre IP

3.1.2 Factores que inciden en la disponibilidad de datos en DMR

Una red de computadoras es un conjunto de equipos y programas informáticos conectados entre sí que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos. La finalidad de estos sistemas es compartir información, recursos y ofrecer servicios (Tanenbaum y Wetherall, 2012). El estándar DMR se encuentra alineado con la definición anterior y hereda como en cualquier red las vulnerabilidades conocidas que afectan directamente los pilares de la seguridad de la información: integridad, disponibilidad y confidencialidad. Se describen a continuación los factores conocidos que afectan la disponibilidad en el estándar DMR:

- Ataques de fuerza bruta
- Problemas del firmware del fabricante
- Envío de comandos OTA (Over The Air) que desactiven terminales
- Clonar un equipo DMR
- Técnicas de radiojamming (interferencias intencionadas)
- Programación incorrecta de la estación base (dispositivo móvil)

3.1.3 Ventajas y desventajas en la transmisión de datos en DMR

Tabla 3-2: Comparativo en trasmisión de datos

VENTAJAS		DESVENTAJAS	
DESCRIPCION	**OBSERVACIONES**	**DESCRIPCION**	**OBSERVACIONES**
Duplicación en la capacidad en los canales autorizados y disponibles	Es posible activar segundo canal como contingencia del primario para el envío de voz	Complejo uso de indicadores por regiones	Interconectar el estándar a la red es codificado bajo un identificador que puede complicar la implementación
Retrocompatibilidad con los anteriores espectros análogos	Es posible implementar el estándar sobre tecnologías anteriores	Uso de CodePlug en la configuración de los móviles	Uso de código de colores en la autenticación de los móviles
Uso efectivo de la infraestructura propuesta	Aprovecha muy bien el espectro	Cada usuario maneja una ranura de tiempo asignada dentro del protocolo TDMA	Puede tender a saturarse el canal
Batería con mayor duración	No es fuente importante de consumo en los dispositivos móviles	Perdida de la trasmisión si no hay celdas disponibles en el protocolo TDMA	El canal saturado entrara fuera de conexión
Creación de aplicaciones especificas	Se pueden adaptar aplicaciones para propósitos específicos	Propenso a distorsión propia del espectro	La onda debe estar en buenas condiciones de emisión y recepción
Flexibilidad por medio de los canales TDMA		Interferencias entre antenas y radios móviles (edificios montañas, etc.)	Los móviles pueden ser afectados por interferencias de liana a vista
Funciones avanzadas de control	Por el lado del dispacher es posible controlar en su totalidad terminales y repetidoras	Retrasos por tiempos límites del sistema por las interferencias	Puede ocasionar encolamiento de entrega y recepción de datos

Mejora en el sonido	Utiliza un códec efectivo de intercambio análogo/digital	Perdida de la señal por los tiempos limites preconfigurados, tiende a ignorar la señal	
Bajo costo de implementación con respecto a otros estándares digitales	Comparado con otras tecnologías, es aplicable por sus bajos costos	Problemas de propagación de la señal cuando no se tiene línea a vista	Las condiciones físicas pueden afectar la emisión y recepción entre repetidoras y móviles
Estándar totalmente abierto	Regido bajo las normas open Source		
Respaldo mundial en diferentes marcas	Tiene mucho respaldo de marcas importantes a nivel mundial		
Uso profesional	Es adoptado por sectores críticos		
No es privativo	No se requiere de licenciamiento		

Fuente: (DMR Association, 2017)

3.1.4 Contexto de las empresas de seguridad privada y las radiocomunicaciones

El sector de la vigilancia y seguridad privada física ha tenido un importante crecimiento en el uso del estándar DMR. El panorama de inseguridad del país se ve reflejado por el uso y contratación de personal para estos fines; tanto ha sido el aumento que las empresas que prestan este servicio han venido creciendo y potencializando en adquirir tecnología que supla las necesidades de la industria. Por esto adoptan las radiocomunicaciones. Estas ofrecen alta disponibilidad y mejor rendimiento ante situaciones extremas que así lo requiera el sector. Las altas inversiones en el sector a nivel mundial así lo muestran:

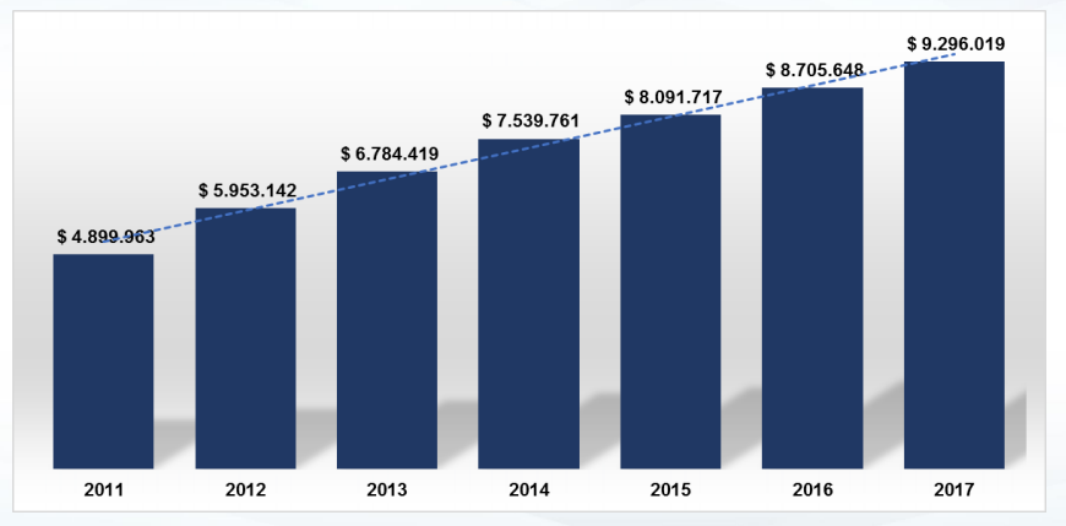
Tabla 3-3: Mercados por país

REGION	MERCADO USD	CRECIMIENTO %
Norteamérica	49.200	7-8
Europa	37.800	6-10
Japón	7.400	7-9
Latinoamérica	6.500	9-11
Resto del mundo	16.200	10-12
TOTAL	**117.100**	**7-8**

Fuente: (Abondano, 2016)

La superintendencia de vigilancia y seguridad privada, entidad adscrita al ministerio de defensa nacional, realiza informes anuales del del desempeño del sector; reflejando un disparo y activación de esta economía en el país (Superintendencia de vigilacia, 2017).

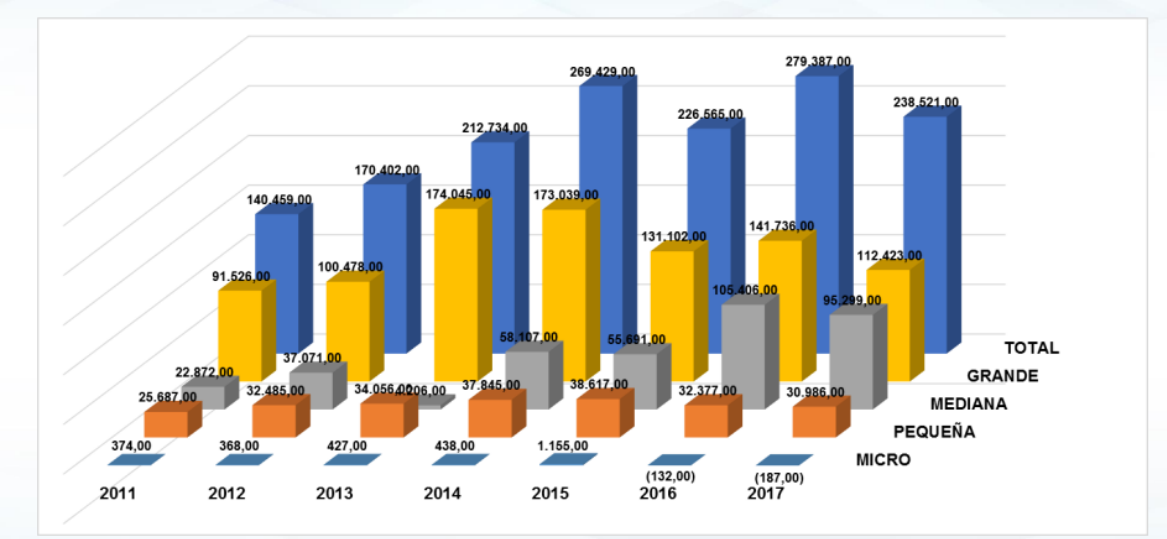
Figura 3-6: Actividad económica por año de la vigilancia privada



Fuente: (Superintendencia de vigilacia, 2017)

Al ser un sector en pleno crecimiento y tratarse de un apoyo general a la seguridad pública es claro que las comunicaciones son claves en la prestación de un servicio de calidad. El crecimiento vertiginoso del sector es una clara muestra de la importancia que tiene una metodología aplicada que permita elevar los niveles de disponibilidad dada la importancia del medio de transmisión para el sector; fortaleciéndolo con controles, detección y respuesta ante ataques de denegación de servicio, permitiendo elevar los indicadores de disponibilidad.

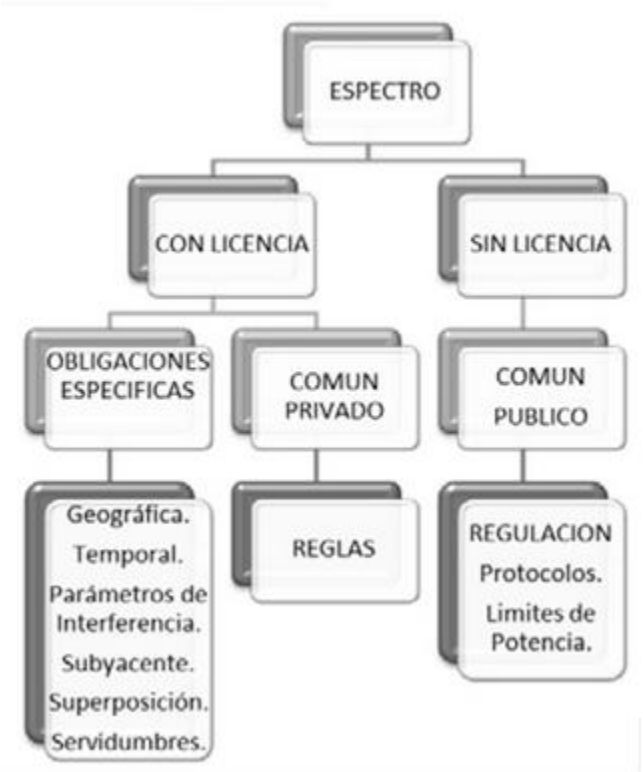
Figura 3-7: Crecimiento del sector de la vigilancia privada



Fuente: (Superintendencia de vigilacia, 2017)

Se puede ver en la figura 3-7 que existe un crecimiento constante año tras año. El crecimiento del sector genera la necesidad de tener apoyos de tipo tecnológico para la prestación de servicios de vigilancia. Por esto, las empresas por lo general para sus labores operativas usan las radiocomunicaciones por la facilidad de reportar y de dar respuesta inmediata a eventos. El consumo de las radiocomunicaciones está regulado por:

Figura 3-8: Jerarquización y control del espectro



Fuente: (Cadena, 2015)

La figura 3-8 representa la gestión actual del espectro en Colombia y la distribución que tiene que puede ser licenciada o sin licencia. Estas asignaciones están sujetas a los lineamientos que establece el ministerio de tecnología y comunicaciones MINTIC. Actualmente, se presentan las tendencias en la gestión del espectro basado en protocolos y requerimientos para su aplicación.

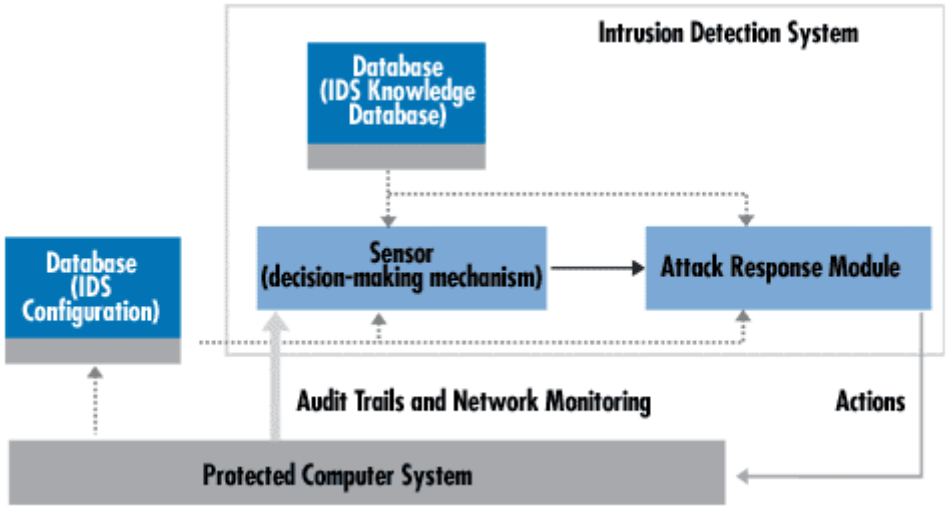
3.2 Detección de intrusos IDS

Existen mecanismos que tienen como objetivo proteger los sistemas de información. Algunos participan dentro de una cadena de conexión como filtros, listas de acceso. Como en el caso de los routers, firewalls, los sistemas de detección como antivirus y los sistemas de detección de intrusos. Estos últimos hacen parte de la última línea de defensa de un esquema de seguridad implementado en un sistema informático y no solo son útiles en la detección de eventos de seguridad sino también posibilitan la reacción temprana ante eventos de intentos de romper la seguridad establecida en líneas de defensa superiores (Ortega, 2004). Los sistemas de detección de intrusos son el fruto de la realización de auditorías relacionadas con datos estadísticos y análisis electrónico de datos. Con el tiempo estos sistemas han tomado un rol fundamental en la seguridad de las redes de comunicación. Con el paso del tiempo los sistemas de información y el crecimiento del uso de computadoras fue mayor, dificultando la tarea de auditoria manual sobre el uso que se les daba. Fue entonces cuando James P. Anderson ideo un sistema capaz de recolectar toda esta información de auditoria en forma electrónica y presentar el que se consideraría el primer informe de detección de intrusos a inicios de los años 80 (Gramajo, 2005). Su sistema era capaz de reconocer intentos de suplantación de usuario y evaluar el comportamiento de un perfil de usuario entre normal o inusual, creado a partir del análisis estadístico de datos que sería la base para los sistemas IDS desarrollados posteriormente. Por esto, existen soluciones de diferentes tipos ofrecidas por empresas de seguridad informática o la comunidad GNU que pretenden aplicar cada vez más sus desarrollos fundamentados desde una perspectiva defectiva a fin de prevenir incidentes que atenten plenamente con alguno de los pilares mencionados (Kaushik y Deshmukh, 2011). Los sistemas de detección de intrusos pueden ser comparados con sistemas de alarmas clásicos que ante alguna obstrucción o ingreso indebido puede generar una advertencia a quien los administre para que se tomen medidas preventivas. Con el tiempo, el concepto ha evolucionado proporcionando no solo alertas sino coexistencia entre la parte correctiva y de control en forma automatizada IDS + IPS teniendo en cuenta que esta relación puede ser costosa en términos de rendimiento debido a latencia por el análisis exhaustivo de todos los paquetes de red. Algunas definiciones propuestas de sistemas de detección de intrusos coinciden con que:

- Un sistema de detección de intrusos IDS es un software capaz de realizar verificación de paquetes de red y los compara con parámetros establecidos previamente asociados a un comportamiento y que al encontrar alguna relación genera alertas de un posible ataque (Benjamas y Saiyod, 2014).
- La implementación de una segunda línea de defensa, que es el Sistema de Detección de Intrusos IDS, se considera necesaria como parte de un enfoque integrado para proteger la red contra los comportamientos sospechosos (Moulad, 2018).
- Una intrusión es un conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso.” (Heady, 2011)
- Desde el año 1980 los firewalls logran proteger a la red de una gran variedad de ataques, sin embargo, existen otros ataques que se presentan ante los firewalls con apariencia de tráfico normal. Mediante la simple inspección de los paquetes es muy difícil descubrir si se ha tratado de un tráfico normal o de uno malicioso, por lo que se hace necesario recurrir a sistemas de detección más específicos, que analicen los paquetes que entran a la red, elaboren estadísticas y traten de identificar el tráfico malicioso; estos sistemas se denominan IDS (Ptacek,1998).
- Según Amoroso la detección de intrusos es "un proceso de identificación y respuesta a actividades maliciosas dirigidas a recursos informáticos y de redes" (Amoroso, 1999).

Si es Analizado lo anterior se puede concluir en forma global que los sistemas de detección de intrusos son mecanismos automatizados que permiten alertar y dar respuesta sobre actividades maliciosas dirigidas a recursos informáticos que atentan contra los pilares fundamentales de la seguridad de la información confidencialidad, integridad y disponibilidad.

Figura 3-9: Arquitectura de un IDS



Fuente: (Villal, 2002)

La figura 3-9 muestra la arquitectura de un sistema de detección de intrusos en un sistema que se pretende proteger. Cuenta con una base de datos de configuración ajustada al sistema protegido y un sensor encargado de la recolección de datos. Los sensores reciben datos brutos de tres fuentes principales de información: propia base de conocimiento de IDS o firmas, registro de SYSLOG y pistas de auditoría. El registro del sistema puede incluir, por ejemplo, la configuración del sistema de archivos, las autorizaciones de los usuarios, etc. Esta información crea la base para un nuevo proceso de toma de decisiones. El rol del sensor es filtrar la información y descartar cualquier información irrelevante obtenida del conjunto de eventos asociados con el sistema protegido, detectando actividades sospechosas.

3.2.1 Metodología para la detección de intrusos

Las metodologías existentes para desarrollar los sistemas de detección de intrusos pueden ser aplicadas según el tipo de comportamiento del sensor usado; esto pueden ser basados en firmas, en políticas de control, anomalías o en reputación. De igual modo, los sistemas de detección de intrusos pueden ser usados basados en host que trabajan de lado del

sistema operativo usado en un punto final de la infraestructura o en red que será ubicado en un punto en donde se pueda evaluar el tráfico de entrada y salida. La elección del sistema de detección dependerá de las necesidades de la red que se quiere monitorear. Según (Ortega, 2004) el sistema de detección depende de los siguientes parámetros:

- **Precisión:** se ocupa del descubrimiento adecuado de los ataques y de evitar una tasa alta de falsas alarmas.
- **Desempeño:** Es la velocidad a la que se procesan los eventos de auditoría comparando con firmas o por comportamiento.
- **Integridad:** es la propiedad de un sistema de detección de intrusos. Para identificar todos los ataques.
- **Tolerancia a fallos:** un sistema de detección de intrusos debe ser resistente a los ataques, especialmente a los ataques de denegación de servicio.
- **Oportunidad:** un sistema de detección de intrusos tiene que cumplir y prosperar su análisis lo más rápido posible para trasladar al administrador de seguridad para que este pueda responder antes de que ocurra un nivel afectación en un sistema de información, y también para evitar que el atacante identifique controles y pueda eliminar huellas.

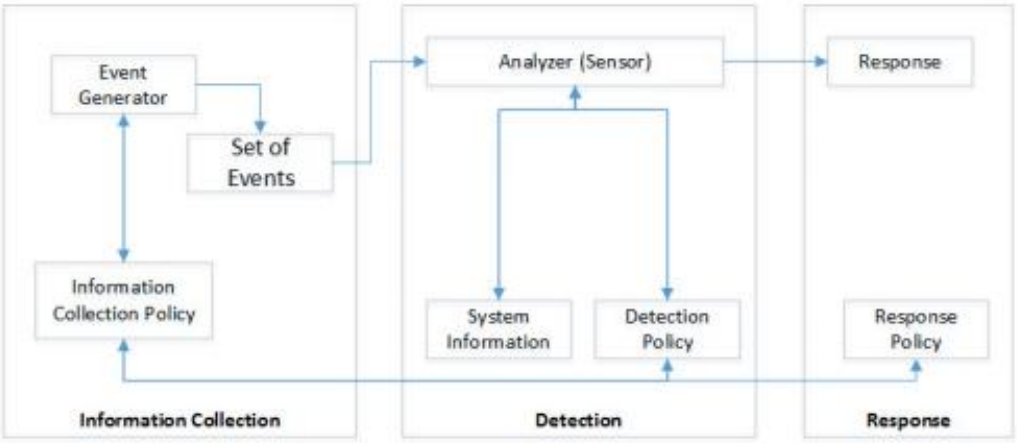
De acuerdo con lo anterior es posible definir una metodología estandarizada de operación de un sistema de detección de intrusos basada en seis fases generales:

- **Preparación para un ataque:** Este paso precede a la detección de cualquier ataque. En esta fase se colocaron los procedimientos y mecanismos disponibles **para detectar y responder a los ataques.**
- **Identificación de un ataque:** que es crucial porque basado en un parámetro se puede descifrar un comportamiento basado en un vector de ataque.
- **Restricción del ataque:** Se restringe sustancialmente el acceso al sistema para evitar la extensión del daño. Pero el ataque se controla de forma pasiva y se convierte en un registro completo de las acciones del atacante para su uso futuro.
- **Neutralización del ataque:** Es realizado un bloqueo virtual del ataque.

- **Recuperación:** el sistema vuelve a una condición segura de acuerdo con lo que requiere la política de seguridad.
- **Monitoreo continuo del ataque:** para tomar medidas contra el agresor, ya que se registró cualquier problema durante el manejo del evento y las experiencias adquiridas (Tsirka, 2016).

Los sistemas de detección de intrusos aplican métodos mediante los cuales se automatiza la detección de intrusiones. Estas se clasifican en falsos positivos y los falsos negativos. Los falsos positivos son las secuencias de eventos al que no se encuentra bien parametrizados que el IDS clasifica como intrusiones, mientras que los falsos negativos se refieren a intentos de intrusión que el IDS no puede informar y pasan por alto.

Figura 3-10: Actividades generales de un sistema de detección de intrusos



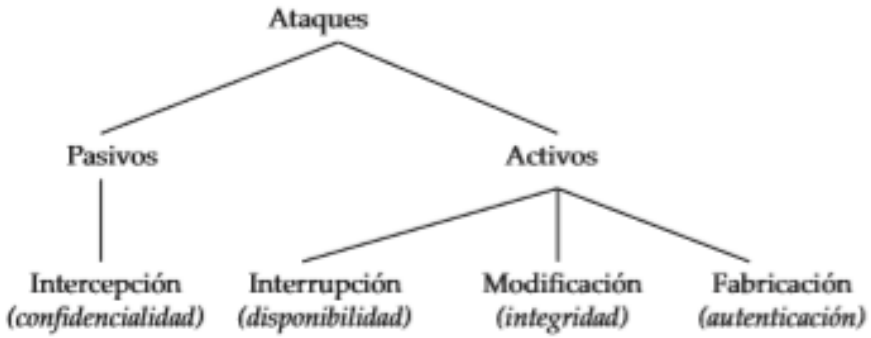
Fuente. (Dorosz, 2003)

En la figura 3-10 se observan las actividades que un sistema de detección de intrusos efectivo y eficiente. Posee una arquitectura que comprende un módulo de detección que recoge datos que contienen evidencia de intrusiones, un motor de análisis que procesa los datos para la identificación de intrusivos y un componente de respuesta que produce un informe de intrusiones.

3.2.2 Denegación de servicios DoS que afectan la disponibilidad

La naturaleza de un ataque DoS se centra en bloquear una actividad lícita de un sistema productivo que si es llevado a la práctica puede ser él envió de una transacción bancaria, una coordenada de un sistema de navegación o el acceso a un sitio web. Por su parte, otros tipos de ataques por lo general centran su atención en la posibilidad de extraer información, tomar control de un sistema, generar alteración o modificar datos. Los ataques DoS están destinados a forzar al objetivo a detener el servicio que proporcionan inundándolo con peticiones ilegítimas. Por lo tanto, para que el ataque DoS sea detectadas deben ser analizadas las características de tráfico como el “porcentaje de Conexiones que tienen el mismo host de destino hacia el mismo servicio”, las características de nivel de paquete como los "bytes de origen" y el “porcentaje de paquetes con errores” sea significativo. Al detectar ataques DoS, puede que no sea importante saber si un usuario está "conectado o no". (Castaño y Segura, 2011).

Figura 3-11: Tipos de ataques DoS



Fuente: (Villal, 2002)

La figura 3-11 muestra los diferentes tipos de ataques y como pueden ser clasificados. Los ataques DoS son clasificados como activos de interrupción que afectan fundamentalmente la disponibilidad y tienen como objetivo reducir la funcionalidad de un sistema que se encuentre activo para limitar una fuente de información a ser accedida y lograr afectar un canal de transmisión o incluso una mezcla de todos. Esto se puede hacer a través de la explotación de fallas, sobrecarga de conexión o inundación de tráfico. El ataque no necesariamente produce una interrupción total de un recurso; en su lugar, podría reducir el rendimiento o introducir latencia para obstaculizar el uso productivo de un recurso. Aunque la mayoría de los ataques DoS son temporales y duran solo mientras el atacante lo considere, claro que también hay algunos ataques DoS permanentes. Los ataques DoS se diferencian de los ataques DDoS en que son realizado por una única fuente atacante que pretende afectar el sistema objetivo a diferencia de los ataques distribuidos que usan diferentes fuentes llamadas “agentes” para generar indisponibilidad en sistemas más complejos o con mayor número de recursos.

La clasificación de ataques DoS atendiendo el objetivo propuesto serán detallados con los mecanismos usados por los atacantes en el Anexo K.

3.2.3 IDS para la detección de DoS en el espectro radioeléctrico

El panorama cambia drásticamente cuando se trata de evaluar la misma disponibilidad bibliográfica en escenarios complejos como el espectro radioeléctrico. La definición precisa del espectro radioeléctrico, tal y como la ha definido la Unión Internacional de Telecomunicaciones UIT, organismo especializado de las Naciones Unidas con sede en Ginebra Suiza es: "Las frecuencias del espectro electromagnético usadas para los servicios de difusión y servicios móviles, de policía, bomberos, radioastronomía, meteorología y fijos."; lo anterior quiere decir que solo comprende las ondas utilizadas para la comunicación de radio, televisión, internet, entre otras. Estas son llamadas también ondas de radiofrecuencia. Este no es un concepto estático, pues a medida que avanza la tecnología se aumentan o disminuyen los rangos de frecuencia utilizados en comunicaciones y corresponde al estado de avance tecnológico. La importancia de tener en cuenta este tipo de escenarios en la actualidad en la seguridad informática actual se basa en que anteriormente no se asociaban sistemas de radio frecuencia con otros sistemas o con redes de datos; pero ante la necesidad de hacerlo y tener acceso cada vez más a información relacionada y a tableros inteligentes de datos para la toma de decisiones, se observa la proliferación de sistemas interconectados que heredan riesgos que comprometen la seguridad de la información. En general, podemos clasificar las amenazas de seguridad de los sistemas de radio frecuencia en dos tipos: intencionadas y no intencionadas. Las primeras aluden a fenómenos incontrolables que, si bien no repercuten directamente a los sistemas de radio, pueden poner en peligro la disponibilidad de la cadena de conexión. Las segundas son aquellas que suponen un origen humano ya sea por una vulnerabilidad conocida del sistema o inundación permitiendo modelar un vector de ataque según el interés o el nivel de afectación que pretende lograr el atacante hacia el sistema víctima. Según el contexto anterior, la disponibilidad de la trasmisión de los datos en la fase de comunicación por radiofrecuencia depende directamente de la condición de espectro en donde se hace necesario tener alternativas de detección que permitan una reacción temprana ante eventos de afectación. Por lo anterior, es posible clasificar los diferentes tipos de sistemas de control o de detección orientados a la disponibilidad.

Las interfaces más importantes y complejas se consideran las "interfaces aéreas" entre la estación base y los terminales de radio. Muchas de las aplicaciones descritas anteriormente solo estaban pensadas para grandes corporaciones y universidades con grandes cantidades de dinero dedicadas a la investigación. Sin embargo, con la creación y posterior evolución del Software Defined Radio SDR hay algunas soluciones de bajo costo que se pueden lograr con el RTL2831 u otro dispositivo similar que use software libre. Pueden ser usados varios softwares gratuitos descargados, junto con algunas soluciones para evaluar el espectro y para esta investigación funcionar como SNIFFER para la detección temprana de anomalías. De igual modo son mencionadas soluciones propietarias desarrolladas para realizar un análisis detallado en la fase de conexión de radiofrecuencia para la marca Motorola Inc., ya que posee un gran porcentaje de uso en el mercado mundial en comunicaciones de radio DMR.

3.2.4 IDS para la detección de DoS en redes TCP/IP

Los IDS se pueden clasificar en varios tipos en TCP/IP. Pueden monitorear eventos en tres niveles: red, host y aplicación. Los eventos generados por el nivel de detección elegido pueden ser analizados mediante detección de firmas o detección de anomalías (Kaushik y Deshmukh, 2011)

- **IDS nivel de red:** El NIDS consiste en un conjunto de hosts de un solo propósito que rastrean el tráfico de red y reportan los ataques a una sola consola de administración. Los NIDS funcionan mediante la revisión de los encabezados de capa de transporte IP de paquetes discretos, el contenido de los paquetes o alguna otra combinación.

- **IDS nivel host:** El sistema de detección de intrusiones basado en host HIDS se refiere a la clase de IDS que reside en una máquina host y lo supervisa. El análisis de las actividades en el host se realiza con una granularidad muy precisa para determinar con precisión qué procesos y usuarios realizan actividades maliciosas en el sistema operativo.

- **IDS nivel aplicación:** Los IDS basados en la aplicación están diseñados para tener una visión detallada de la actividad sospechosa al interactuar con una aplicación directamente y deben estar en la capacidad de alertar basados en conocimiento significativo de la aplicación que defiende.

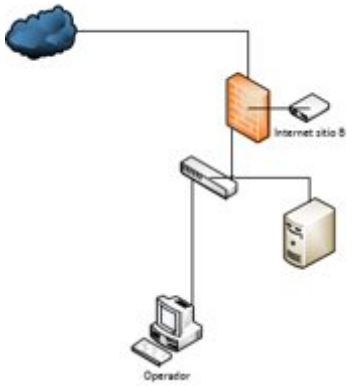
- **Detección basada en firmas:** Los IDS basados en firmas se centra en el uso de un sistema experto para identificar las intrusiones basadas en una base de conocimientos predeterminada. Puede usarse para detectar cada ataque conocido si está programado correctamente. Esta técnica es un método efectivo utilizado en productos comerciales para detectar ataques.

- **Detección basada en anomalías:** El IDS basado en anomalías se basa en la lógica de que algunos atacantes se comportan de manera diferente a los usuarios normales y, por lo tanto, los sistemas que identifican estas diferencias pueden detectar fácilmente los ataques. Estos sistemas pueden generar un número abrumador de falsas alarmas, ya que la variación del comportamiento normal de los usuarios y la red puede variar. Los IDS basados en anomalías pueden usarse para detectar ataques nunca vistos.

4.Capítulo 4: Servicios y tecnologías implicadas en las comunicaciones del estándar DMR

En este capítulo se identificarán todos los posibles actores que intervienen en la cadena de conexión del estándar DMR, tanto en la parte digital como en la parte análoga. Serán listados en base a dos grupos: Servicios y tecnologías implicados. Además, se realizará una exploración de los fabricantes con más peso en DMR. También se ilustrará los componentes que permiten la comunicación, ver Tabla 4-1. Serán revisados los diferentes componentes del estándar que aportan a las funcionalidades extendidas más allá de la voz; donde se encuentran servicios y tecnologías que hacen parte de la transmisión de datos. Analizar estos componentes dará una visión del alcance del estándar en cuanto a datos se refiere y como puede ser afectada la disponibilidad si es analizado desde el punto de vista del atacante en un escenario productivo teniendo conocimiento de estas funcionalidades.

Tabla 4-1: Topología de un escenario DMR

PARTE DIGITAL INTERFACES AEREAS DE LA TOPOLOGIA	PARTE TCP DE LA TOPOLOGIA
	

Fuente: Creación propia

4.1 Servicios implicados en el protocolo DMR en la transmisión de datos

Cuando se tiene un sistema de radio que usa el estándar DMR, el mapa general de la infraestructura debe ser comprendido como equipos digitales fabricados por uno o varias marcas comerciales a los cuales se les aplicaron una serie de características de compatibilidad reguladas por la ETSI (instituto europeo de normas de telecomunicación) para que operen con señales de radiofrecuencia TDMA (time division multiple Access) y ser usados para comunicación de voz y transmisión de datos. Este último aspecto es materia de estudio en el presente análisis y lo largo de los siguientes capítulos en detalle.

Cuando son evaluadas las características generales de los equipos (radios y repetidoras) con el estándar DMR, se perciben diferencias en cuanto a la capacidad técnica en cada uno de los equipos que van ligados a factores tales como el nivel del estándar DMR usado, la marca y al sector industrial en el que se implementan; que afectan el valor comercial y en la capacidad operativa del equipo.

El estándar divide su capacidad en básicamente dos escenarios; los servicios convencionales de voz y los servicios de datos, a continuación, se listan los servicios implicados en ambos escenarios descritos previamente:

Tabla 4-2: Servicios sobre el estándar DMR

SERVICIOS EN DMR		**SERVICIOS SUPLEMENTARIOS EN DMR**
voz	llamada individual	Ingreso tardío
		Apertura de canal de voz en modo de llamada
		Identificación de la parte hablada
	llamada grupal	Ingreso tardío
		Llamadas de voz sin dirección
		Apertura de canal de voz en modo de llamada
		Identificación de la parte hablada
	llamada a todos	Ingreso tardío

		Identificación de la parte hablada
	llamada múltiple	Ingreso tardío
		Identificación de la parte hablada
confirmación paquetes (PDP)	IP sobre PDP	
	Paquetes pequeños sobre PDP	
paquetes de datos sin confirma (PDP)	IP sobre PDP	
	Paquetes pequeños sobre PDP	

Fuente: (DMR Association, 2017)

En la tabla 4-2 se pueden visualizar los servicios generales. Realizando una visión general del marco DMR en cuanto a datos se refiere se observan dos familias de servicios: paquetes de datos confirmados y sin confirmar. Estos están compuestos de IP sobre PDP y de paquetes pequeños PDP independientemente de en donde se sitúen. De acuerdo con los niveles del estándar el comportamiento del paquete de datos y sus servicios es el siguiente (Onali, Sole, Y Giusto, 2011):

- Los niveles 1 y 2 de DMR utilizan el PDP para datos no confirmados, confirmados, y datos cortos.

- El nivel III de DMR también puede usar PDP para datos no confirmados y confirmados en el canal de carga útil, pero el enlace troncal tiene sus propios servicios de datos cortos que utilizan el canal de control.

El Protocolo de Paquetes de Datos (PDP)

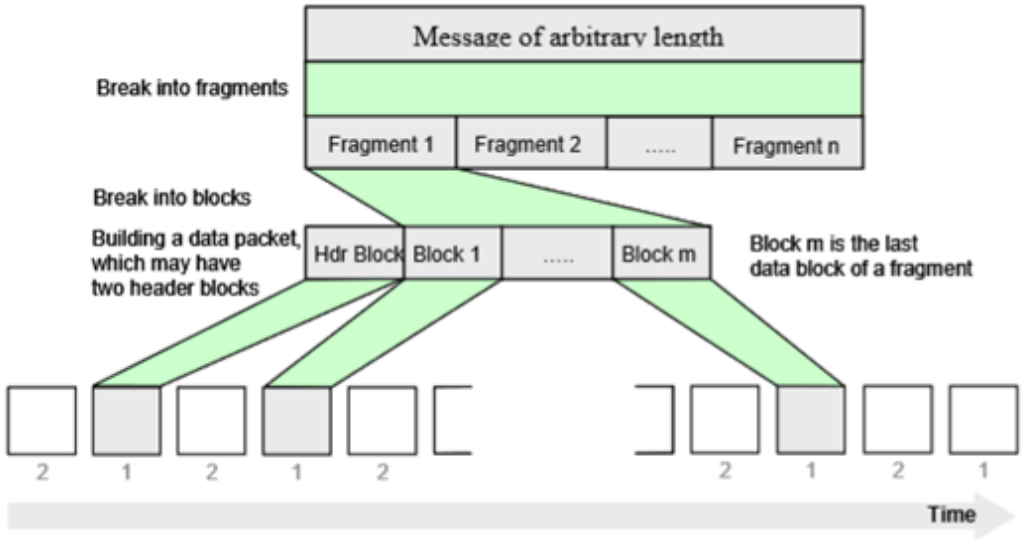
El "protocolo de datos en paquetes predeterminado" es la forma en que se envían los datos producidos por los equipos bajo el estándar DMR. El estándar DMR permite a los fabricantes definir e implementar conjuntos de características "privadas" que contienen señalización "privada" adicional, que posiblemente no puedan ser entendidas por

productos que no son compatibles con este conjunto de características "privadas". (DMR Association, 2009).

El protocolo de paquetes de datos contiene los siguientes tipos de transmisiones de datos:

- Transmisión de datos no confirmados;
- Datos confirmados: transmisión de datos y respuesta de transmisión. El PDP soporta los siguientes servicios de datos:
- Protocolo de Internet
- Servicios de datos pequeños: datos sin procesar; Estado / datos precodificados; y datos definidos.

Figura 4-1: Descomposición de un paquete PDP



Fuente: (Report, 2013).

En la figura 4-1 se muestra la descomposición de un datagrama IP en donde el mensaje PDP se divide primero en fragmentos si el protocolo de capa 3 solicita que transporte un mensaje cuya longitud sea mayor que la longitud máxima. Cada fragmento se asigna luego en un paquete único que consiste en una secuencia de bloques de datos precedidos por

uno o dos bloques de encabezado. Cada bloque está protegido por su propio código de corrección de errores (FEC). La transmisión puede utilizar una sola ranura o capacidad de datos de doble ranura. (Report, 2013)

El paquete de datos PDP es transmitido mediante diferentes escenarios usando el medio de transmisión.

IP sobre PDP

La especificación DMR es compatible con el siguiente protocolo de capa de red protocolo de Internet versión 4 (IPv4). IPv4 proporciona una entrega de datagramas de mejor esfuerzo, sin conexión, entre dos puntos de acceso de servicio. El protocolo IPv4 es activado por los protocolos de host a host (por ejemplo, TCP, UDP) en un entorno de Internet. IPv4 llama al protocolo Air Interface para que transmita el datagrama IP por el aire. El servicio portador IP de DMR se construye sobre los servicios portadores de DLL (datos no confirmados y datos confirmados). DMR PDP extiende DMR para que actúe como una subred IP. Esto permite a los programadores de aplicaciones construir sus aplicaciones en un entorno bien estandarizado. Nota: La implementación del enrutamiento y la retransmisión IP, así como la conexión a redes externas está fuera del alcance de la especificación DMR (ETSI, 2008).

Paquetes pequeños sobre PDP

El Servicio de datos cortos SDS sobre PDP es un mecanismo para transmitir mensajes de datos cortos de una entidad DMR a otra (s) entidad (s) DMR. La transmisión puede ser confirmada o no confirmada. Puede transmitir hasta 1130 bytes (18 bytes / bloque x 63 bloques - 4 bytes). El encabezado corto de datos contiene los parámetros que especifican el servicio portador y, en particular, la cantidad de datos transportados por el mensaje y su formato. (ETSI, 2008).

Datos cortos sobre PDP - Estado / Precodificado

Es la transmisión de un mensaje de estado / precodificado de una entidad DMR a otra (s) entidad (s) DMR. Este servicio permite que se envíe un código por el aire cuyo significado es conocido por todas las otras partes. Por lo general, hay una tabla de búsqueda almacenada en cada entidad DMR que contiene el mapeo entre el código y el significado (es decir, código = 00000000012 significado = "Arrived"). (ETSI, 2008).

Datos cortos sobre PDP - Datos sin procesar

Los datos sin procesar son la transmisión de una pequeña cantidad de datos entre las aplicaciones que se ejecutan en entidades DMR que deja la gestión del formato de los datos transmitidos a las aplicaciones en sí. La DLL de DMR proporciona la transmisión de datos entre un puerto de origen y un puerto de destino de las entidades de DMR según se especifica en los campos Puerto de origen y Destino, respectivamente. (ETSI, 2008).

Datos cortos sobre PDP - Datos definidos

Datos definidos es la transmisión de una pequeña cantidad de datos entre entidades DMR con un formato de datos predefinido. (ETSI, 2008).

El paquete de datos PDP por lo anterior posibilita el desarrollo o aplicación de estos servicios. La representación de los servicios DMR para diferentes niveles se basa en la división de los servicios de telecomunicaciones en servicios de portador, servicios de telecomunicación y servicios suplementarios.

- Servicio portador: un tipo de servicio de telecomunicación que proporciona la capacidad para la transferencia de información entre las interfaces de red del usuario, involucrando solo funciones de capa baja (capas 1 a 3 del modelo OSI).
- Servicio suplementario: un servicio suplementario modifica o complementa un servicio de teleservicio o portador. En consecuencia, no se puede ofrecer a un usuario como un servicio independiente. Debe ofrecerse junto con un servicio de

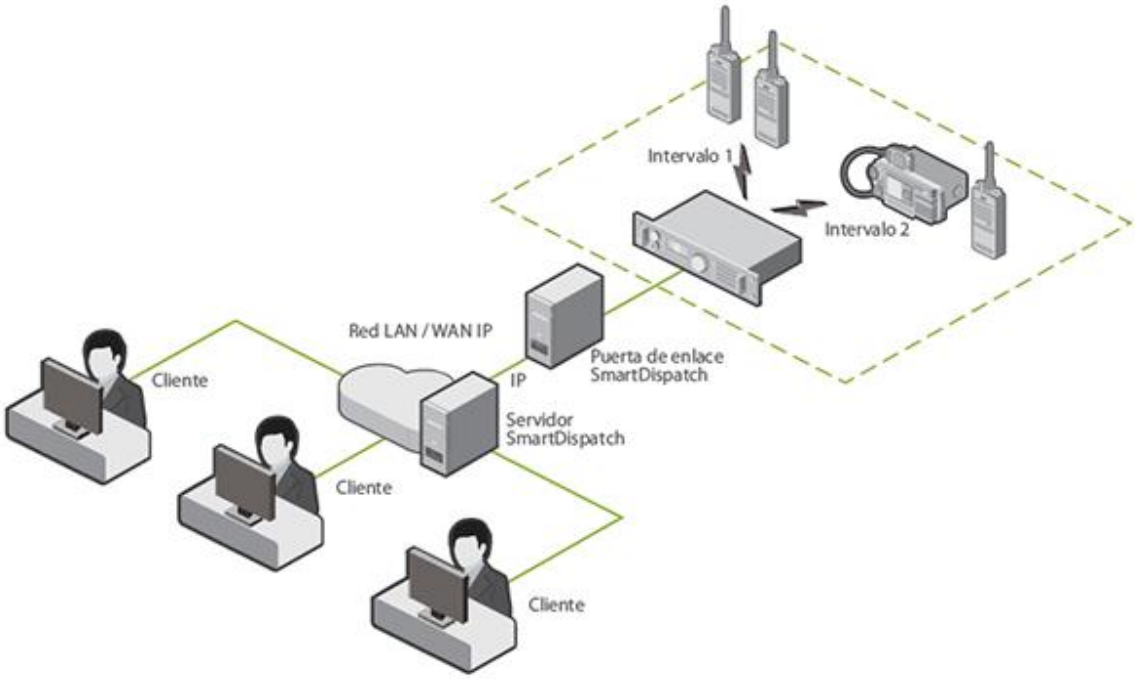
teleservicio o portador o en asociación con él. El mismo servicio suplementario puede ser común a varios servicios de telecomunicaciones.

- Teleservicio: un tipo de servicio de telecomunicaciones que proporciona la capacidad completa, incluidas las funciones de los equipos terminales, para la comunicación entre usuarios. De igual modo, se deben contemplar dos escenarios para que los servicios de telecomunicación operen según la especificación del equipo con el estándar implementado:
- Procedimiento de red: es un servicio de telecomunicaciones ofrecido por un sistema DMR para proporcionar un funcionamiento eficiente de la red.
- Característica: atributo intrínseco a una estación de radio.

4.2 Tecnologías implicadas en el protocolo DMR en la transmisión de datos

Para (Telefónica, 2011), las tecnologías implicadas en las comunicaciones son las encargadas de ofrecer capacidades a los servicios. Estas tecnologías pueden ser otros estándares o protocolos que aportan los recursos necesarios al funcionamiento de DMR en la capa de datos. Cuando se tiene un sistema de radios que usa el estándar DMR, el mapa general de la infraestructura del sistema no es más que la adaptación de los equipos existentes aplicados a las características de compatibilidad del estándar DMR con equipos que operan con tecnología TDMA. Lo anterior quiere decir que la infraestructura de DMR es similar a cualquier topología análoga que utiliza TDMA. Con el fin de entender ilustrativamente la anatomía del estándar y listar las tecnologías implicadas para ello, se ilustra la figura 4-2:

Figura 4-2: Tecnologías implicadas en DMR



Fuente: (Motorola Solutions, 2013)

En la figura 4-2 se muestra el uso de diferentes tecnologías que posibilitan el uso de los servicios, procedimientos de red y características implementadas por la especificación DMR. Por lo anterior; se pueden destacar y relacionar las siguientes tecnologías basados en la división de los servicios de telecomunicaciones vista en la anterior sección en cuanto a transmisión de datos se refiere:

Tabla 4-3: Relación de tecnología y servicio

COMPONENTE	TIPO DE SERVICIO QUE REPRESENTA	OBSERVACION
Radio digital DMR	portador	Dispositivo móvil para la transmisión de voz por radio frecuencias
Antena RF	portador	Dispositivo para la transmisión de frecuencias de radio
Canal físico	portador	12.5 KHZ
Esquema de modulación	portador	4FSK
Canal de transferencia de datos	portador	4.8 Kbps por slot
Cifrado	suplementario	ARC4/DES/AES
Repetidora DMR	Teleservicio	Repetidora: Dispositivo para interconectar y comunicar diferentes una o diferentes radios ()
mensajes de texto (datos)	Teleservicio	Mensajes de texto con una función de toque para mensajes de texto preprogramados
GPS (datos)	Teleservicio	Sistema de posicionamiento mediante el cual el operador puede ubicar la posición actual del usuario o su vehículo en el MAP 3D dimensional (3-D) digital usando Automático Software de Localización de Vehículos (AVL

COMPONENTE	TIPO DE SERVICIO QUE REPRESENTA	OBSERVACION
Telemetría (datos)	Teleservicio	Permite realizar mediciones mediante el control remoto del monitor, recibir alertas y grabar operaciones de un radio especifico.
Internet Cerro	Procedimiento de red	Red TCP/IP
Internet Sitio	Procedimiento de red	Red TCP/IP
Firewall Sitio	Procedimiento de red	Dispositivo de red para controlar la entrada y salida de tráfico en una red TCP/IP
Switch Sitio	Procedimiento de red	Dispositivo de interconexión utilizado para conectar equipos de red TCP/IP sobre redes LAN
Servidor Sitio	suplementario	Equipo de red para la centralización y guardado de información ya sean de voz o de datos
Operador Sitio	suplementario	Dispacher que monitorea y controla la red DMR en su composición

Fuente: Construcción propia

En la tabla 4-3 se pueden apreciar los componentes tecnológicos de una infraestructura DMR productiva y como se puede realizar una relación basada en el servicio que representa. (Motorola Solutions, 2013)

Las tecnologías proveen los medios necesarios para la implementación de servicios extendidos. En el caso de la transmisión de datos en DMR, los servicios basan su

despliegue en diferentes recursos tecnológicos que potencian su uso dentro del estándar. Cabe anotar que estos lineamientos son llevados mucho mas allá por otras tecnologías y servicios de uso privativo por algunas marcas que salen de los lineamientos base para mejorar temas de seguridad, compatibilidad entre terminales o por simple estrategia de mercado para ser un punto diferenciador. A continuación, son caracterizados los servicios de datos y las tecnologías para la transmisión de los datos en una cadena de conexión promedio.

Tabla 4-4: Caracterización de servicios y tecnologías

SERVICIOS DE DATOS	DESCRIPCION	EMISOR	RECEPTOR	TIPO	USO	TECNOLOGIA
mensajes de estado	Mensajes numéricos de 1 a 128	unidades	Unidades, despachador	RF, PDP, IP	Botones de pánico, alertas de estado	TDMA, IP V4, IP V6, SOFTWARE DE CONTROL+ BD
mensajes cortos de datos (mensajes de texto)	Cadena de texto de 50 caracteres	unidades con función de teclado	Unidades, despachador	RF, PDP, IP	chat, Reportes, Noticias	TDMA, IP V4, IP V6, SOFTWARE DE CONTROL+ BD
Mensajes de canal de tráfico: Confirmados y no confirmados	Datos IP o paquetes de datos	Unidades, Despachador, Aplicac.	Unidades, Despachador, Aplicac.	RF, PDP, IP	Software de monitoreo de unidades	TDMA, IP V4, IP V6, SOFTWARE DE CONTROL+ BD
Georreferenciación	Geolocalización, rastreo satelital, geocercas	unidades	Despachador	RF, PDP, IP	Posicionamiento geográfico de unidades	GPS, TDMA, IPV4, IPV6

SERVICIOS DE DATOS	DESCRIPCION	EMISOR	RECEPTOR	TIPO	USO	TECNOLOGIA
Llamada IP	Permite a las unidades establecer enlaces de voz hacia plantas de telefonía IP	Unidades	Gataway	RF, PDP, IP	Comunicación con troncales SIP	TDMA, IP V4, IP V6, SIP
Accesibilidad	Conectividad con accesorios vía Bluethoot	n/a	n/a	RF	manos libres	Bluethoot
Puente de conexión	Permite realizar puentes de conexión entre repetidoras vía IP	Repetidor	Repetidor, Aplicación	IP	Interconexión de repetidoras para aumentar la cobertura	IPSC, MBRIDGE, IPV4, IPV6
Cifrado	Permite proteger las comunicaciones en los diferentes escenarios de la cadena de conexión	Unidades, Despachador, Aplicación	Unidades, Despachador, Aplicación	IP	Aumentar la confidencialidad de los mensajes	TDMA, IP V4, IP V6, AES
Monitoreo y control	Consola de monitoreo al despachador, grabación y reproducción	Despachador	Despachador	RF, PDP, IP	Comunicación a terminales y monitoreo	TDMA, IP V4, IP V6, AES

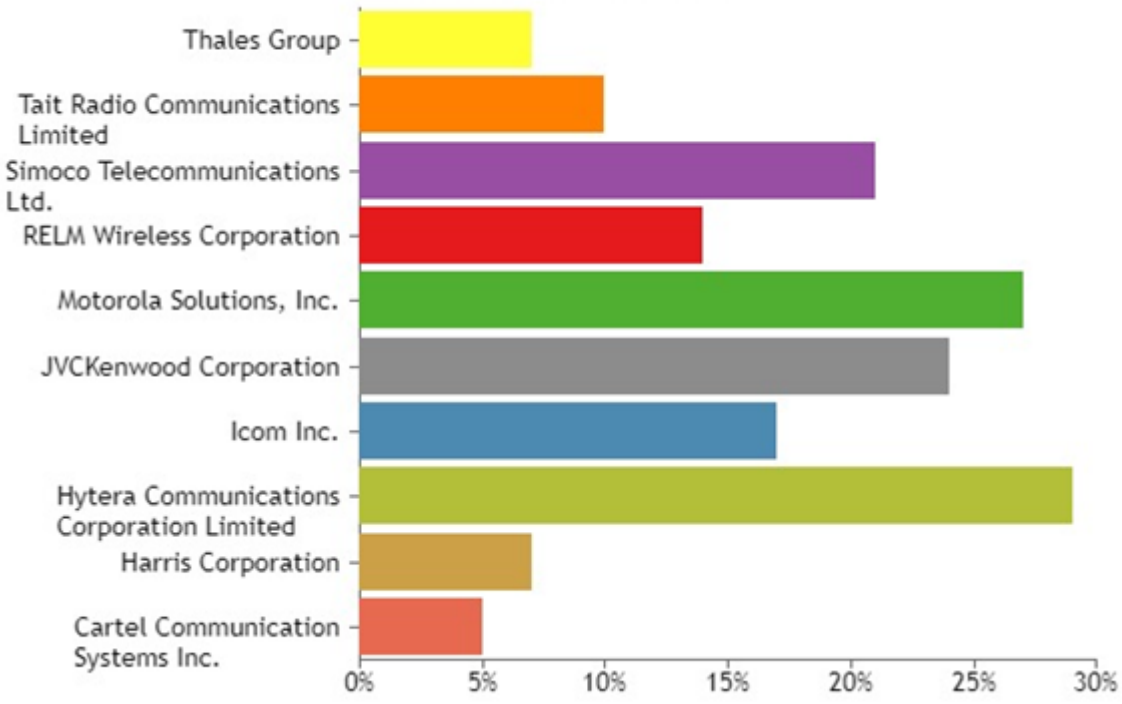
Fuente: Construcción propia

La tabla 4-4 representa por medio de la investigación que los servicios de datos tienen apoyo de tecnologías referentes dentro de la transmisión de datos. Estas tecnologías más allá de ser avaladas por el estándar pueden tener consideraciones importantes desde el punto de vista funcional y de seguridad que pueden representar afectación de la disponibilidad en algún punto de transmisión. Esto será motivo de análisis en posteriores capítulos.

4.3 Comparativo de fabricantes de radio con funciones de datos

Para tener un mapa de competitividad entre las diferentes marcas de radios y repetidoras (base primaria de DMR) se caracterizan las marcas más relevantes que han apostado por el mercado basado en estándar DMR. Para esto se realizó una búsqueda en la página oficial del desarrollador del estándar y así lograr listar los más relevantes; referenciando a los servicios, radios y repetidoras.

Figura 4-3: Caracterización de marcas en radios



Fuente: (Industry today, 2018)

En la figura 4-3 se observa que la investigación cubre el tamaño actual del mercado del mercado de la radio móvil terrestre global y sus tasas de crecimiento basadas en datos históricos de 5 años. También cubre varios tipos de segmentación, por ejemplo, por geografía [Norteamérica, Estados Unidos, Canadá, México, Asia-Pacífico, China, India, Japón, Corea del Sur, Australia, Indonesia, Singapur, Resto de Asia-Pacífico, Europa, Alemania. , Francia, Reino Unido, Italia, España, Rusia, Resto de Europa, América Central y del Sur, Brasil, Argentina, Resto de América del Sur, Oriente Medio y África, Arabia Saudita, Turquía y Resto de Oriente Medio y África], por producto / tipo de usuario final [por tipo, portátil de mano, en vehículo, por tecnología, analógico, digital, TETRA y DMR, por aplicaciones [comercial, industrial y de seguridad pública] en el mercado general. La información detallada por segmentos del mercado de Land Mobile Radio ayuda a monitorear el desempeño y toma decisiones críticas para el crecimiento y la rentabilidad. Proporciona información sobre tendencias y desarrollos, se centra en mercados y materiales, capacidades, tecnologías, ciclo de CAPEX y la estructura cambiante del mercado global de radio móvil terrestre.

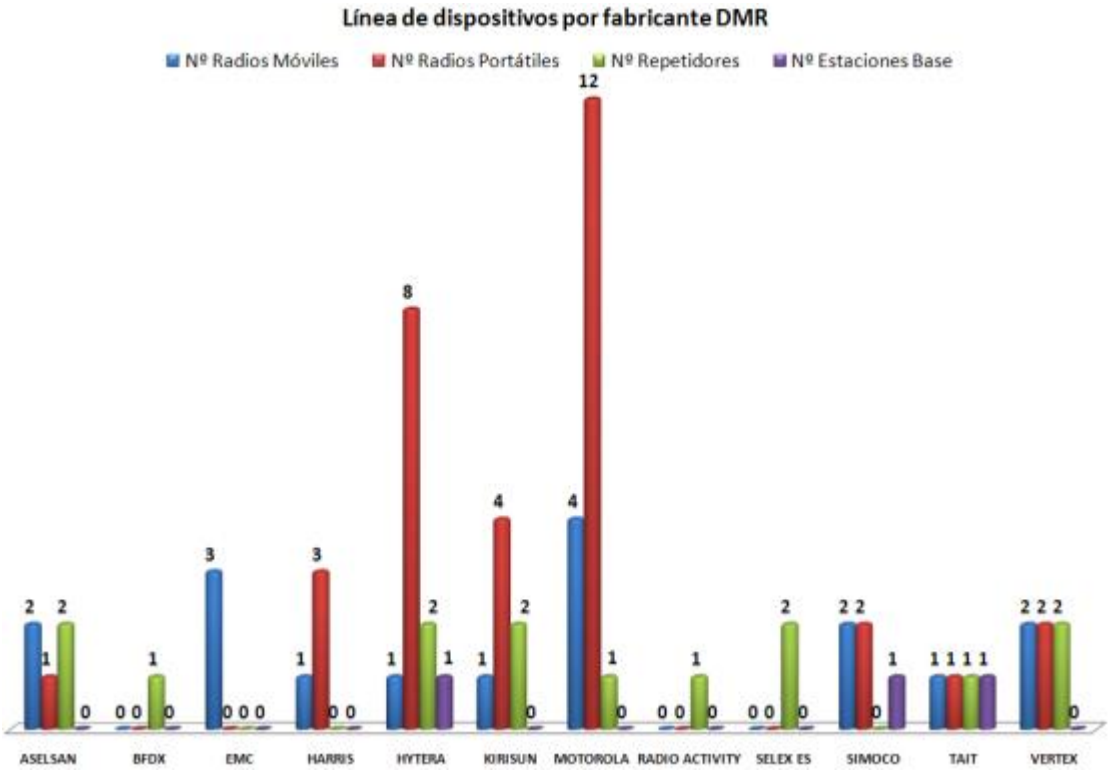
Tabla 4-5: Fabricantes relacionados a los servicios

FABRICANTE	PRODUCTOS DESPACHADOR	SOFTWARE/APLICACIONES	GRABADORAS VOZ/DATOS
AWCSL	disponible	disponible	
CATALYST	disponible	disponible	
EVENTIDE			disponible
FRIENDLY COMPANY	disponible		
HYTERA	disponible	disponible	disponible
LARIMART	disponible	disponible	disponible
MOTOROLA	disponible	disponible	disponible
SIMOCO	disponible	disponible	disponible
SMART PTT	disponible	disponible	disponible
TASSTA	disponible	disponible	disponible
NEOCOM	disponible	disponible	disponible
OMNITRONICS	disponible	disponible	disponible
TAIT	disponible	disponible	disponible
TELEX	disponible		
ZETRON	disponible		

Fuente: Construcción propia

En la tabla 4-5 se describen las marcas más representativas del mercado en cuanto a producción de equipos con el estándar DMR. De igual modo es caracterizado el fabricante con los diferentes alcances asociados a la transmisión de datos en donde son en mayor medida aplicados por las empresas como Hytera y Motorola; lo anterior se encuentra sustentado en el siguiente Comparativo de Fabricantes de radios y repetidoras:

Figura 4-4: Dispositivos por fabricantes



Fuente: (Perez, 2013)

Figura 4-5: Consolidado de fabricantes y dispositivos en el mercado

Fabricante	Línea de Dispositivos	Ancho de banda de operación		Banda de operación			
		Nº Dispositivos 12.5 kHz	Nº Dispositivos 25 kHz	Nº Dispositivos 12.5 kHz (410-430 MHz)	Nº Dispositivos 12.5 kHz (800 MHz)	Nº Dispositivos 25 kHz (410-430 MHz)	Nº Dispositivos 25 kHz (800 MHz)
ASELSAN	5	5	5	5	0	5	0
BFDX	1	1	0	1	0	0	0
EMC	3	3	1	3	0	1	0
HARRIS	4	4	0	4	0	0	0
HYTERA	12	12	11	12	0	11	0
KIRISUN	7	7	3	7	0	3	0
MOTOROLA	17	17	14	17	0	14	0
RADIO ACTIVITY	1	1	0	1	0	0	0
SELEX ES	2	2	2	2	0	2	0
SIMOCO	5	5	5	2	0	2	0
TAIT	4	4	4	0	4	0	3
VERTEX	6	6	6	6	0	6	0
Totales	67	67	51	60	4	44	3

Fuente: (Perez, 2013)

Como se muestra en la figura 4-5 se denota amplio el abanico de productos disponibles basados en DMR. Por lo que es importante tener un mayor nivel de detalle basando la exploración de acuerdo con la utilización de servicios, tecnologías y sector en forma más predomínate.

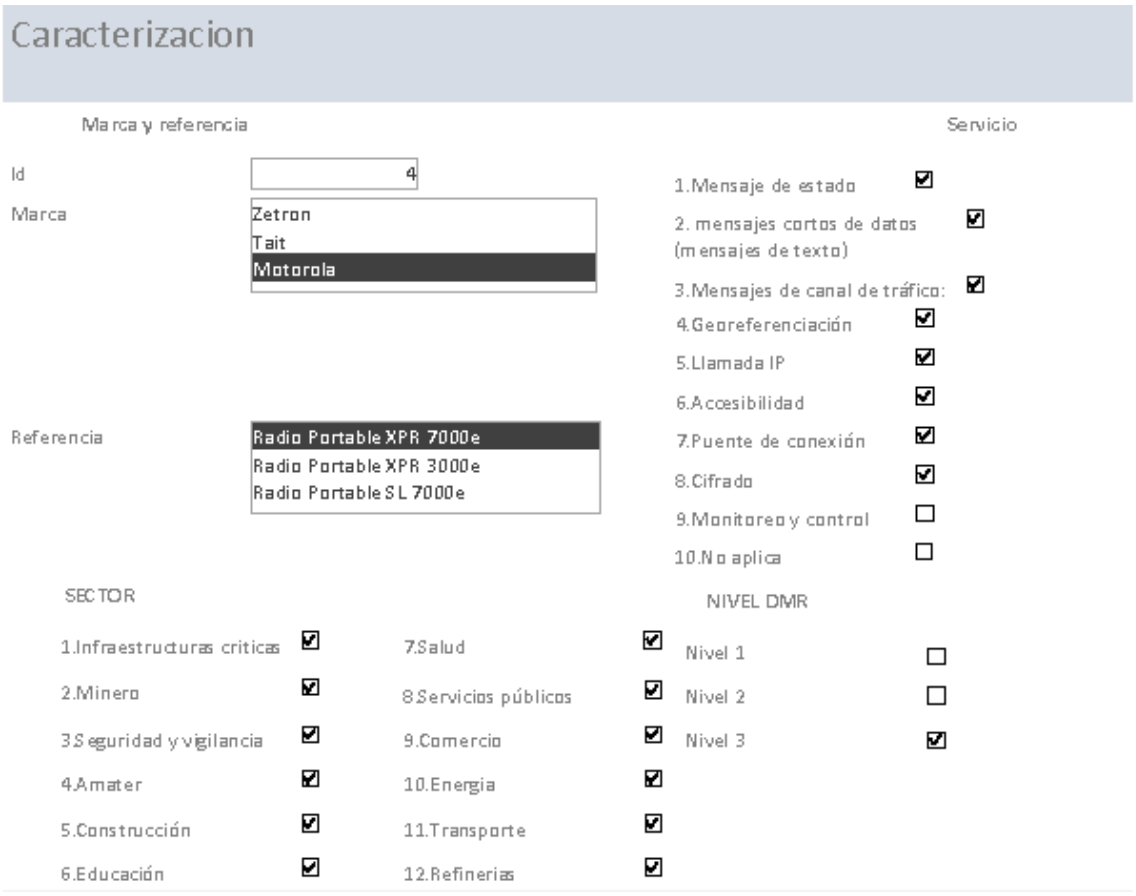
4.4 Sectores que usan protocolo DMR en la transmisión de datos

Para cada sector existen diferentes especificaciones que deben ser tenidas en cuenta para el uso de las tecnologías; ya que no son iguales las condiciones en todos los sectores económicos y las diferencias no solo son notorias en cuanto en la forma en que pueden ser distribuidos los equipos sino en las medidas de seguridad correspondientes para no poner en riesgo las comunicaciones. Por lo anterior, es necesario realizar un comparativo general de sectores y especificaciones técnicas de uso para conocer a fondo sus finalidades de acuerdo con las propiedades que ofrecen (Tait, 2015), ver Anexo L.

4.5 Caracterización del estándar DMR

Las fuentes de información proporcionan de forma general conceptos técnicos que permiten conocer cómo opera la transmisión de datos independientemente del fabricante que la adopte. Por esto es necesario abarcar un número importante de fabricantes representativos, referencias y características que permitan definir con mayor precisión aspectos predominantes de funcionamiento de los diferentes dispositivos. Para lograrlo, es aplicada la caracterización mediante el uso de una tabla general que incluye todos estos elementos y unas graficas de inteligencia de datos que representan los índices de uso de cada característica mencionada.

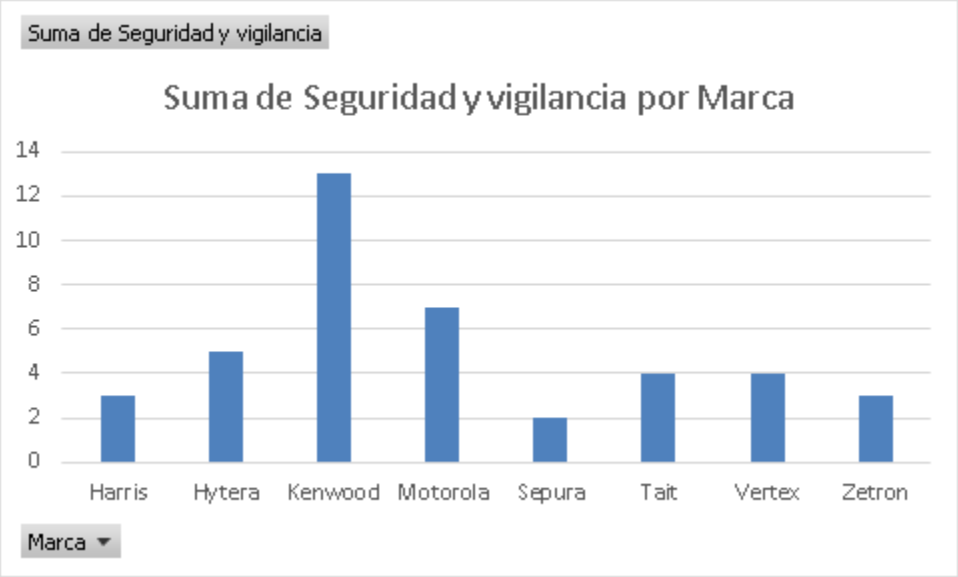
Figura 4-6: Caracterización fabricantes más relevantes



Fuente: Construcción propia

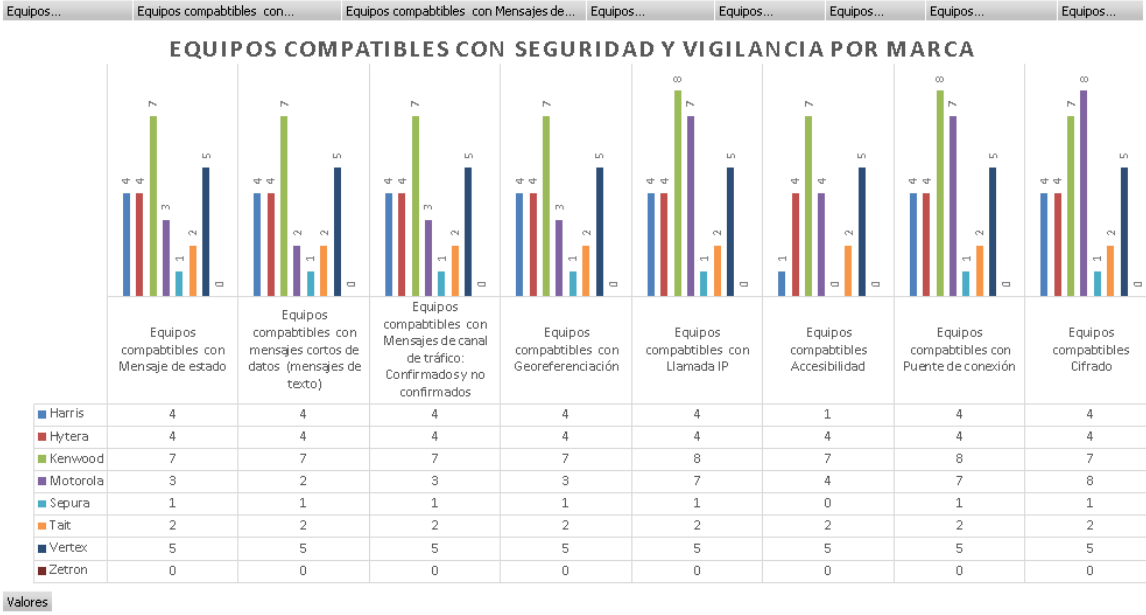
En la figura 4-6 Inicialmente se construye una base de datos con la información recolectada y las características asociadas a los radios basados en DMR; para que con el resultado se puedan evaluar datos generales de uso general y que pueda aportar elementos para orientar la investigación a la hora de evaluar las tendencias más significativas en cuanto tecnologías y servicios de los fabricantes más sobresalientes.

Figura 4-7: Indicador de equipos DMR disponibles a la seguridad y vigilancia por marca



Fuente: Construcción propia

Figura 4-8: Equipos compatibles con seguridad y vigilancia por marca



	Equipos compabtibles con Mensaje de estado	Equipos compabtibles con mensajes cortos de datos (mensajes de texto)	Equipos compabtibles con Mensajes de canal de tráfico: Confirmados y no confirmados	Equipos compabtibles con Georeferenciación	Equipos compabtibles con Llamada IP	Equipos compabtibles Accesibilidad	Equipos compabtibles con Puente de conexión	Equipos compabtibles Cifrado
Harris	4	4	4	4	4	1	4	4
Hytera	4	4	4	4	4	4	4	4
Kenwood	7	7	7	7	8	7	8	7
Motorola	3	2	3	3	7	4	7	8
Sepura	1	1	1	1	1	0	1	1
Tait	2	2	2	2	2	2	2	2
Vertex	5	5	5	5	5	5	5	5
Zetron	0	0	0	0	0	0	0	0

Fuente: Construcción propia

Los resultados de la figura 4-8 reflejan una importante tendencia de las marcas Kenwood, Vertex, Motorola y Hytera con compatibilidad en las modalidades de transmisión de datos especificadas por el estándar DMR en la muestra tomada de cada fabricante de sus referencias recientes comerciales para en varios sectores corporativos. De igual modo; es tomado el indicador del caso de estudio basado en empresas de seguridad y vigilancia privada motivo de la presente investigación y donde se observa el uso de servicios de datos en mayor medida relacionados con mensajes de texto, georreferenciación, llamadas ip y cifrado. Los resultados anteriores facilitaran la revisión detallada de estas características asociadas al nivel de riesgo en una infraestructura.

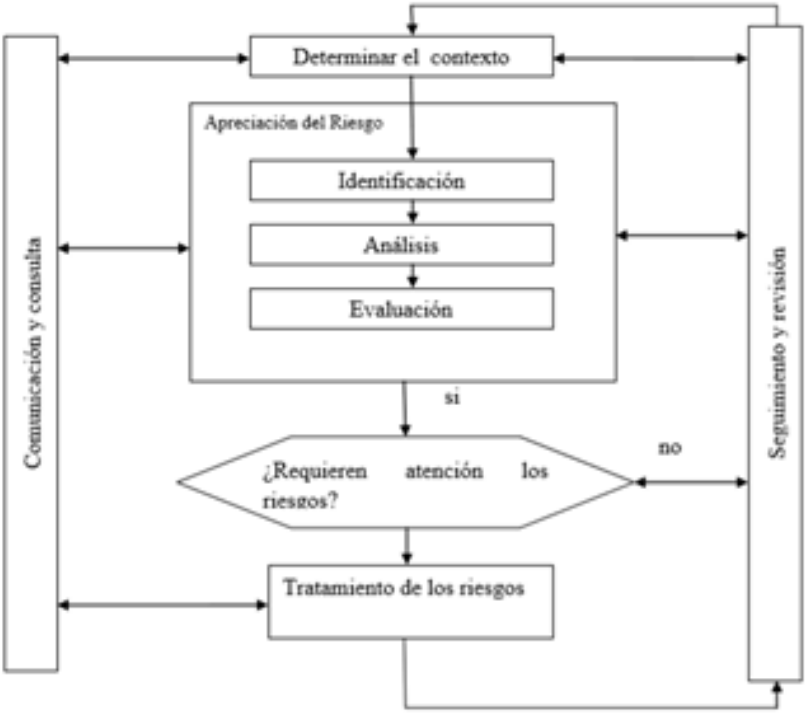
5.Capítulo 5: Análisis de riesgos para identificar ataques informáticos que generen denegación de servicio en la transmisión de datos en DMR.

Considerar un correcto análisis de riesgo dentro de la metodología propuesta, permitirá obtener un panorama de los componentes generales de una infraestructura de comunicaciones bajo el estándar DMR. Para el análisis de riesgo propuesto se busca realizar una identificación de activos de información. Luego aplicar una metodología basada en Magerit V3 “Metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno” que se encuentra alineada con la norma ISO 31000 y la ISO 27001; donde serán analizadas las vulnerabilidades y amenazas existentes. Para sugerir mecanismos de control y realizar un informe final de hallazgos que permita definir puntos de fallo y para proponer las estrategias de control para este tipo de infraestructuras.

5.1 Metodología MAGERIT para identificar los peligros y valorar los riesgos

Con el presente análisis y gestión de riesgos se pretende considerar amenazas, vulnerabilidades, ataques y salvaguardas a los que se enfrenta el estándar DMR enfocado a la disponibilidad en la transmisión de datos, teniendo en cuenta que llegar a una protección total no es posible y que el máximo grado de seguridad tampoco es el más adecuado para salvaguardar los datos. Cabe anotar que el uso de esta metodología es de carácter privado y público en general, pertenece al Ministerio de Administraciones Públicas MAP de España (Vásquez y Rocío, 2013).

Figura 5-1: Proceso de gestión de riesgos



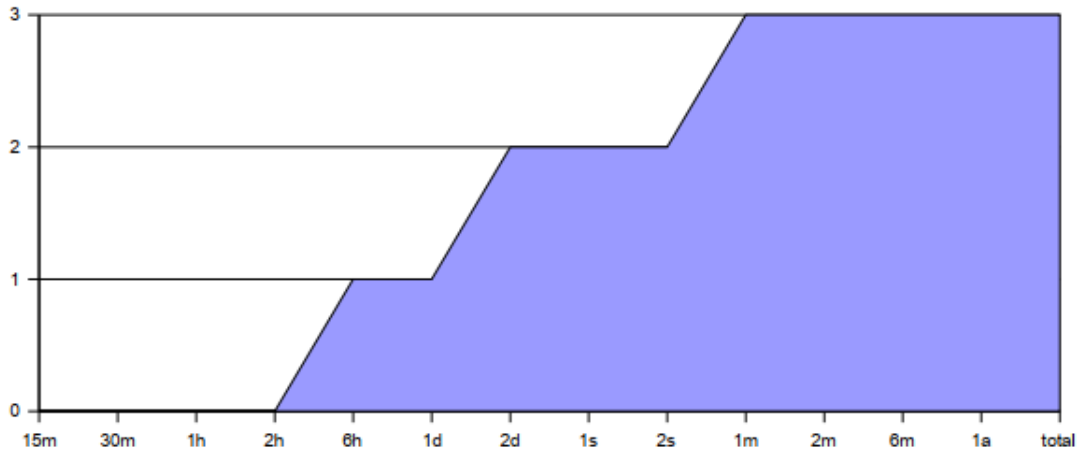
Fuente: (NTC ISO 31000, 2011)

La figura 5-1 representa el flujo del tratamiento del riesgo sobre el que se apoya Magerit v3; la cual toma cada activo de información clasificado en una matriz de acuerdo con su interrelación el valor que posee, identificando que depreciación o coste generaría en la organización. Proyecta un descubrimiento de riesgos a raíz de eventos adversos encontrados para cada activo enlistado. Posteriormente se realiza una matriz de priorización de riesgos donde el objetivo principal es evaluar el impacto que genera cada riesgo encontrado, clasificando su causa y probabilidad de reproducción. Finalmente se crean controles a partir de los riesgos encontrados se elabora un documento relacionando la forma de implementación de dichos controles y buenas prácticas de gestión de sistemas informáticos para que la organización lo utilice.

Magerit describe que no es lo mismo interrumpir un servicio una hora, un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa

un daño moderado; pero un mes detenido suponga la terminación de la actividad. Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias. (Consejo Superior de Administración Electrónica, 2012)

Figura 5-2: Relación coste contra disponibilidad



Fuente: (Consejo Superior de Administración Electrónica, 2012)

La figura 5-2 representa como un sistema puede tener problemas de disponibilidad de hasta 6 horas que se pueden asumir sin consecuencias. Pero a las 6 horas se disparan las alarmas que aumentan si la parada supera los 2 días; y si la parada supera el mes, se puede decir que la organización ha perdido su capacidad de operar. Desde el punto de vista de la remediación, la gráfica dice directamente que no hay que gastarse mucha atención por evitar paradas de menos de 6 horas. Vale la pena un cierto gasto por impedir que una parada supere las 6 horas o los 2 días. Y cuando se valore lo que cuesta impedir que la parada supera el mes, hay que poner en la balanza todo el valor de la Organización frente al coste de las salvaguardas. Para este caso pudiera ser que no valiera la pena. (Consejo Superior de Administración Electrónica, 2012).

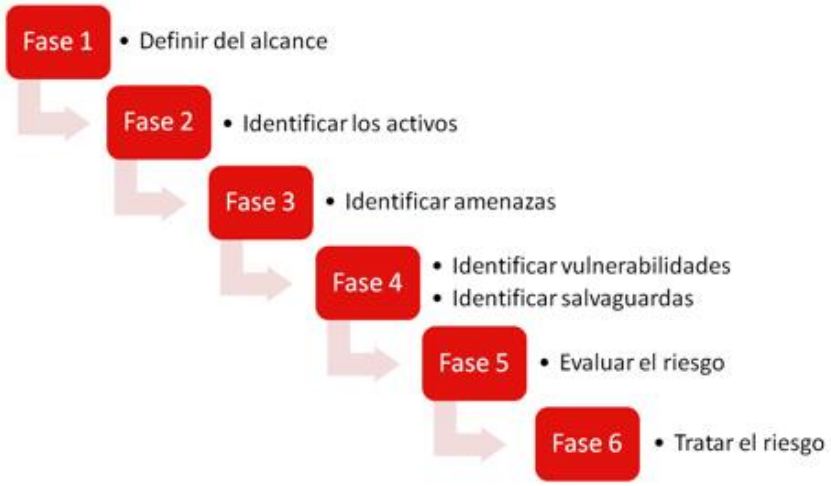
Si es evaluada la disponibilidad de tecnología DMR para la transmisión de datos se debe plantear un panorama mucho más crítico; en el que quizás minutos de inactividad en los servicios de datos deriven en un problema de seguridad para empresas de vigilancia y seguridad privada en casos especiales tales como no recibir una señal de pánico, una ubicación georreferenciada o un mensaje de texto describiendo una situación insegura.

Por lo anterior se tendrá un “apetito” del riesgo mayor en la dimensión de disponibilidad en el que se puedan analizar las causas en que los activos se puedan ver afectados para aplicar los tratamientos correspondientes.

Para realizar la gestión del riesgo basado en la metodología debe evaluarse:

- **Análisis de riesgo:** análisis general de activos y estimación de lo que podría pasar.
- **Tratamiento del riesgo:** basado en las estrategias de mitigación de los riesgos analizados para que sean llevados a nivel asumible por organizaciones o a nivel de riesgo residual.

Figura 5-3: Pasos de análisis de riesgo con MAGERIT V3



Fuente: (Consejo Superior de Administración Electrónica, 2012)

La figura 5-3 muestra el paso a paso del análisis de riesgo usando la metodología propuesta. Serán usados en forma ordenada a fin de evaluar los riesgos de los activos y proponer salvaguardas. Para ello, la metodología cuenta con la herramienta PILAR desarrollada por EAR. PILAR dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son:

- ISO/IEC 27002 (2005, 2013)- Código de buenas prácticas para la Gestión de la Seguridad de la Información.
- ENS - Esquema Nacional de Seguridad.

EAR/PILAR ha sido parcialmente financiada por el Centro Criptológico Nacional de España.

La aplicación puede descargarse libremente:

- Uso libre para consultar análisis de riesgos realizados en soporte fichero (.mgr) (modo "read only").
- Para generar nuevos análisis de riesgos se requiere una licencia comercial
- Para utilizar PILAR sobre base de datos se requiere una licencia comercial extendida.

La herramienta pilar como se mencionó anteriormente es una un software aplicado al análisis de riesgo alineado con la metodología Magerit V3. La herramienta sirve de apoyo para abordar de forma ordenada cada etapa que compone la metodología y por medio de procesos automatizados probados por el consejo de seguridad de España evaluar el nivel del riesgo y las salvaguardas sugeridas para su tratamiento.

Configuración inicial de la herramienta PILAR

PILAR inicialmente solicita información básica de configuración del proyecto. Se define por parte del analista si se realizará un análisis cualitativo o cuantitativo de acuerdo con el escenario; para el análisis de la presente investigación es usado el análisis cualitativo ya que la valoración cuantitativa podría ser tema de una investigación propia de una infraestructura específica y no general como la que se pretende evaluar. Al usar el análisis cualitativo se pretende:

- Identificar los activos más significativos.

- Identificar el valor relativo de los activos.
- Identificar las amenazas más relevantes.
- Identificar las salvaguardas presentes en el sistema.
- Establecer claramente los activos críticos (los que están sujetos a un riesgo máximo).

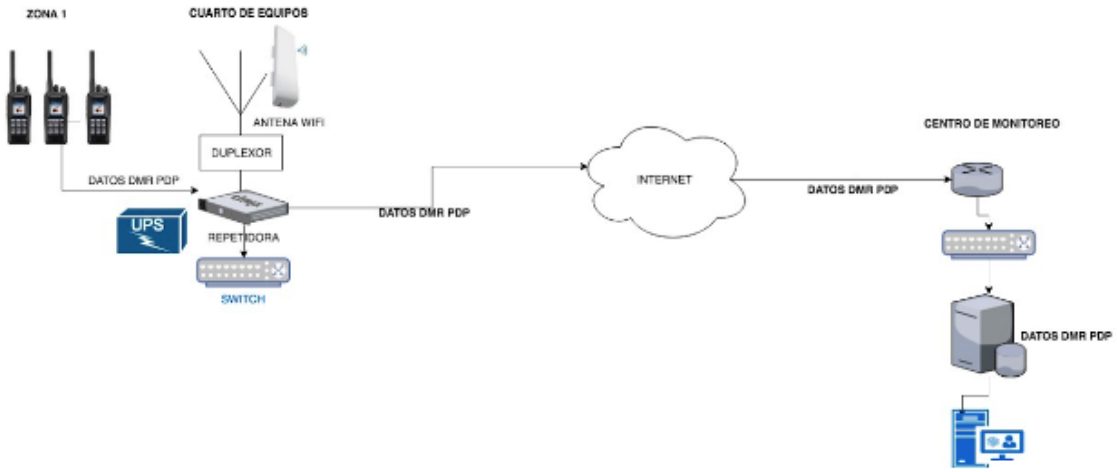
El Anexo M muestra como está compuesto el paso a paso de desarrollo del análisis de riesgo usando la herramienta. En forma estructurada, permite abordar cada paso de la metodología e ir recolectando información importante sobre los activos levantados en el escenario expuesto. Los resultados recolectados en cada fase con la aplicación serán adjuntados a partir del Anexo M al final del documento.

5.1.1 Definir el alcance

El análisis de riesgos es utilizado como una estrategia de evaluación que permite cualificar y cuantificar lo que se desee basados en la necesidad de organizar e interpretar datos científicos, facilitando decisiones para llegar a acuerdos en organizaciones o en escenarios de investigación (Consejo Superior de Administración Electrónica, 2012). MAGERIT como método cumple a cabalidad la función de analizar los servicios y tecnologías asociadas al estándar DMR, ya que brinda la rigidez y solidez necesarias para el cumplimiento del análisis de gestión de riesgos. Los elementos para la captura de datos se encuentran disponibles en el libro de catálogo de elementos de MAGERIT versión 3, las cuales facilitan la recolección de la información específica de cada uno de los activos que pueden hacer parte de una cadena de conexión productiva. Allí; será tomada en cuenta la correlación entre activos y las correspondientes dimensiones de seguridad. Luego, partiendo de estos activos se podrá determinar las amenazas, riesgos y el nivel de impacto que los activos puedan ejercer basados en la disponibilidad de servicios de datos. El nivel de seguridad será determinado por la incorporación de salvaguardas que permiten prevenir o mitigar los riesgos analizados en el análisis de gestión de riesgos.

El dominio general del análisis de riesgo es la cadena de conexión, tecnologías y servicios que permiten la transmisión de datos DMR y en donde la alteración de alguno de estos puede ocasionar indisponibilidad del sistema.

Figura 5-4: Topología de una cadena de conexión DMR estándar



Fuente: Construcción propia

El alcance esta dado por la oportunidad de realizar el Análisis y Gestión de Riesgos sobre las tecnologías y servicios implicados en DMR. Estará basado en los siguientes puntos:

- Dividir la cadena de conexión en cuatro subdominios de seguridad para un mejor análisis: Cadena de conexión, radiofrecuencia, enlace y centro de despacho.
- Aplicar el análisis basado en el riesgo de los activos de información y los posibles puntos de fallo para su debido tratamiento.
- Analizar las condiciones generales de una cadena de conexión y definir controles que permitan ofrecer niveles de disponibilidad mayores en la transmisión de datos.
- Escoger los mecanismos que permitan salvaguardar los servicios y tecnologías implicadas en la transmisión de datos DMR.

El dominio general del análisis de riesgo es la cadena de conexión, tecnologías y servicios que permiten la transmisión de datos DMR y en donde la alteración de alguno de estos puede ocasionar indisponibilidad del sistema. En una infraestructura DMR es fundamental

el análisis de riesgo usando una metodología estandarizada como Mageritv.3. Por lo anterior, será aplicado el análisis de los riesgos asociados al pilar de la seguridad de la información llamado disponibilidad por afectación de ataques intencionados o no de denegación de servicios DoS como objetivo de la investigación propuesta.

Dimensión para evaluar

[D] disponibilidad

Fuentes de información

- [F1] DMR ASSOCIATION

Sitio especializado en el desarrollo del estándar DMR

- [F2] Bibliografía

Información extraída de fuentes bibliográficas

- [F3] Investigación

Mediante la investigación del grupo de trabajo

Dominios de seguridad

- [0PRESENCIAGRL] FASE 0 PRESENCIA EN TODA LA CADENA DE CONEXIÓN

Componentes generales que tienen una influencia directa en las demás fases de conexión DMR para la transmisión de datos

- [1RADIOFREQ] FASE 1 RADIOFRECUENCIA

Equipos necesarios para la transmisión de datos por radio frecuencia

- [2TCP/IP] FASE 2 ENLACES TCP/IP

Equipos necesarios para la transmisión de datos por protocolo TCP/IP

- [3CENTDESPACHO] FASE 3 CENTRO DE DESPACHO

Equipos necesarios para la decodificación de señales de datos y toma de decisiones a nivel operativo

5.1.2 Identificar activos

Magerit basa el análisis de activos en dimensiones según la triada de seguridad de seguridad de la información: disponibilidad, integridad y confidencialidad; incluyendo la trazabilidad y el no repudio. El siguiente análisis de riesgo estará basado únicamente en la dimensión disponibilidad, en donde es realizado el cuestionamiento ¿Qué importancia tendría que el activo no estuviera disponible?, por lo tanto, los activos serán relacionados y evaluados sobre los criterios que puedan afectar la continuidad en la transmisión de datos en cada fase dentro de la transmisión de datos DMR.

Para el levantamiento de los activos se identifican un grupo general de activos que componen una infraestructura básica de transmisión de datos DMR en organizaciones dedicadas a diferentes sectores, tecnologías, servicios y afines. El formato para la identificación de realiza con base a lo recomendado en el libro II del catálogo de elementos donde se definen capas y una codificación a cada activo. El Anexo O, muestra como son agrupados los activos de información por medio de capas o características para facilitar el análisis de riesgo.

Tabla 5-1: Valorización de activos

Valoración de Activos			
Valor			**Criterio**
10	Muy Alto	MA	Daño muy grave
7-9	Alto	A	Daño grave
4-6	Medio	M	Daño importante
1-3	Bajo	B	Daño menor
0	Despreciable	D	Irrelevante

Fuente: (Consejo Superior de Administración Electrónica, 2012)

La tabla 5-1 especifica los criterios de valoración de los activos de información y las consecuencias en términos de disponibilidad si se vieran afectados. El Anexo N permite valorar los activos de acuerdo con la dimensión seleccionada. Se describe el criterio de valoración con algunas referencias de afectación y ocurrencia de materialización que sustenta la valoración propuesta.

Valoración de activos por Dominio de seguridad

Cuando se tiene la valoración de activos por dimensión se pasa a la valoración común para todos los activos en el dominio de seguridad bajo el pilar de seguridad disponibilidad. La valoración por dominio se refiere al análisis de cada fase en la que el dato viaja por la cadena de conexión y como debe ser tratado para evitar niveles de afectación del activo evaluado bajo el pilar de seguridad usado. Los activos evaluados son los incluidos en el Anexo O y la valoración usada es la de la tabla 5-2 valoración de activos. La descripción de cada ítem en el Anexo P sustenta los criterios de evaluación usados.

Tabla 5-2: Valoración de dominios

Dominio de seguridad	Valoración disponibilidad [D]
[0PRESENCIAGRL] FASE 0 PRESENCIA EN TODA LA CADENA DE CONEXIÓN	[MA]
[1RADIOFREQ] FASE 1 RADIOFRECUENCIA	[MA]
[2TCP/IP] FASE 2 ENLACES TCP/IP	[MA]
[3CENTDESPACHO] FASE 3 CENTRO DE DESPACHO	[MA]

Fuente: Construcción propia

La tabla 5-2 muestra los resultados de evaluación final por dominio de seguridad que toma como referencia la valoración más alta que tuvo el activo y debe ser considerado para todos los demás activos que componen el dominio. En este caso, al existir activos con evaluación [MA] en cada dominio, debe ser considerada esta valoración en cada fase en forma general.

5.1.3 Identificar amenazas

El origen de cada una de las amenazas utilizadas es definido en la metodología MAGERIT y forman parte del catálogo de amenazas incluido en el libro 2 (Consejo Superior de Administración Electrónica, 2012). En este apartado se realiza el cuestionamiento de cuál es la probabilidad de materialización y cuan perjudicado resultaría el activo al materializarse la amenaza. La valoración es usada de acuerdo con el Anexo N y la valoración de activos y los resultados pueden ser validados en el G. Anexo: Amenazas y sus factores agravantes en la herramienta PILAR.

El Anexo X muestra las amenazas de los activos, probabilidad de ocurrencia y la afectación si se materializa la amenaza. Sobresalen las más relevantes para el tema de investigación propuesto:

[I.4.31] Jamming

Sabotajes jammers o perturbadores. Ataques de interrupción DoS, dispositivos caza frecuencias. Uso de aparatos que perturban el espectro radioeléctrico para neutralizar o provocar el mal funcionamiento de las comunicaciones impactando la disponibilidad

[E.1] Errores de los usuarios

Insiders o factor humano. Falta de procesos procedimentales claros y rigurosos de control de terminales de radio que permitan su baja inmediata en caso de robo o de pérdida de estos para evitar el uso por parte de personas u organizaciones mal intencionadas

[A.5] Suplantación de la identidad

Ataques de imitación o confusión. Emisión de señales con el objeto de engañar a los receptores dando una información falsa, confusa y contradictoria.

[A.10] Alteración de secuencia

Ataques de grabación y reproducción. Grabar señales producidas por los terminales DMR para reproducir comportamientos provocando un comportamiento inseguro y logrando la desconexión de algún elemento que afecte la disponibilidad del servicio.

[A.14] Interceptación de información (escucha)

Interceptación de comunicaciones sensibles. Todo lo que viaja por el aire corre el riesgo de ser captado o descifrado; esta amenaza impacta la disponibilidad cuando se capta información por un tercero y no llega al destino correcto.

[A.19] Revelación de información

Enumeración de objetivos y recopilado de información. Información revelada por las organizaciones a terceros que menciona las condiciones generales de su red DMR y puede ser indexada por los diferentes buscadores de internet brindando al atacante la información necesaria para iniciar un ataque que afecte la disponibilidad del sistema objetivo.

[A.24] Denegación de servicio

- Afectación de la integridad de la información puede afectar la disponibilidad del sistema al no contar con la información precisa cuando se requiera.
- Sabotajes en las señales producidas.
- Imitación y confusión.

5.1.4 Identificar vulnerabilidades y salvaguardas

Un impacto es el daño que causa o que se puede causar sobre el activo derivado de la materialización de una amenaza. La tipificación de los impactos puede variar de acuerdo con el proyecto. Para efectos de la metodología de detención de intrusos en radio DMR que afecten la disponibilidad de datos se presenta y se evalúan los impactos de acuerdo con la parte técnica del estándar y de los componentes de infraestructura.

Figura 5-5: Potencial del impacto y el riesgo

IMPACTO /RIESGO POTENCIAL		DEGRADACIÓN				
		MB	B	M	A	MA
ACTIVO	MA	M	M	A	MA	MA
	A	B	M	A	MA	MA
	M	B	B	M	A	A
	B	MB	B	B	M	A
	MB	MB	MB	MB	B	B

Fuente: (Consejo Superior de Administración Electrónica, 2012)

La figura 5-6 representa un mapa de calor que permite clasificar el activo según la valoración ver Anexo O y ubicarlo en la sección de impacto tabla 5-6. Es decir, si el activo tuvo una valoración en el Anexo N de [MA] y el impacto evaluado en la tabla 5-6 fue [MA], el activo debe ser ubicado en el mapa de calor con riesgo alto y deben ser propuesta salvaguardas para mitigar el riesgo.

En el Anexo AM se muestra el impacto potencial que es la medida de daño a raíz de la materialización de una amenaza, esta materialización se da sobre el activo. El cálculo de este valor se toma a partir del valor de la degradación en la dimensión disponibilidad y el valor del activo; luego, son marcados los valores según el mapa de calor elaborado.

El Anexo AN muestra el riesgo al que están expuestos los activos que es la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos realizado anteriormente, es directo derivar el riesgo sin necesidad de tener la probabilidad de ocurrencia y son marcados los valores según el mapa de calor elaborado.

Caracterización salvaguardas

Por definición de Magerit: “Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se mitigan con buenas prácticas, otras requieren de elementos técnico (programas o equipos), otra seguridad física y, por último, está la política de personal.” (Consejo Superior de Administración Electrónica, 2012) La caracterización de las salvaguardas consta de dos fases: Identificación de las salvaguardas y Valoración de las salvaguardas.

Para identificar las salvaguardas existentes y proponer nuevas salvaguardas, MAGERIT proporciona un catálogo de salvaguardas de acuerdo con las recomendaciones de la ISO/IEC 27001, y 27002.

Las salvaguardas se caracterizan, además de su existencia, por su eficacia frente al riesgo que pretenden conjurar.

Tabla 5-3: Criterios de salvaguardas

Eficacia	Nivel	Madurez	Estado
0%	L0	inexistente	inexistente
10%	L1	inicial/ad hoc	iniciado
50%	L2	reproducible pero intuitivo	parcialmente realizado
90%	L3	proceso definido	en funcionamiento
95%	L4	gestionado y medible	monitorizado
100%	L5	optimizado	mejora continua

Fuente: (Consejo Superior de Administración Electrónica, 2012)

El Anexo AD muestra la valoración estado inicial y madurez de las salvaguardas en la herramienta PILAR, muestra el nivel de madurez al que puede llegar una salvaguarda o medida tomada para mitigar el riesgo. Son seleccionadas las salvaguardas generales para cada dominio de la cadena de conexión.

El Anexo M muestra las salvaguardas seleccionadas que mitigan el riesgo a valores asumibles por la organización y son planteados los niveles de madurez inicial y recomendado según la tabla 5-8 Criterios de salvaguardas.

Se destacan como principales salvaguardas la protección de las comunicaciones y los sistemas de detección de intrusos en cada fase de conexión que apoyan la gestión del riesgo por su valor en reconocimiento temprano de anomalías en infraestructuras productivas DMR y motivan la realización de la metodología propuesta.

Evaluar el riesgo

Tras aplicar salvaguardas a los activos podemos validar la reducción del riesgo especifico según el dominio de seguridad:

Tabla 5-4: [S.3rd] contratado a una tercera parte

Activo	[Potencial]	[Estado inicial]	[Salvaguardas]
[FRQRADIO] FRECUENCIAS DE RADIO	MA	M	B
[SERVINTERNET] SERVICIO DE INTERNET PARA ENLACES	M	M	B

Fuente: construcción propia

Tabla 5-5: [COM] Redes de comunicaciones

Activo	[Potencial]	[Estado inicial]	[Salvaguardas]
[G1] Componentes de conectividad	MA	A	B
[ROUTER] ROUTER	A	M	B
[ACCPOINTWIFI] ACCESS POINT WIFI	A	M	B
[SWITCH] SWITCH	A	B	B
[FIREWALL] FIREWALL	A	M	B
[RDIOFRE] RF	MA	A	B
[G3] Componentes de Infraestructura	MA	A	B

[RADIODMR] RADIOS DMR	M	M	B
[REPETIDORADMR] REPETIDORA DMR	MA	M	B
[DUPLEXOR] DUPLEXOR	A	M	B
[ANTENARX/TX] ANTENA RX/TX	A	M	B
[LAN] RED DE DATOS	A	A	B
[CABLEADO] CABLEADO	M	M	B

Fuente: construcción propia

Tabla 5-6: [TechyProt] Tecnologías o protocolos en DMR

Activo	**[Potencial]**	**[Estado inicial]**	**[Salvaguardas]**
[TRAMATCP] PAQUETE DE DATOS DE RED	MA	M	B
[TDMA] TDMA	A	A	B
[4FSK] 4FSK (MODULACIÓN CUARTO NIVEL)	M	M	B
[Bluethoot] Bluethoot	M	B	B

[GPS] GPS	A	M	B
[AES] AES	M	B	B
[PDP] PDP	MA	A	B
[PROTTCP] PROTOCOLO TCP	A	A	B
[PAQDIGITALESRF] PAQUETES DIGITALES RADIOFRECUENCIA DMR	MA	A	B
[PROTUDP] PROTOCOLO UDP	M	B	MB

Fuente: construcción propia

Tabla 5-7: [Dat] Servicio de datos

Activo	**[Potencial]**	**[Estado inicial]**	**[PILAR]**
[GEOREFER] Georreferencia	A	M	B
[MENSTEXTO] Mensaje de texto	A	M	B
[TELEMETRIA] Telemetría	A	M	B

Fuente: construcción propia

Tabla 5-8: [E] Equipamiento

Activo	[Potencial]	[Estado inicial]	[PILAR]
[SW] Aplicaciones	A	B	B
[ANTIVIRUS] SOFTWARE ANTIVIRUS ESTACIONES-SERVIDOR	A	B	B
[SOFTDESPACH] SOFTWARE GESTION DMR DESPACHADOR	M	MB	MB
[SISTOERATIVO] SISTEMA OPERATIVO ESTACIONES-SERVIDOR	M	MB	MB
[MOTBASEDATOS] MOTOR BASE DE DATOS EVENTOS DE DATOS	M	B	B
[PCS] Equipos Finales	A	B	B
[SERVMONITOREO] SERVIDOR MONITOREO	A	B	B

[PC] ESTACIÓN DE TRABAJO (PC)	A	B	B
[AUX] Elementos auxiliares	M	M	MB
[UPS] UPS	M	M	MB

Fuente: construcción propia

Tabla 5-9: [L] Instalaciones

Activo	**[Potencial]**	**[Estado inicial]**	**[PILAR]**
[ESTACIONBASE] ESTACIÓN BASE	MA	M	B
[DATACENTER] DATACENTER	MA	M	B
[CENTRAL_MONITOREO] CENTRAL_MONITOREO	MA	M	B

Fuente: construcción propia

Tabla 5-10: [P] Personal

Activo	[Potencial]	[Estado inicial]	[PILAR]
[USERDESPACHADOR] DESPACHADOR MONITOREO	M	M	B
[ADMRED] Administrador de red interna	A	A	B
[ADMDMR] Administrador de infraestructura DMR	M	M	B
[USRRADIO] USUARIO RADIO	M	M	B

Fuente: construcción propia

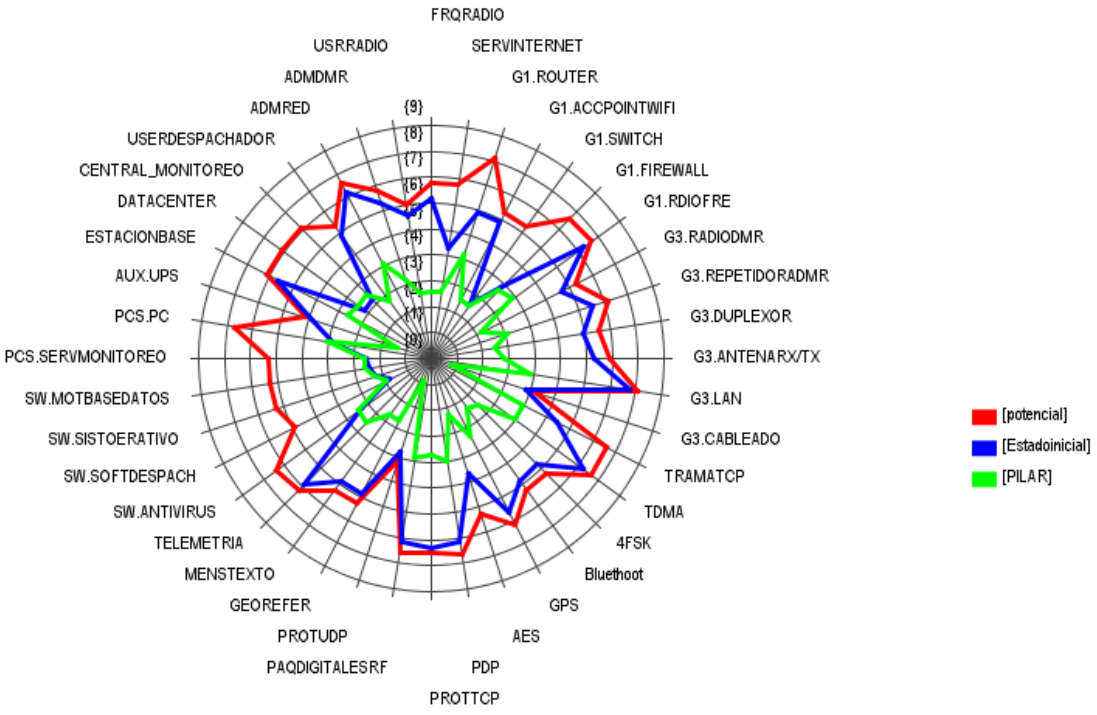
Análisis de resultados

Los resultados que se muestran de las tablas 5-4 a la 5-10, clasifican inicialmente los activos en los dominios de seguridad y evalúan la efectividad de las salvaguardas propuestas de la tabla 5-3. Esta efectividad es valorada en dos estados o momentos que son cuando se instaura la medida de mitigación y el estado Pilar o estado de madurez de la medida que muestra una reducción considerable del nivel del riesgo e invita a una fase superior que se refiere a una mejora continua según los lineamientos de la norma ISO 31000 y el ciclo PHVA que sugieren las normas ISO.

Después de haber realizado el análisis de riesgos quedan a la vista los impactos y los riesgos a los que está expuesta una cadena de conexión de datos DMR, y estos son una medida del estado al que puede estar expuesto un escenario productivo sin ningún tipo de

control, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores manejables.

Figura 5-6: Valoración de los riesgos potenciales



Fuente: Construcción propia

La figura 5-6 tipo radar, concentra el resumen general de análisis de riesgo propuesto en cada etapa y muestra como fue inicialmente valorado el riesgo (potencial) de cada activo en cada etapa hasta logar la reducción a un nivel asumible (estado inicial) que permite mejorar los niveles de disponibilidad al ser aplicadas las medidas o controles sugeridos (pilar). La elaboración del análisis de riesgo apoyado de la metodología Magerit V.3 para determinar el nivel del riesgo al que están sometidos los activos de una cadena de conexión DMR sensible a ataques de denegación de servicio que afectan la disponibilidad, arrojó resultados que muestran la necesidad de abordar con detenimiento las posibles afectaciones que tendrían los activos en una infraestructura productiva y las medidas de tipo técnico y procedimental que deben ser aplicadas por los administradores de dichos

recursos para evitar impactos que incidan en la transmisión de datos. Fueron mostrados los activos que pueden estar más expuestos mediante el análisis por etapas como el caso de la transmisión por radio frecuencia, las tramas de paquetes y el protocolo de paquete de datos; elementos fundamentales en la transmisión adecuada de los datos y que le da un mayor valor a la metodología propuesta para identificar y dar respuesta ante eventos de intrusión de denegación de servicio que pueden afectar la disponibilidad.

6.Capítulo 6: Proceso de realización de la metodología orientada a la detección de DoS en las comunicaciones basadas en el estándar DMR que contenga las posibles alternativas de protección y respuesta

Una metodología es una secuencia sistémica de etapas cada una de las cuales incluye acciones o procedimientos dependientes entre sí y que permiten el logro de determinados objetivos (URIZARRI, 2006); basado en lo anterior, la presente metodología integral, se desarrolla mediante un enfoque Top-Down (de lo general a lo particular), es decir, partiendo de una infraestructura productiva DMR en la que se trasmiten datos que están expuesta a diferentes tipos de ataques generales de denegación de servicio evaluados anteriormente hasta la verificación particular de ataques. Para cada una de las fases se debe:

Fase de identificación: Se hace un levantamiento de los activos relacionados en infraestructura DMR analizada. Como un proceso de gestión de riesgos orientada a la dimensión disponibilidad, los activos son fundamentales a la hora de la identificación de posibles vulnerabilidades que puedan ser explotadas y generar DoS.

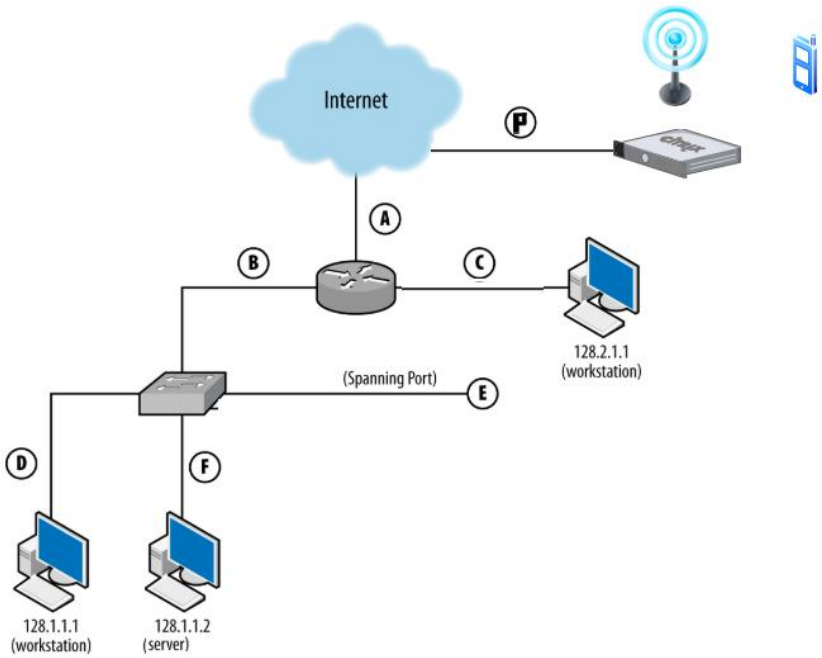
Fase de clasificación: según la caracterización de activos y el análisis de riesgo se deben ubicar los activos en un dominio de seguridad que será la etapa de envió del paquete de datos. Son consideradas tres etapas o momentos de transmisión de los datos en DMR: radio frecuencia, enlace de datos y área local. Los activos que permiten la transmisión de los datos deben ser asociados a estas fases que tienen características de detección diferentes a fin de poder gestionara detección adecuada de ataques DoS.

Fase comunicación: Se debe realizar una identificación de las fases de trasporte (protocolos y componentes) hasta los activos finales de la infraestructura.

- Para cada protocolo identificado es necesario establecer posibles fallas y amenazas que puedan generar DoS. Se recomienda el uso de metodologías de análisis de seguridad como Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM) que se centra en qué probar en lugar de como probarlo y se puede adaptar a varios tipos de pruebas, incluidas las evaluaciones de vulnerabilidad, las pruebas de penetración, las auditorías de caja blanca y más; estos serán insumos clave para la definición de las reglas de los sensores.

Fase sensores: En la etapa de implementación se requiere ubicar los sensores en las zonas de concentración de tráfico para validar el comportamiento. Para esto, se debe realizar un mapa de la red, determinar los puntos ventajosos potenciales y luego determinar la cobertura óptima.

Figura 6-1: Puntos de implementación de sensores



Fuente: Construcción propia

En la figura 6-1 se puede notar:

Sensor P: Supervisa el espacio radioeléctrico y variaciones en la transmisión

Sensor A: Monitoriza la interfaz que conecta el enrutador a internet.

Sensor B: Supervisa la interfaz que conecta el enrutador al switch.

Sensor C: Supervisa la interfaz que conecta el enrutador al host con la dirección IP 128.2.1.1 usado como correlacionar eventos.

Sensor D y G: Monitores host

Sensor E: Supervisa por medio de un puerto en modo espejo operado por el switch de red. Se debe ajustar un puerto en modo espejo que permita el registro de todo el tráfico que pasa por el switch.

- Una vez identificados los posibles escenarios dentro de la infraestructura y protocolos, es necesario establecer en dónde se deben fijar sensores de detección de ataques.

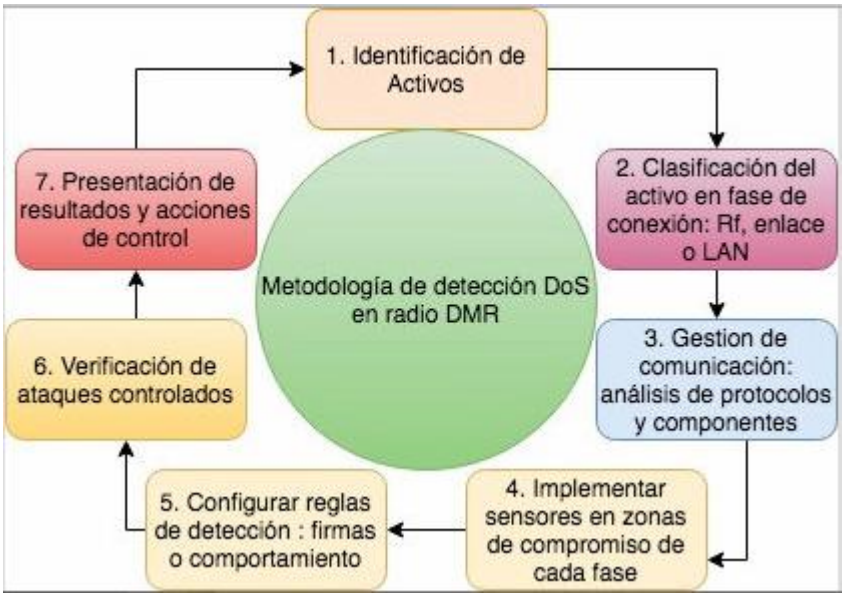
- **Implementar dichos sensores:** Es necesario establecer cual herramienta para la detección de intrusos (ataques de tipo DoS) pueden ser implementadas. Las áreas de concentración de tráfico para los sensores serian:
    - **Radiofrecuencia:** zona de concentración de tráfico ubicada entre la repetidora DMR y las terminales de radio haciendo uso de un dispositivo de captura de trafico de señales usando SDR (software definida por radio) con las herramientas estudiadas anteriormente; servirá de sniffer de red y evaluará comportamientos generales del espectro teniendo en cuenta el comportamiento ante los ataques DoS evaluados en fase de comunicación.
    - **Enlace:** Sensores ubicados entre las conexiones sitio a sitio haciendo uso de Snort definido por firmas y comportamiento.
    - **Lan:** Sensores ubicados en switch, servidores y equipos finales, haciendo uso de Snort definido por firmas y comportamiento para olfatear de la red local y OSSET para estaciones finales.

Fase configuración: Lo siguiente es realizar una configuración de reglas de detección en los sensores, dichas reglas están asociadas a las posibles amenazas para DoS identificadas. Se debe establecer el tipo de acuerdo con elección que se usará de acuerdo con el momento de conexión que puede ser basado en firmas (Enlace o LAN) o por comportamiento (radiofrecuencia).

Fase verificación: En la verificación de los ataques y los resultados, se hace un compendio de lo identificado a través de alguna prueba de concepto, generando diferentes ataques DoS sobre DRM y validando los resultados obtenidos.

Fase de resultados y acciones de control: Presentar la información sobre todos los fenómenos observados por los sensores. Esta información es útil para desarrollar firmas y alertas para fenómenos que aún no se han configurado para definir sensores de alerta y bloqueo. Esta sería la función del correlacionador de eventos AlienVault OSSIM™ que registraría todos los datos de los sensores implementados.

Figura 6-2: Esquema metodológico



Fuente: Construcción propia

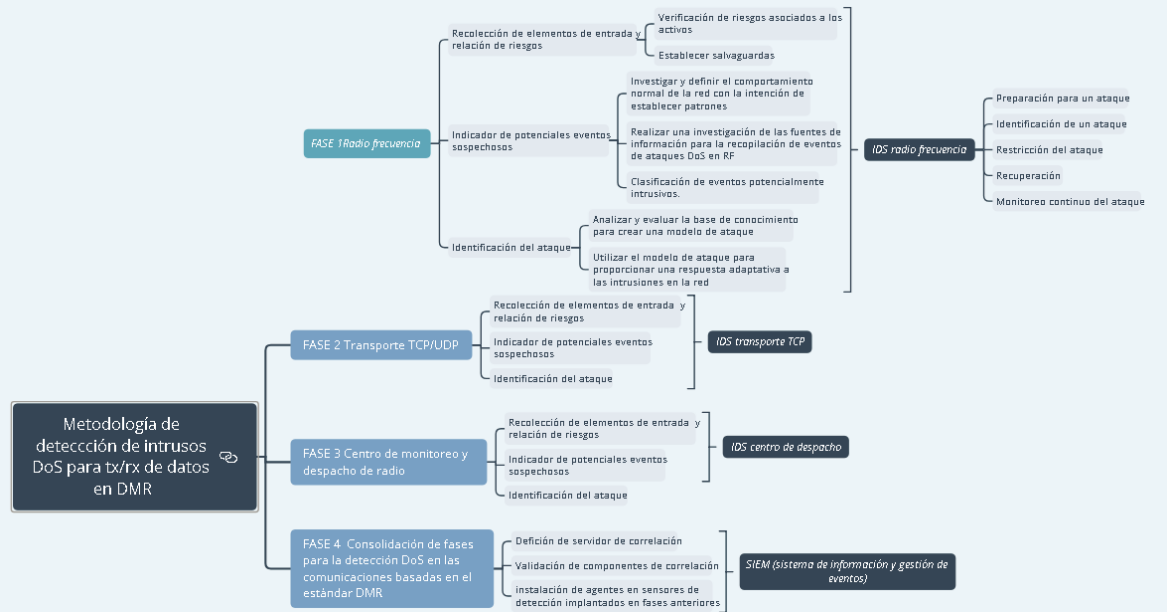
La figura 6-2 representa la metodología que aborda el diseño de estrategias de control resistentes y conscientes de los recursos de las comunicaciones basadas en DMR y de los componentes de red sujetos a ataques maliciosos de denegación de servicio (DoS). En particular, la estrategia de detección y respuesta planteada para estas comunicaciones es un esquema de control desencadenado por eventos previamente configurados, basada en activos que están sujetos a perturbaciones que limitan la transmisión de datos, generando con ello, indisponibilidad. El marco propuesto, son aquellos escenarios con presencia de perturbaciones y ataques DoS que inciden directamente en la disponibilidad de las comunicaciones DMR. Los ataques DoS están restringidos en términos de frecuencia y duración, así como el nivel de indisponibilidad que genera al sistema afectado.

La estructura interna del sistema de detección propuesto es:

- **Fuente de información:** Sensores en fases de conexión
- **Estrategia de análisis:** Detección de anomalías supervisadas y de uso indebido.
- **Aspectos temporales:** Predicción en tiempo real
- **Arquitectura:** heterogénea distribuida
- **Reacción:** Activa de tipo correctiva
- **Continuidad:** Monitoreo continuo con correlación de eventos

6.1 Mapa conceptual de la metodología

Figura 6-3: Metodología propuesta



Fuente: Construcción propia

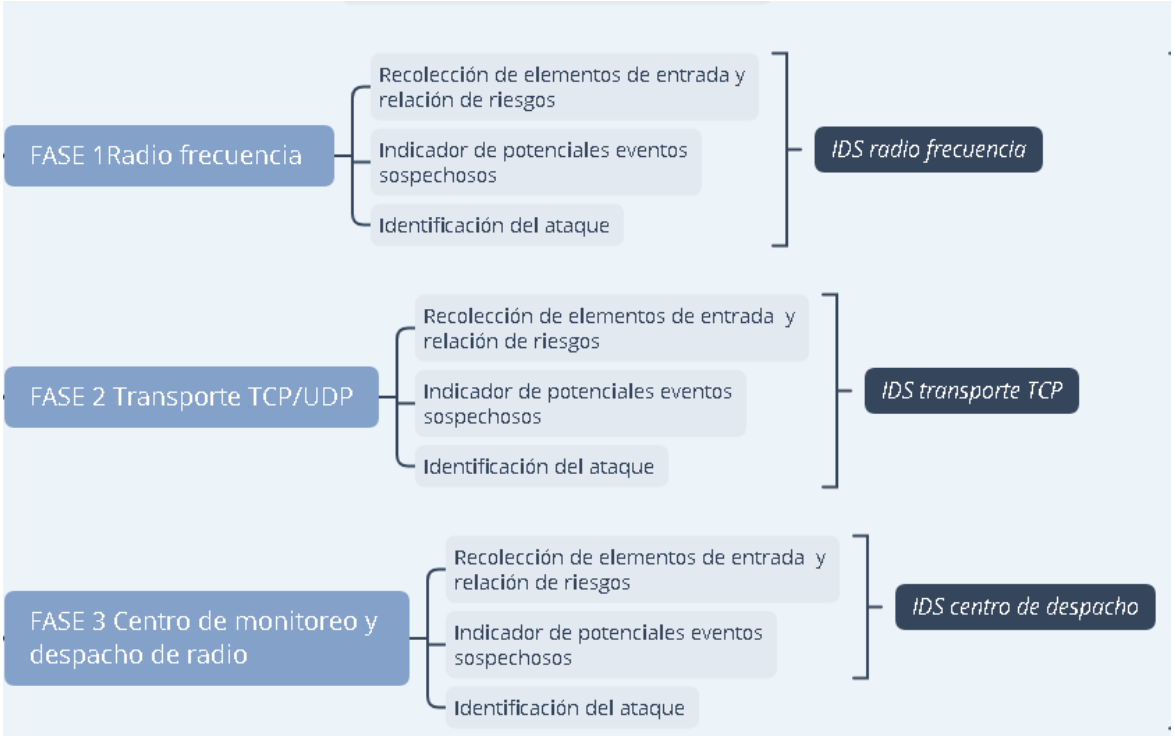
En la figura 6-3 se puede apreciar cómo se desarrolla la metodología la cual se basa en el estudio general de la cadena de conexión de la transmisión y recepción de los datos en DMR y que se desglosa en cuatro fases o momentos de conexión llamadas fase 1 o de radio frecuencia, fase 2 o de trasporte TCP/UDP, fase 3 o de centro de monitoreo o despacho de radio y fase 4 de correlación de del sistema de detección basado en los resultados obtenidos. En cada fase son caracterizados los activos y las salvaguardas que permiten tratar ataques DoS por medio de sistemas de detección de intrusos IDS y buenas prácticas de implementación.

Figura 6-4: Proceso de iniciación

Fuente: Construcción propia

Como se muestra en la figura 6-4 inicialmente se plantea un análisis introductorio de toma de conciencia de las amenazas existentes en escenarios como el propuesto que, aunque es poco explorado guarda consigo diferentes amenazas que pueden materializarse y generar interrupciones de servicios de transmisión o recepción de datos que son considerados claves para la operación de empresas que prestan vigilancia y seguridad privada. Para esto se entrarán a definir roles, dominios de seguridad y clases de activos para que puedan ser valorados según el riesgo evaluado de los componentes de una infraestructura en etapa de producción o si por el contrario se plantea la especificación de una nueva siguiendo los lineamientos propuestos.

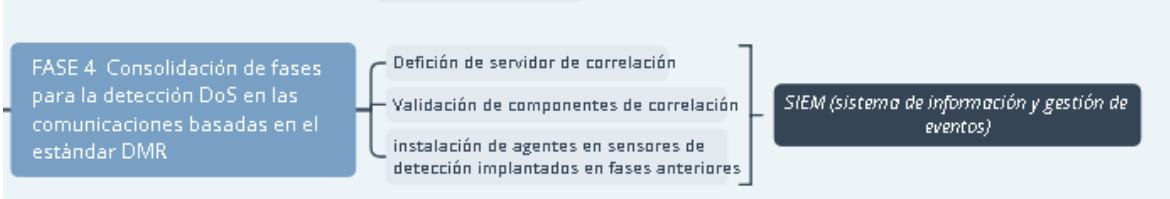
Figura 6-5: Fases de la metodología



Fuente: Construcción propia

En la figura 6-5 se muestran las demás etapas que plantean un escenario que separa cada momento en que el dato se transmite y viaja por la cadena de conexión para realizar un análisis con mayor precisión y validar la pertinencia del tratamiento sugerido y la posterior implementación del sistema de detección; en donde se hace claridad que no es solo una herramienta como se conoce en la seguridad informática, sino que detrás de esta deben existir componentes que deben ser considerados para su desarrollo y funcionamiento de forma efectiva.

Figura 6-6: Fase de consolidación



Fuente: Construcción propia

En la figura 6-6 se muestra la última fase que consiste en consolidar la información de las etapas de la metodología y generar una propuesta general para tratar ataques DoS que afecten la transmisión de datos en cadenas de conexión DMR, teniendo en cuenta que quien la implemente pudo elegir libremente en qué fase hacer un mayor hincapié de acuerdo con los activos, los controles y las técnicas de detección sugeridas.

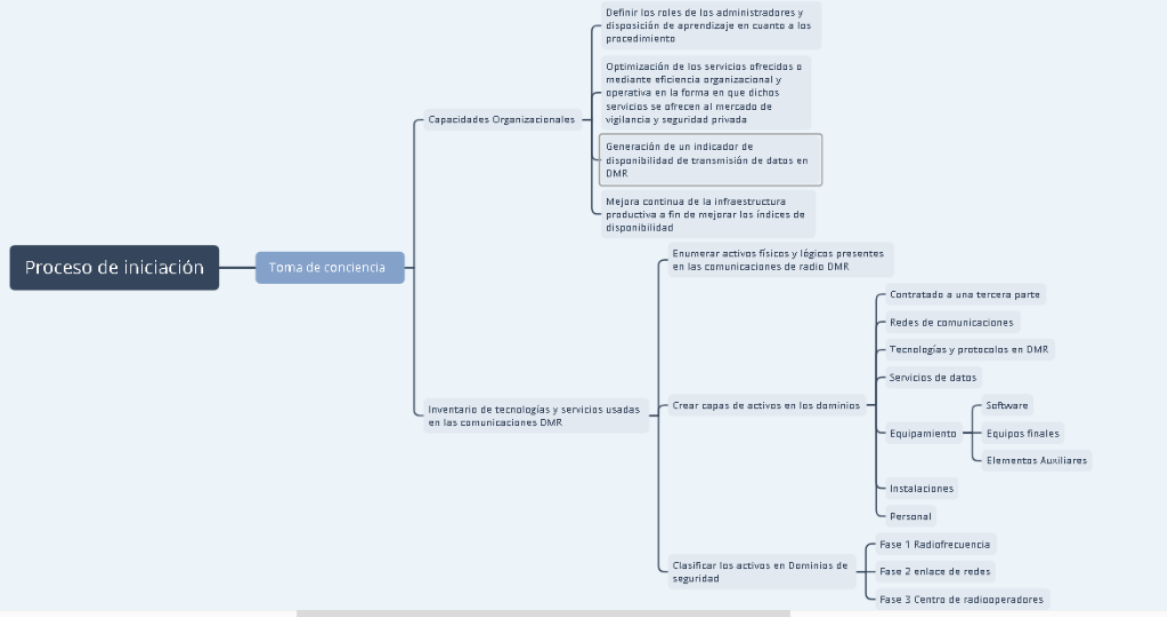
6.2 Proceso de iniciación

En el proceso de iniciación se derivaron en dos ítems específicos, se describen a continuación:

6.2.1 Toma de conciencia

Para la etapa de toma de conciencia lo principal es que exista dentro de la organización un nivel de responsabilidad en cuando al cuidado de las comunicaciones existentes. Deben ser considerados los procedimientos técnicos, las buenas prácticas y las recomendaciones como una opción que contribuye en la estabilización de la transferencia de datos en redes productivas basadas en DMR sensibles a ataques de DoS en donde por medio de sistemas de detección de intrusos se pueda mejorar la disponibilidad de los servicios usados.

Figura 6-7: Toma de conciencia



Fuente: Construcción propia

Capacidades organizacionales

Las empresas deben desarrollar y fortalecer como parte de su estrategia de optimización y transformación organizacional unas capacidades a partir del empleo inteligente y efectivo de las tecnologías de información. La expresión Capacidades Organizacionales, se refiere, en este contexto, a la habilidad que tienen las organizaciones para llevar a cabo una determinada actividad, habilidad que puede ser mayor, menor o igual a la de la competencia, a la de la industria o incluso a la de otras áreas dentro de la misma organización. Las capacidades organizacionales adquiridas en parte mediante la implementación y el desarrollo de una infraestructura DMR potente en funcionalidades, no deben tener el propósito de no solamente de contar con ellas, sino de desarrollarlas de tal manera que se conviertan rápidamente en ventajas competitivas o competencias distintivas, es decir, no solamente hacer bien las cosas internamente para que el sistema opere, sino con respecto a la competencia con el fin de generar una ventaja sostenible en el tiempo. Estas capacidades organizacionales deben tener las siguientes características principales para ser realmente una fuente de excelencia competitiva para una cadena de conexión en DMR:

- Definición de roles de los administradores y disposición de aprendizaje en cuanto a los procedimientos sugeridos para la disminución de la materialización de amenazas que afecten la disponibilidad.
- Generación de un indicador de disponibilidad de transmisión de datos en DMR. El indicador propuesto Permite medir el porcentaje de disponibilidad media anual del servicio ofrecido con base en la cadena de conexión DMR, mediante la comprobación sistemática, de manera automática, del estado del servicio y el proceso que lo provee, almacenando los periodos de tiempo no operativos.

Cálculo del valor del indicador: Disponibilidad = 100 – 100 *(suma de horas no operativo del servicio de datos) /número total de horas anual de uso de servicio de datos) (Belaustegui, 2007).
Se sugiere para la realización de este cálculo automático la herramienta Zabbix de distribución GNU que se adapta plenamente a cualquier infraestructura y en donde son aplicados conceptos como los SLA, auditoría de acciones, el control de acceso a la información, catalogación, provisión e inventariado, escalado de incidentes y composición de los Elementos de Configuración del IT. (2018) tomado de https://www.zabbix.com/. El grado de fiabilidad es total, dado que los valores se obtienen de forma automática sin procesos de transformación intermedios.

Con el cálculo de la disponibilidad inicial se podrá validar en qué condiciones se encuentra la cadena de conexión a evaluar y su ponderación final tras ser aplicada la metodología propuesta.

- Contribuir de una manera importante a generar valor de negocio en el sentido en que se usan los servicios DMR con funciones de datos mediante la optimización de los servicios ofrecidos. (aplicación de salvaguardas)
- Promover o fundamentar la base de mejora continua de la infraestructura productiva a fin de mejorar los índices de disponibilidad de los datos por afectaciones externas como ataques de DoS apoyándose de metodologías como la propuesta. (monitoreo permanente, generación de alertas, respuesta y lecciones aprendidas)

6.2.2 Inventario de tecnologías y servicios usados en DMR

Es fundamental realizar un levantamiento organizado de activos para el posterior análisis de riesgo basado en la disponibilidad aplicado a cada fase. Los activos deben clasificarse por capas, dominios de seguridad y en fases de conexión para lograr un mejor entendimiento del riesgo al que están expuestos y para tomar las medidas correctivas que se adapten mejor. Usar como referencia la tabla de activos del capítulo anterior.

6.3 Fases de la metodología

Las cuatro fases de la metodología se describen a continuación:

6.3.1 Fase 1: Detección de DoS en la transmisión de datos en el espectro radioeléctrico aplicado a DMR

Esta fase se basa en la relación de activos y la evaluación del riesgo, la realización de indicadores de eventos sospechosos y la clasificación posterior de ataques DoS que pueden ocurrir en radiofrecuencia que afecten la disponibilidad en la transmisión de datos en DMR. Luego, se plantean los requisitos para la construcción de un sistema de detección de intrusos ajustado a este escenario.

El desarrollo de esta fase proporcionará a la metodología final los lineamientos de detección en el espectro radioeléctrico; aportando estrategias para monitorear, detectar y dar respuestas de control a posibles afectaciones de servicios de datos por ataques DoS en esta etapa de transmisión de la cadena de conexión del estándar DMR.

Figura 6-8: Componentes de la topología DMR

Fuente: Construcción propia

En el análisis de riesgo propuesto se pudieron evidenciar riesgos altos asociados a la transmisión de datos en el espacio radioeléctrico mediante interfases áreas y en conexiones locales ubicadas en la estación base de radio. Por lo tanto, se deben usar como referencia las salvaguardas propuestas de acuerdo al dominio de seguridad fase 1 radiofrecuencia, siendo las más relevantes: los acuerdos de servicio con terceros, la creación de roles, la aplicación de buenas prácticas de implementación (son entregadas las salvaguardas generales en la tabla de salvaguardas del capítulo anterior de esta fase para que sean aplicadas acorde al escenario) y la detección de intrusos basados en anomalías de denegación de servicio. Para la metodología de detección de intrusos DoS en esta fase se sugieren los siguientes pasos:

- **Paso 1:** Crear indicador de disponibilidad de servicios y tecnologías para la transmisión de datos en DMR fase 1.
- **Paso 2:** Investigar y definir el comportamiento normal de la red con la intención de establecer patrones; validando las posibles fuentes de información que conduzcan a la detección y clasificación de intrusos potenciales. Esto significa que se debe crear una base de conocimiento de red anómala que constituirá la base para la clasificación de eventos potencialmente intrusivos, que permita posteriormente analizar y evaluar para crear un modelo

de ataque y utilizarlo para proporcionar una respuesta adaptativa (anomalía) para la posterior aplicación de un esquema de recuperación de la intrusión. Para la realización de las actividades en esta fase se sugieren herramientas libres para analizar el espectro radio eléctrico que harán las veces de SNIFFER usando radio definido por software SDR como se puede observar en la tabla 6-1.

Tabla 6-1: Herramientas libres

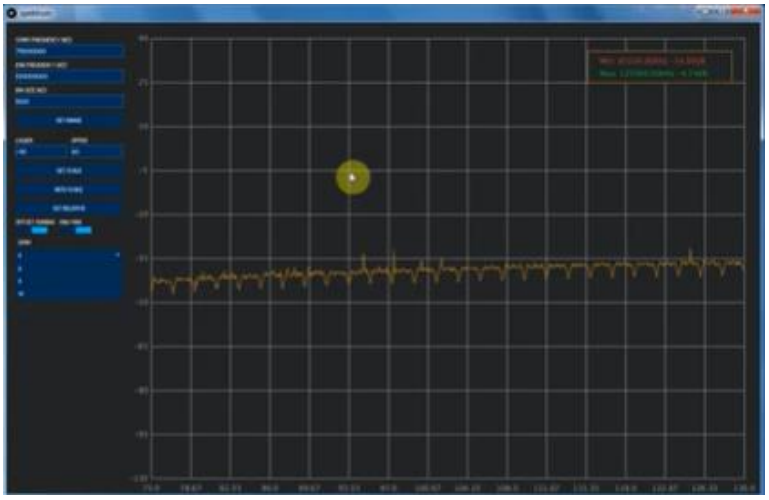
HERRAMIENTA DE DETECCIÓN PROPUESTA	BENEFICIOS
RTLSDR Scanner	La aplicación es un analizador de espectro que realiza exploraciones consecutivas y permite recopilar datos y hacer comparaciones.
SDR-Sharp SPEKTRUM	Muestra el espectro mostrado en tiempo real.
GNU radio	Es una herramienta que provee un marco de desarrollo adaptable que permite entender el funcionamiento del espectro y aplicar técnicas para inhibir radioescuchas intencionados o no intencionados
Trbonet Watch SDR-Sharp	Software propietario de la marca Motorola Inc. Puede monitorear redes MOTOTRBO de cualquier tamaño, a partir de sistemas de simple repetidores solo a redes complejo radioeléctrico de múltiples sitios. También; SDR-Sharp Es usado para evaluar este tipo de agentes con soluciones libres SDR.
RDAC	Software propietario de la marca Motorola Inc. permite a un administrador u operador de una red MOTOTRBO diagnosticar y controlar los repetidores MOTOTRBO. RDAC brinda un gran nivel de conveniencia, permitiendo reaccionar rápidamente a cualquier problema que pueda surgir en la red.
TRBONET TRIANGULACIÓN GPS	Software propietario de la marca Motorola Inc. Es una aplicación fesional desarrollada especialmente para centros de despacho controlan grandes cantidades de tráfico. Permite: Seguimiento equipos, Unidad de seguridad, dad de seguimiento, emetría y emergencia

Fuente: Construcción propia

A continuación, se muestran resultados de la herramienta Spektrum que servirá para recopilar la información del espectro y facilitar la investigación basada en comportamiento para la clasificación posterior del ataque. Los valores de referencia usados en la herramienta fueron los siguientes:

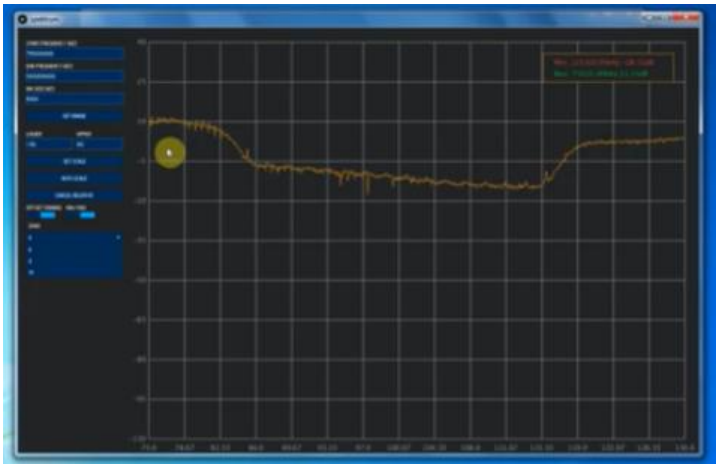
- Frecuencia mínima a 24 Mhz con frecuencia máxima a 1766 Mhz.
- Chip usado R820T compatible con RTL2832U.
- Cada sintonizador ofrece diferentes rangos de frecuencia, ganancias, amplificadores y filtros. Se recomienda usar una frecuencia de al menos 60 a 1100 MHz.
- Generar una señal de interferencia entre esos rangos a fin de detectar la anomalía.

Figura 6-9: Visual de condiciones normales del espectro radioeléctrico



Fuente: Construcción propia en base a la herramienta Spektrum

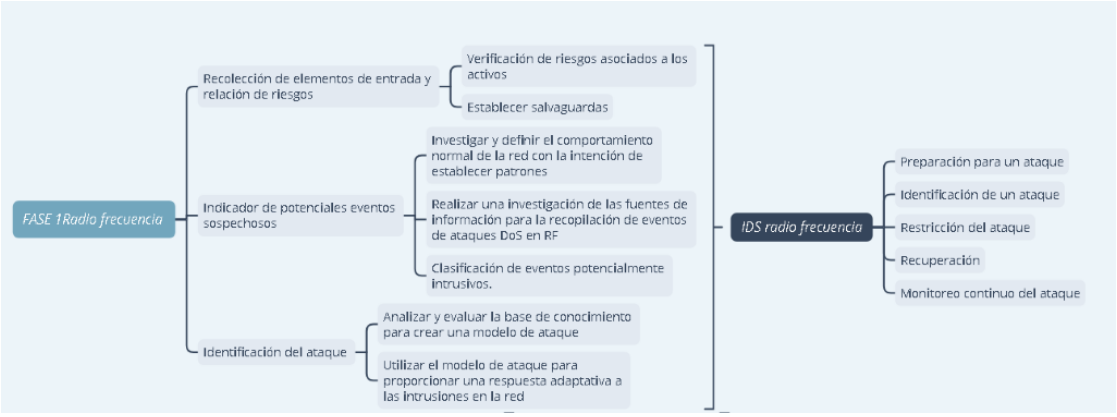
Figura 6-10: Visual con interferencia del espectro radioeléctrico



Fuente: Construcción propia en base a la herramienta Spektrum

Los resultados entregados por las herramientas permiten caracterizar el tipo de ataque y clasificar la anomalía para relacionarla a la base de conocimiento y apoyar la detección del sistema propuesto.

Figura 6-11: Fase 1 radiofrecuencia



Fuente: Construcción propia

- **Paso 3:** Realizar una investigación de las fuentes de información para la recopilación de eventos de ataques DoS en RF en el mundo real para la actualización de la base de conocimientos.
- **Paso 4:** Clasificación de eventos potencialmente intrusivos.
- **Paso 5:** Analizar y evaluar la base de conocimiento para crear un modelo de ataque. Tomando como referencia los resultados que entregan las herramientas sugeridas pueden ser clasificados los ataques según la siguiente tabla:

Tabla 6-2: Clasificación de ataques

Ataque DoS	**Intento de ataque**	**Manifestación**
Jamming por ruido	DoS por interferencia	Las interferencias impactan negativamente el rendimiento
Jamming por red	Dos para ocasionar impacto en la red de datos	Negación del nivel de red para la transmisión de datos.
Aparición de unidades maliciosas	DoS por suplantación	Participantes duplicados en red legítima pasiva. Aparición de unidades maliciosas.
Transmisión inoficiosa	DoS por transmisión incorrecta de datos	Envió masivo de paquetes mal formados de datos que ocupan el canal evitando la transmisión de otras unidades.

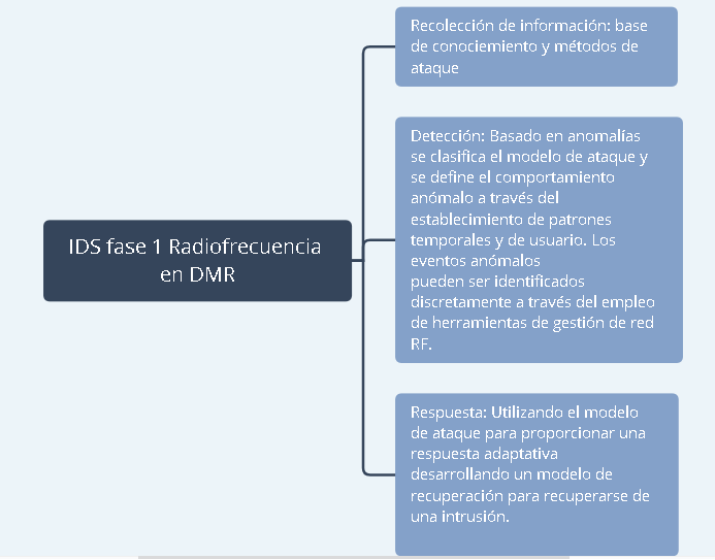
Fuente: Clasificación de ataques DoS. (Kong, 2011).

- **Paso 6:** Utilizar el modelo de ataque para proporcionar una respuesta a las intrusiones en la red.

Luego, se debe preparar la respuesta a las intrusiones en el enlace de datos táctico basado en RF que inciden en la transferencia de datos en DMR. Para la respuesta de intrusiones debe establecerse un sistema de detección de intrusos basado en anomalías que alerte sobre intrusiones mediante la observación de las desviaciones

del comportamiento típico del tráfico de la red relacionadas con la base de conocimiento realizada y que cuente con la siguiente estructura para su desarrollo:

Figura 6-12: Sistema de detección de intrusos en Fase 1



Fuente: Construcción propia

La figura 6-12 muestra la estructura de un sistema de detección de intrusos para la fase 1 de radiofrecuencia en donde se cumple con los tres elementos estándar de diseño de un IDS compuesto de los elementos: recolección de información, detección y respuesta; en donde se pretende por medio de una base de conocimiento, herramientas de detección y correlación de modelos de ataques alertar sobre los eventos que afecten la disponibilidad por ataques DoS y la transmisión de datos en RF. Se recomienda usar los indicadores de disponibilidad para evaluar la efectividad de las estrategias de respuesta.

Algunas respuestas recomendadas ante a los modelos de ataque citados se muestran en la Tabla 6-3:

Tabla 6-3: Correlación detección de ataque y respuesta

Ataque DoS	Intento de ataque	Respuesta
Jamming por ruido	DoS por interferencia	Minimizar en lo posible, potencias de transmisión y direcciones de radiación para limitar la emisión para que solo lleguen a áreas de interés de la infraestructura de radio DMR. Recomendada la implantación de sistemas antijamming (Ángel, 2015). Hacking práctico de redes wifi y radiofrecuencia.
Jamming por red	Dos para ocasionar impacto en la red de datos	Tratamiento a subsistemas y conexiones a redes externas. Separación física y lógica de comunicaciones de radio fase 1 con otras fases de la cadena de conexión. (Ángel, 2015). Hacking práctico de redes wifi y radiofrecuencia.
Aparición de unidades maliciosas	DoS por suplantación	Control y actualización de diferentes inventarios de equipos. Monitoreo constante de unidades de radio. (Ángel, 2015). Hacking práctico de redes wifi y radiofrecuencia.
Transmisión inoficiosa	DoS por transmisión incorrecta de datos	Monitoreo y vigilancia de estado de canales y de unidades con mayor índice de transmisión de datos errados para que sea aislado de la red productiva. (Ángel, 2015). Hacking práctico de redes wifi y radiofrecuencia.

Fuente: Construcción propia

La respuesta a diferentes tipos de ataques DoS apoya de forma directa la disponibilidad de servicios en escenarios hostiles como el espacio radioeléctrico. El nivel de sofisticación de un posible ataque va de nivel básico ha avanzado y la respuesta es clave para mitigar este tipo de amenazas, que siempre deben estar acompañadas de estrategias procedimentales y técnicas. En este sentido, los patrones de detección son un insumo muy importante en la confección de la base de conocimiento de sistemas de detección que pueden alertar en forma temprana condiciones inseguras, anticipando posibles interrupciones que afecten servicios en infraestructuras productivas.

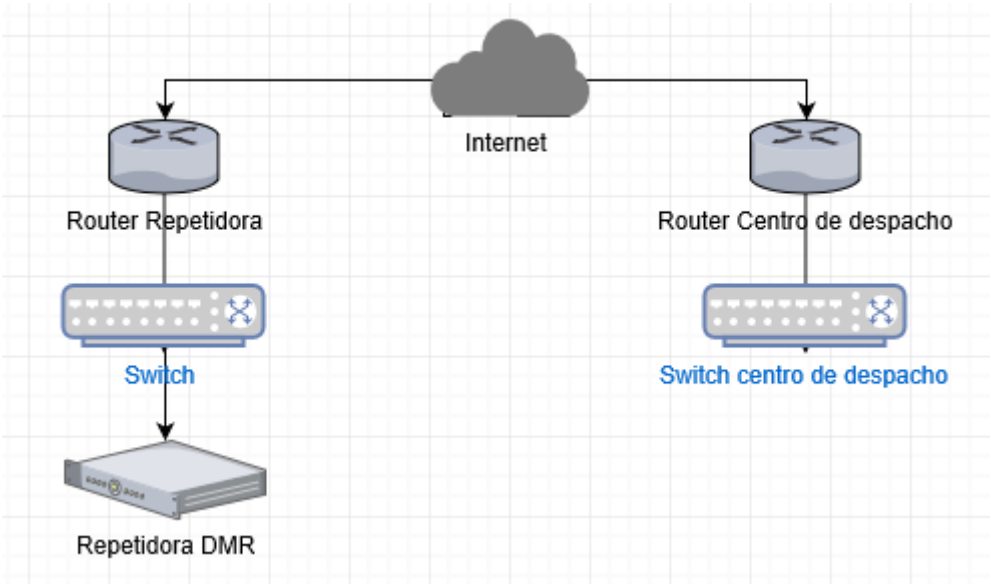
6.3.2 Fase 2: Detección de DoS en la transmisión de datos en repetidoras sitio a sitio aplicado a DMR

Las comunicaciones sitio a sitio entre repetidoras y centros de monitoreo en la cadena de conexión DMR se implementan por dos métodos; conexión directa por IP publica con cifrado básico (poco recomendada) o conexión por dispositivo de enrutamiento y transmisión segura de datos por túnel de comunicación (recomendada). Las comunicaciones en esta fase se encuentran establecidas bajo el protocolo de saludo de tres vías TCP/IP. Por lo tanto, deben ser considerados los ataques DoS que puedan afectar a este protocolo en cuanto a la disponibilidad y la transmisión de datos de acuerdo al escenario. Esta fase se basa en la relación de activos presentes enumerados anteriormente en el dominio de seguridad, la evaluación del riesgo, la captura de eventos sospechosos asociados y la tipificación posterior de ataques DoS que pueden ocurrir en la transmisión de datos entre repetidoras sitio a sitio que afectan la disponibilidad en la transmisión de datos. Luego, se plantean los requisitos para la construcción de un sistema de detección de intrusos ajustado a este escenario.

El desarrollo de esta fase proporcionará a la metodología final estrategias de detección para monitorear, detectar y dar respuestas de control a posibles afectaciones de servicios de datos por ataques DoS en la etapa 2 o de conexiones sitio a sitio de la cadena de conexión del estándar DMR. El tratamiento de eventos en esta fase permitirá que un mensaje de datos codificado pueda ser enviado para ser administrado por el

centro de monitoreo o para ser enviado entre repetidoras en un esquema de conexión troncalizado (varias repetidoras y un sitio de control).

Figura 6-13: Topología fase 2 de enlace TCP/IP repetidor y centro de despacho



Fuente: Construcción propia

Inicialmente se recomienda aplicar las salvaguardas propuestas (relacionadas en la tabla de salvaguardas del capítulo anterior) de acuerdo al dominio de seguridad fase 2 enlace TCP/IP, siendo las más relevantes: Aseguramiento de la transmisión por medio de claves criptográficas, evitar puntos únicos de fallo y usar herramientas de monitoreo de enlaces; para esta última se propone un sistema de detección de intrusos basado en firmas de denegación de servicio; en donde se sugieren los siguientes pasos de aplicación:

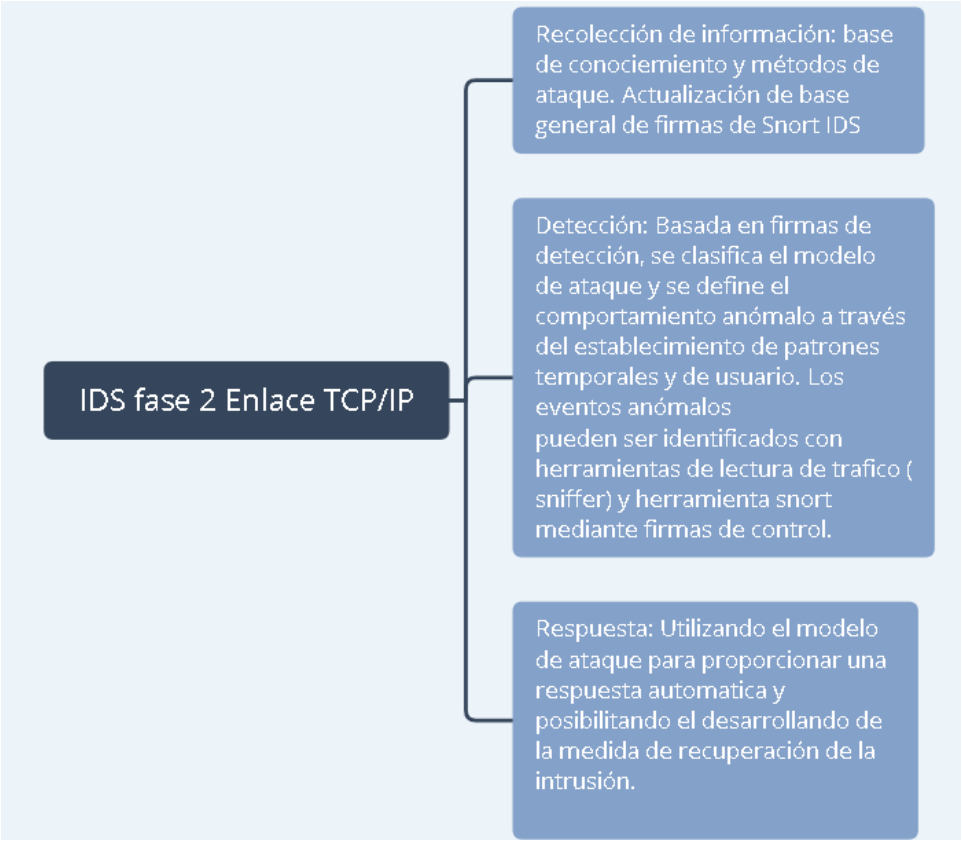
- **Paso 1:** Crear indicador de disponibilidad de servicios y tecnologías para la transmisión de datos en DMR en la fase 2.
- **Paso 2:** Realizar una búsqueda de patrones conocidos dentro del tráfico TCP/IP, mediante técnicas conocidas como inspección profunda de paquetes DPI que permita comparar el tráfico de la red con firmas conocidas de ataques.

Si una porción del tráfico coincide con un ataque conocido, es generada una alarma y almacena la alerta en el registro.

- **Paso 3:** Mantener la base de firmas actualizada.
- **Paso 4:** Desarrollar firmas propias ante nuevos ataques y variaciones de los ataques conocidos potencialmente intrusivos y que afecten la disponibilidad de los datos. (ataques de día cero).
- **Paso 5:** Proporcionar una respuesta adaptativa las intrusiones en la red que afecten la disponibilidad en la transmisión de datos DMR.

Se propone en esta fase la implantación el IDS snort producto bajo licencia GNU que permite aplicar los pasos del 2 al 5. Snort es un sistema de detección de intrusos basado en red (NIDS) que implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida con patrones que corresponden a ataques conocidos, intentos de aprovechar alguna vulnerabilidad, análisis de protocolos, etc.; Realizando todas estas tareas en tiempo real. http://www.snort.org

Figura 6-14: Sistema de detección de intrusos para enlaces TCP/IP



Fuente: Construcción propia

El sistema de detección de intrusos propuesto compara con una base de datos de firmas de ataques conocidos asociados a la base de conocimiento y relaciona huellas digitales de paquetes maliciosos generando la respectiva alerta.

6.3.3 Fase 3: Detección de DoS en la transmisión de datos en infraestructura local aplicado a DMR

Esta fase se basa en la relación de activos enumerados anteriormente y la evaluación del riesgo, la realización de indicadores de eventos sospechosos asociados y la tipificación posterior de ataques DoS que pueden ocurrir en la en la transmisión de datos en infraestructura local aplicado a DMR. Luego, se plantean los requisitos para la adaptación de un sistema de detección de intrusos ajustado a este escenario en donde se propone la construcción de un sistema de detección de intrusiones basada en servidores HIDS (Host Intrusión Detection Systems), diseñado para responder a ataques sobre un determinado servidor basado en la supervisión de las acciones de los usuarios y de los archivos del servidor que servirá para detectar ataques externos como internos.
Inicialmente se recomienda aplicar las salvaguardas propuestas (relacionadas en la tabla de salvaguardas del capítulo anterior) de acuerdo al dominio de seguridad fase 3 centro de despacho, siendo las más relevantes: aplicar perfiles de seguridad, protección de las Aplicaciones Informáticas (SW) y el aseguramiento de la disponibilidad; para esta última se propone un sistema de detección de intrusos HIDS basado en firmas de denegación de servicio.

El desarrollo de esta fase proporcionará a la metodología final estrategias de detección para monitorear, detectar y dar respuestas de control a posibles afectaciones de servicios de datos por ataques DoS en la etapa 3 o en infraestructuras LAN que es donde se recibe el paquete final de datos que es administrado por el centro de monitoreo. El tratamiento de eventos de seguridad asociados a la disponibilidad en esta fase permitirá que un mensaje de datos pueda ser evaluado por el sistema despachador.

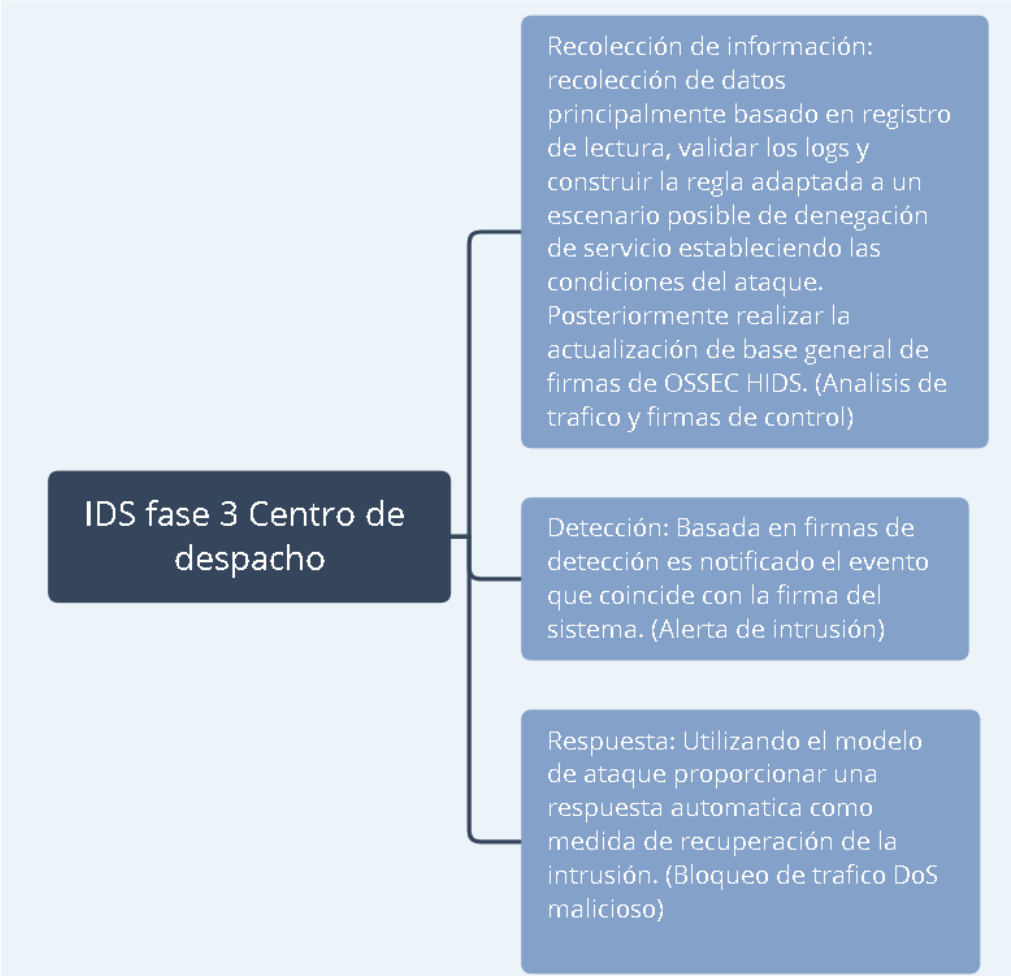
Se sugieren los siguientes pasos de desarrollo:

- **Paso 1:** Crear indicador de disponibilidad de servicios y tecnologías de para la transmisión de datos en DMR fase 3.

- **Paso 2:** Desplegar la herramienta local con conexión a servidor que por medio de agentes permita monitorear los hosts implicados en la cadena de conexión; servidor y equipo radio operador.
- **Paso 3**: Mantener la base de firmas actualizada.
- **Paso 4:** Proporcionar una respuesta adaptativa las intrusiones en la red que afecten la disponibilidad en la transmisión de datos DMR.

Se propone en esta fase la herramienta OSSEC con licencia GNU la cual se adapta con los pasos anteriores sugeridos de implantación. Funciona como detector de intrusos en host y proporciona análisis de log, verificación de integridad de ficheros, monitorización del registro de Windows, detección de ROOTKITS en tiempo real, etc. De igual modo, permite configurar respuestas activas. Funciona con sistemas operativos como Linux, OpenBSD, FreeBSD, MacOS, Solaris y Windows. Permite el esquema de instalación centralizado en donde por medio de un servidor se administran las estaciones que cuentan con el agente de conexión. https://www.ossec.net/docs

Figura 6-15: Sistema de detección de intrusos centro de despacho



Fuente: Construcción propia

El sistema inicialmente debe ser parametrizado mediante a la lectura de logs para establecer el tráfico anómalo de denegación de servicio que puede ser generado por ataques de inundación de paquetes constantes al servidor de aplicaciones o un host de despacho. Luego, se debe especificar en la base de conocimiento y relacionar huellas digitales de paquetes maliciosos (cabeceras de tramas) para la generación de una alerta.

El sistema de detección de intrusos propuesto compara con una base de datos de firmas de ataques conocidos y las firmas personalizadas ajustadas al escenario propuesto.

6.3.4 Fase 4: Consolidación de fases para la detección DoS en las comunicaciones basadas en el estándar DMR

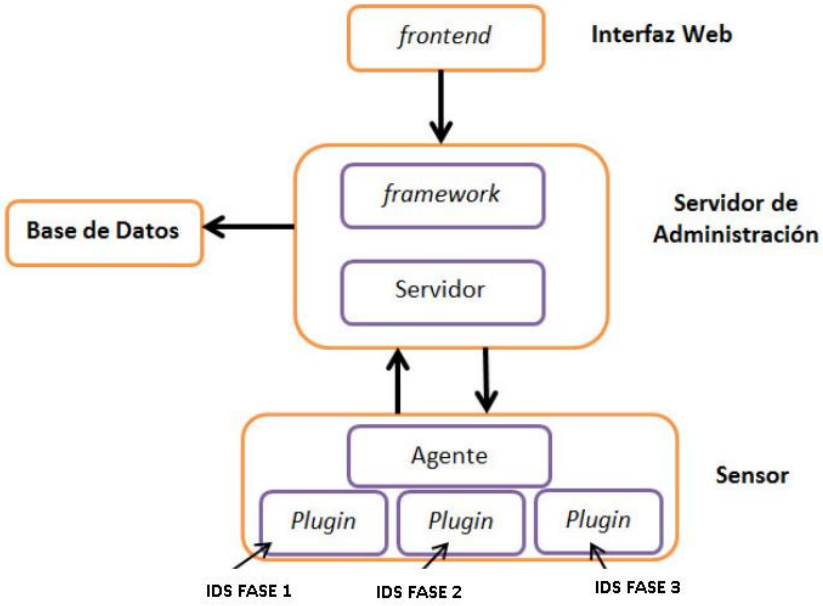
Para la consolidación de las fases propuestas se propone la implementación de un sistema correlacionador de eventos que permita tener referencia de todos los datos capturados de los sensores establecidos en toda la cadena de conexión asociados a ataques de denegación de servicio. Se propone implementar el sistema SIEM (sistema de información y gestión de eventos) llamado OSSIM (https://www.alienvault.com/products/ossim) distribuido con licenciamiento libre que está diseñado bajo una infraestructura robusta que permite almacenar eventos de diferentes sistemas y facilitar la gestión del escenario de detección de intrusos distribuido propuesto.

La fase 4 de consolidación de resultados, permitirá tener un sistema centralizado de eventos de detección que brindará una visual general de lo que ocurra en cada fase o momento de transporte de los datos DMR en donde fueron colocados los subsistemas de detección de intrusos. El producto final de desarrollo de esta fase será la consola general de detección de intrusos de ataques DoS para comunicaciones DMR.

Se proponen los siguientes pasos de adaptación de la solución propuesta:

- **Paso 1:** Definir el equipo que tendrá implementados los servicios de recolección de los agentes distribuidos en cada fase encargados de la detección de intrusos. (Ossim server).
- **Paso 2:** Validar el funcionamiento del framework y la base de datos dentro del servidor principal que serán los encargados del frontend de gestión y el almacenamiento de parámetros respectivamente.
- **Paso 3:** Implementación de agentes distribuidos en toda la cadena de conexión en donde se requiera notificación de eventos y en los detectores de intrusión implementados. (Ossim agent).

Figura 6-16: Arquitectura propuesta interna de OSSIM



Fuente: Construcción propia

La Figura 6-14 muestra como está compuesto el sistema de correlación de eventos que proporcionará una visual completa de la cadena de conexión y generará las alertas para atender los ataques de denegación que pudiesen afectar la transmisión de datos. Para el desarrollo se recomienda establecer las siguientes políticas de uso para una adaptación optima al escenario propuesto:

- **Política 1:** El modo de transmisión de eventos será basado en niveles de disponibilidad.
- **Política 2:** El protocolo propuesto para el envío de eventos es SYSLOG por ser ampliamente aceptado para él envió de estado de dispositivos y de los IDS dispuesto en la cadena de conexión.
- **Política 3:** Tipificar los eventos de acuerdo con el nivel del riesgo de la alerta y la fase de conexión para abordarlo y brindar respuesta adaptativa.
- **Política 4:** Clasificar los eventos en nivel de prioridad y de confiabilidad de acuerdo con la alerta generada.

Tabla 6-4: Consolidado de logro de objetivos

OBJETIVO	EVIDENCIA DE REALIZACIÓN
Objetivo General: Elaborar una metodología de detección de intrusos para radios que utilizan protocolo DMR, que permitirá identificar y tratar ataques de denegación de servicios que afectan la disponibilidad en la transmisión de datos para empresas de seguridad privada a fin de reducir los riesgos de perdida de paquetes de datos en la cadena de conexión.	Es propuesta una metodología de detección de intrusos estandarizada por fases que recoge los insumos entregados por la caracterización de servicios y tecnologías, así como del análisis de riesgo; que permite identificar y tratar ataques de denegación por firmas o por patrones de comportamiento, lo cual permite que las empresas que la usen tengan un instrumento que les suministra diferentes alternativas para mejorar la disponibilidad de la transmisión de datos en cadenas de conexión productivas. Se puede evidenciar en el Capítulo 6 de este documento.
• **Objetivo específico 1:** Identificar servicios y tecnologías implicadas en las comunicaciones a través del protocolo radio digital móvil (DMR).	En el Capítulo 4: Servicios y tecnologías implicadas en las comunicaciones del estándar radio digital móvil (DMR) en la transmisión de datos; Se identifican servicios y tecnologías implicadas en las comunicaciones, además es analizado el estado actual del mercado en el cuanto al estándar DMR, los sectores de uso y es realizada la caracterización de tecnologías y servicios que permiten que las comunicaciones bajo el estándar funcionen para la transmisión de datos.
• **Objetivo específico 2:** Realizar un análisis de riesgos para determinar posibles impactos negativos	En el Capítulo 5: Análisis de riesgos para determinar posibles impactos negativos ocasionados por posibles ataques

ocasionados por diferentes ataques informáticos que generen denegación de servicio.	informáticos que generen denegación de servicio en la transmisión de datos en DMR; Teniendo la caracterización de servicios y tecnologías, se procede a aplicar una metodología de análisis de riesgo que permite evaluar amenazas y proponer salvaguardas de mitigación del riesgo para mejorar los niveles de disponibilidad de los servicios de datos en DMR.
• **Objetivo específico 3:** Proponer una metodología orientada a la detección de DoS en las comunicaciones basadas en el estándar DMR que contenga las posibles alternativas de protección y respuesta.	Con el análisis de riesgo, es desarrollada una propuesta orientada a la implantación de un sistema de detección de intrusos por fases y correlacionado en donde se contemplan los diferentes momentos en que el dato viaja por la cadena de conexión y el tratamiento que se debe dar para detectar mediante firmas o anomalías comportamientos que sugieran una posible intrusión que origine ataques DoS que afecte la disponibilidad en la trasmisión y recepción de datos.

Fuente: Construcción propia

7.Conclusiones y recomendaciones

7.1 Conclusiones

Dado los resultados obtenidos se pudo crear una metodología basada en sensores distribuidos en fases de conexión que logra la identificación de ataques DoS en infraestructuras DMR apoyada de la caracterización y el análisis de riesgo de los activos de información; en donde se obtienen eventos de seguridad asociados a la disponibilidad que inciden directamente en la transmisión de datos, facilitando el monitoreo general de la red productiva y aportando a la generación de estrategias de respuesta ante este tipo de eventos que pueden ir desde el mejoramiento propio del diseño de la infraestructura productiva hasta la aplicación de técnicas de detección en cada fase de conexión.

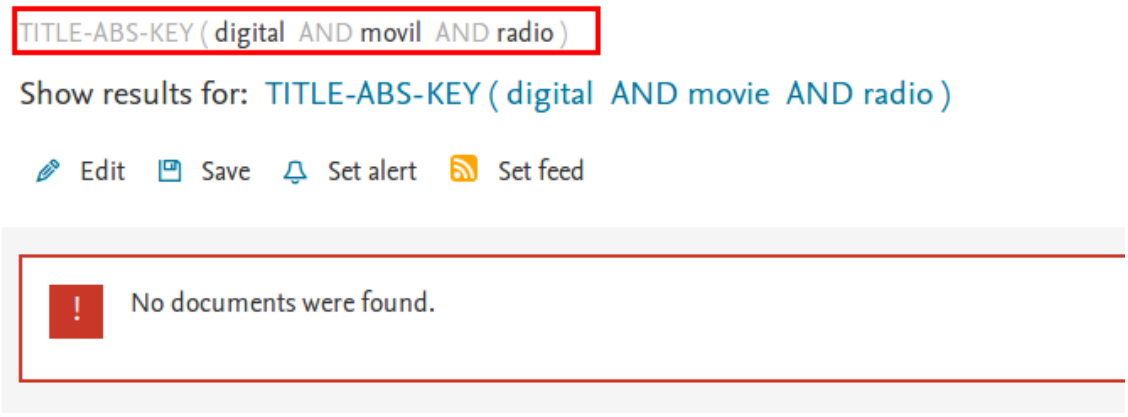
Basados en el análisis bibliométrico en una ventana de observación del 2005 al 2018, teniendo como motor de búsqueda SCOPUS, se evidenció una falencia en la producción científica en cuanto a validación de riesgo y respuesta ante incidentes en comunicaciones basadas en alguno de estos estándares especialmente en radio móvil digital DMR; en donde es claro que existen amenazas latentes que atentan contra los pilares fundamentales de la seguridad de la información en este tipo de comunicaciones. dado lo anterior se puede concluir que a pesar que en la actualidad diferentes técnicas de detección de intrusos para diferentes tipos de infraestructuras, no existe una metodología propiamente de implementación de un sistema sensorial que permita alertar y tratar eventos de denegación de servicio que inciden en la transmisión de datos, permitiendo obtener en este trabajo una propuesta estructurada que resuelve las necesidades de establecer controles que van desde la evaluación general de una infraestructura productiva hasta el análisis detallado de los activos que conforman la cadena de conexión, teniendo relevancia la aplicación de buenas prácticas de implementación y la estructuración de un sistema de monitoreo defensivo de este tipo de intrusiones.

Los resultados obtenidos de la caracterización de los servicios y las tecnologías que hacen parte de una infraestructura productiva y que hacen posible la transmisión de datos, permitió identificar tres fases de conexión o momentos en el que el dato es tratado: radiofrecuencia, enlace de redes y red local; que fueron determinados en espacios en que el dato puede verse afectado en el trasporte y donde es necesario olfatear para detectar y remediar eventos de disponibilidad.

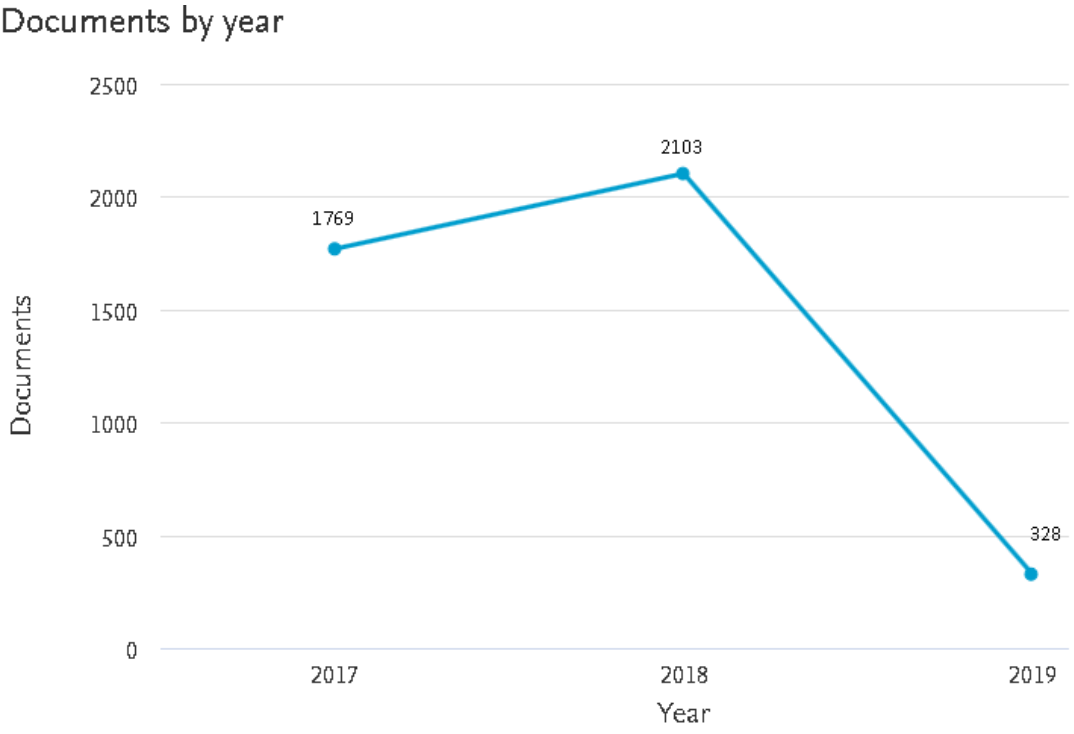
Luego, mediante el análisis de riesgo aplicando una metodología de análisis relacionada con las tecnologías de información y con el marco general del análisis de riesgo ISO 31000 como lo es Magerit V3, se obtuvieron resultados basados en el análisis de la dimensión disponibilidad y evaluando los diferentes activos clasificados previamente en dominios de seguridad relacionados a los momentos o fases de conexión en el que los datos son trasmitidos por la cadena de conexión DMR, pudiendo evaluar amenazas, nivel del riesgo y mitigación del riesgo.

Como un trabajo futuro que permitiría fortalecer los resultados de esta investigación, o como un nuevo trabajo de investigación, sería propone fortalecer los resultados con implementaciones en diversos escenarios DMR productivos o realizar nuevas investigaciones basadas en la detección de intrusos en espacio radioeléctrico que permita brindar mayor confianza para el uso de interfaces áreas en DMR para el transporte de datos sensibles y que apoyen no solo tareas operativas de personal sino que sean una real solución segura para infraestructuras criticas tales como SCADA que pueden usar este estándar de radio.

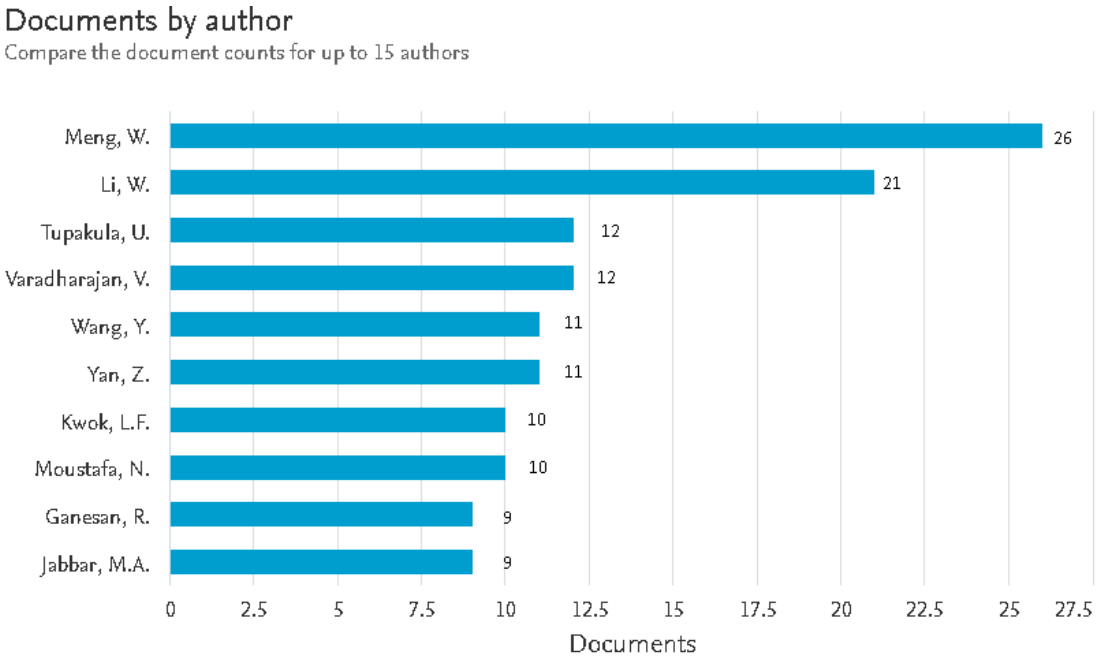
A. Anexo: Actividad científica del estándar DMR



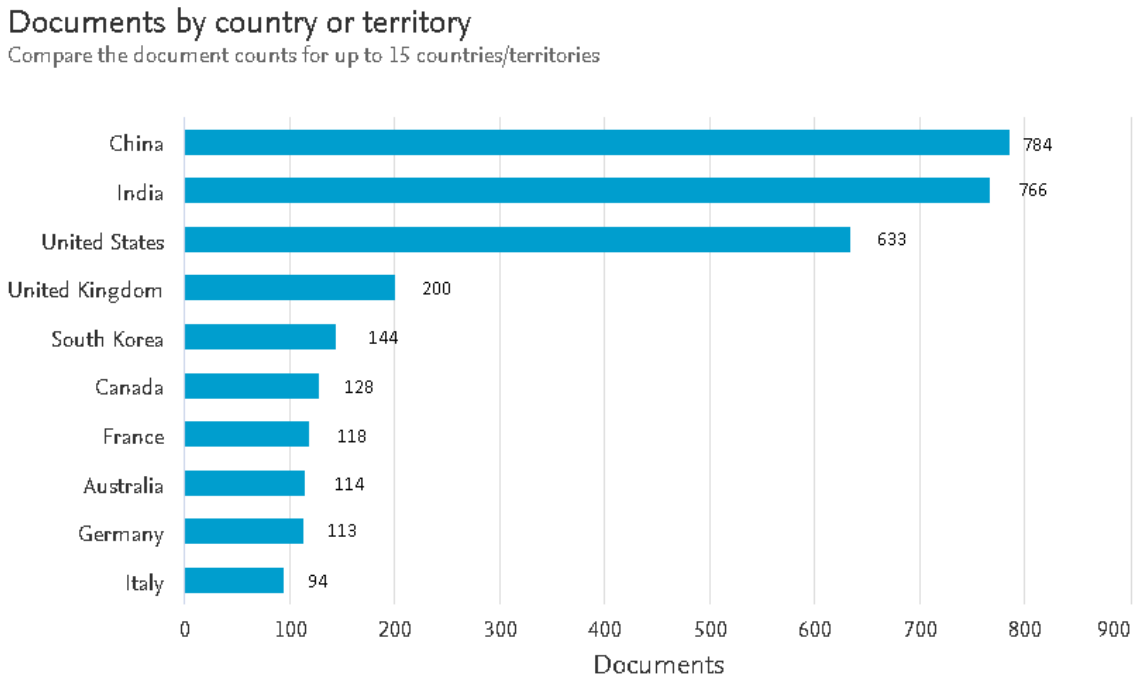
B. Anexo: Actividad científica por año



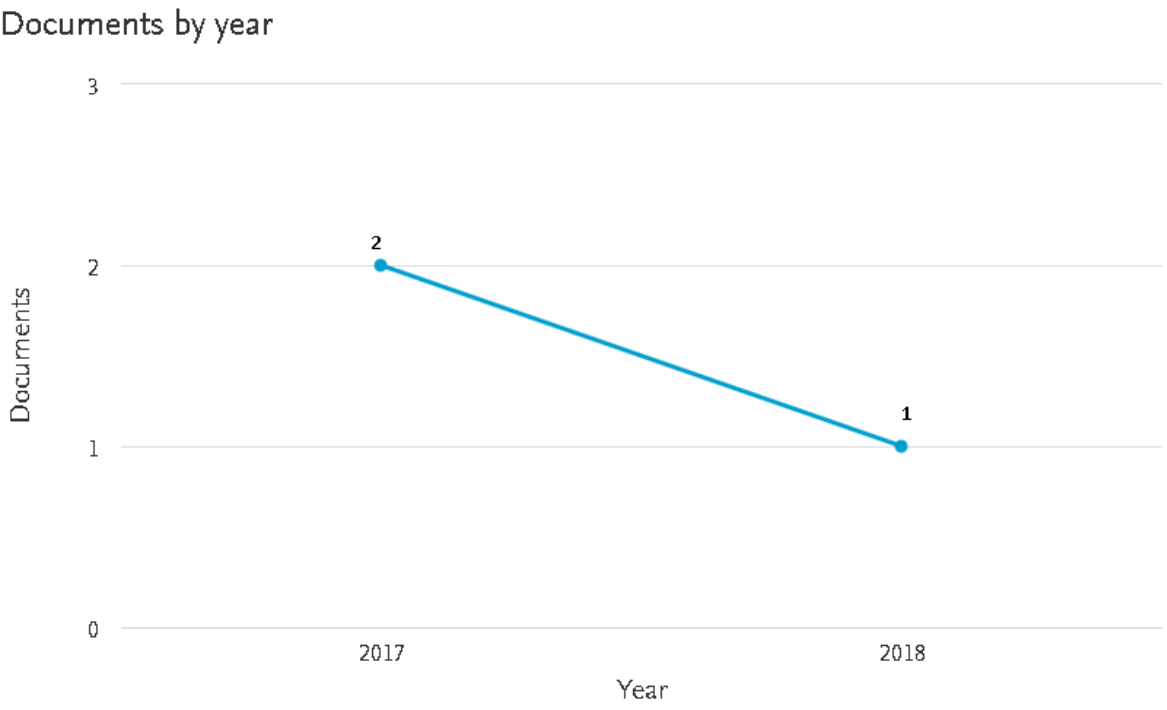
C. Anexo: Actividad científica por autores



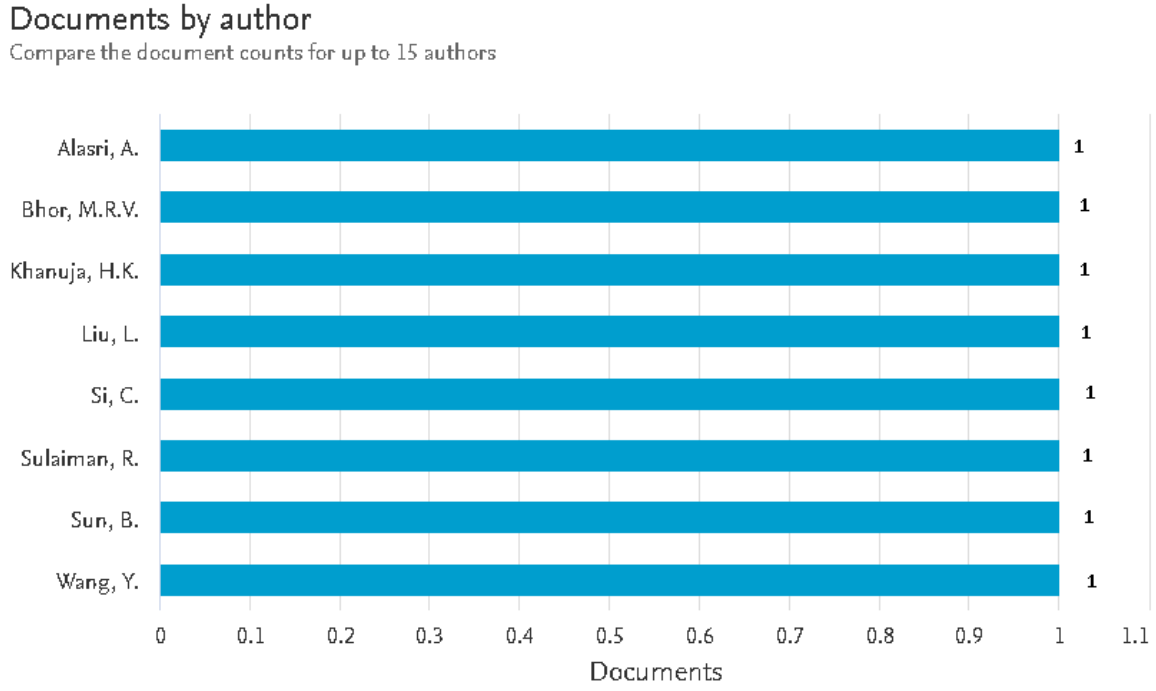
D. Anexo: Actividad científica por país



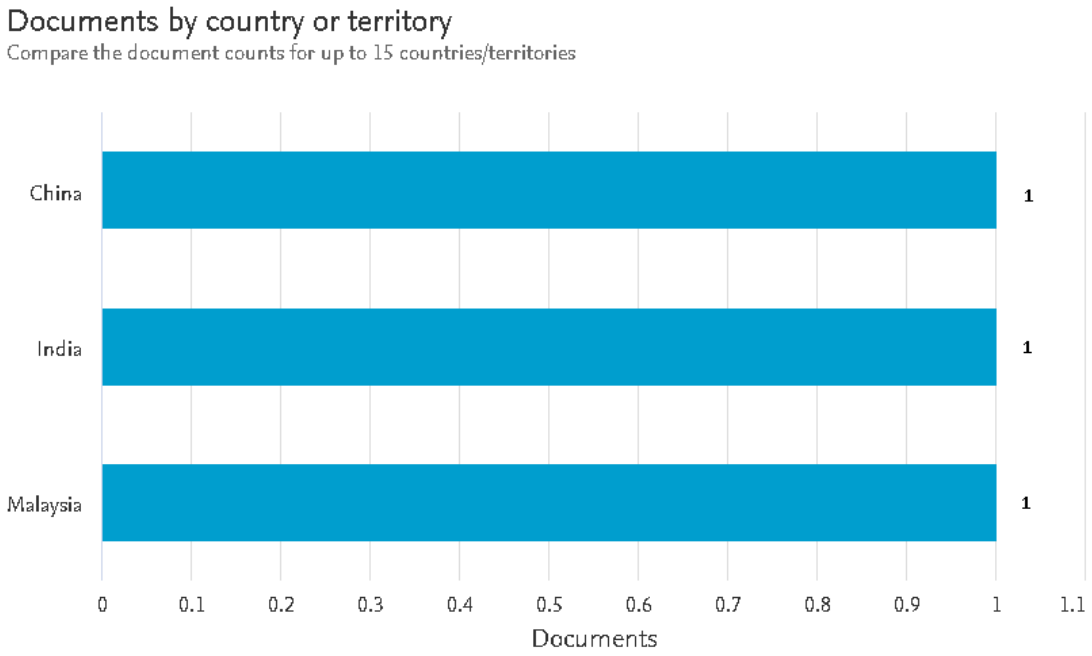
E. Anexo: Actividad científica por año



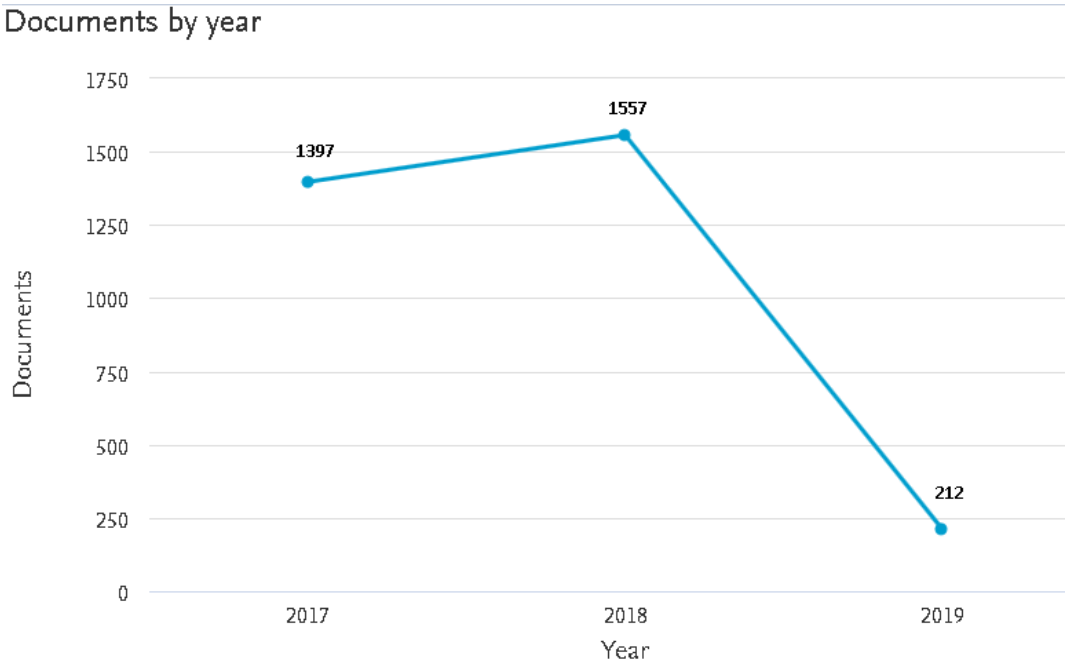
F. Anexo: Actividad científica por autor



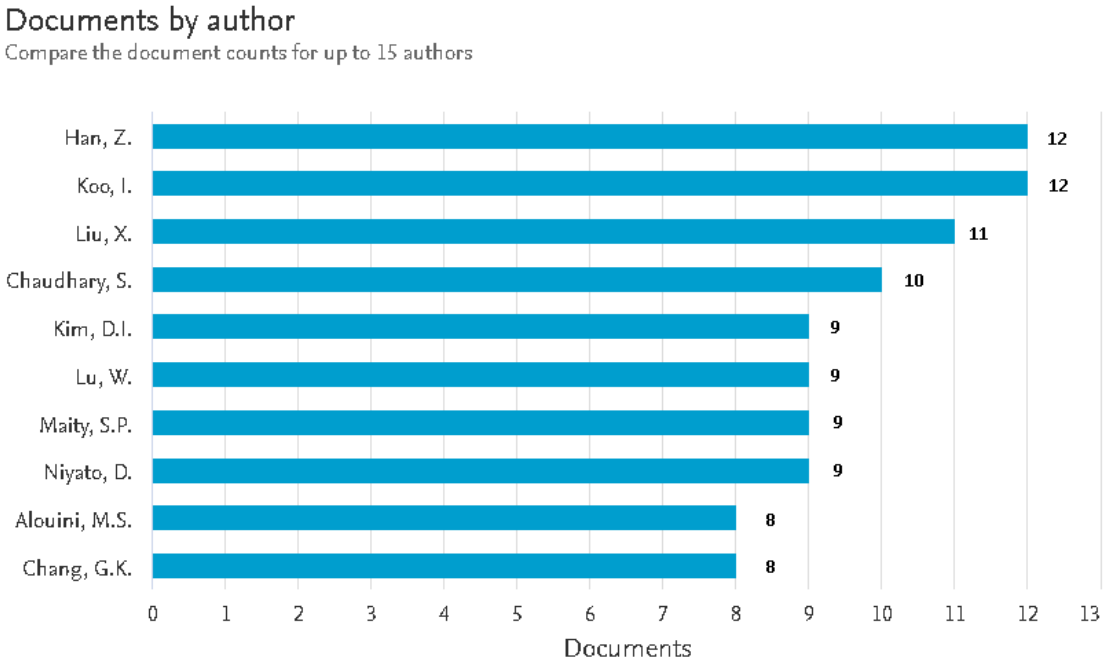
G. Anexo: Documentación técnica por país



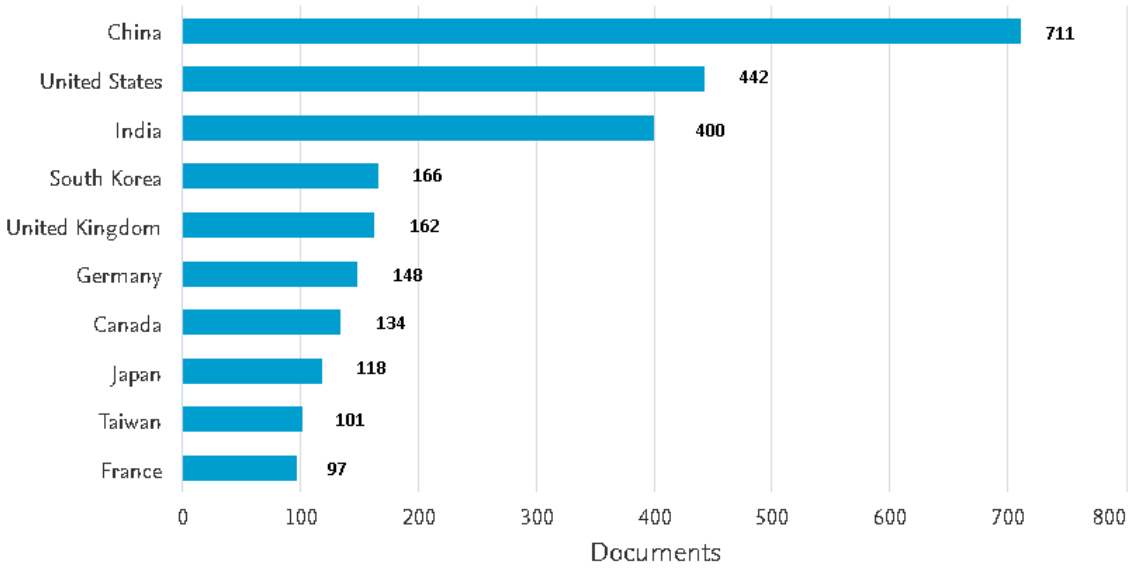
H. Anexo: Actividad científica por año



I. Anexo: Actividad científica por autor



J. Anexo: Actividad científica por país



K. Anexo: Clasificación de ataques DoS

Ataque DoS	Descripción	Nivel de complejidad	Ejemplo
Ataques de vulnerabilidad	Consiste aprovechar determinada falla que puede ser explotada de un sistema, tecnología o de un dispositivo que hace parte de una cadena de conexión enviando paquetes mal formados. (Ramos,2015)	Nivel medio: se deben conocer los dispositivos que hacen parte de la cadena de conexión, explorar la vulnerabilidad y de acuerdo con esta explotarla para que sea efectivo el ataque	Sistemas DMR: XPR4000 con versión FW superior a R01.11.02 XPR5000/7000 con versión FW superior a R02.06.02 La vulnerabilidad puede considerarse grave, ya que un atacante podría ser capaz de enviar comandos capaces de deshabilitar equipos radio remotos, enviar falsos mensajes de alerta y/o hacer uso de los recursos radio interfiriendo en el normal funcionamiento de la red de comunicaciones. (Security Art Work, 2014)
Ataques de inundación	Envió en gran cantidad de paquetes que puede saturar un canal de transferencia o un servicio asumiendo que no existe un filtrado de dichos paquetes o fuente generadora de interferencia. (Ramos,2015)	Nivel bajo: puede relacionarse a un ataque de fuerza bruta, en donde se envían múltiples paquetes o se trata de generar ruido sin conocimiento y se espera que el sistema víctima sea inhibido o bloqueado.	En el ataque "smurf", los atacantes están utilizando paquetes de solicitud de eco ICMP dirigidos a direcciones de transmisión IP desde ubicaciones remotas para generar ataques de denegación de servicio. Hay tres partes en estos ataques: el atacante, el intermediario y la víctima (tenga en cuenta que el intermediario también puede ser una víctima). En este caso enviar múltiples solicitudes ICMP sobre la red para validar el estado de las partes involucradas en la infraestructura puede generar congestión masiva y producir una

Ataque DoS	Descripción	Nivel de complejidad	Ejemplo
			denegación de servicio en la transmisión de datos. (Hlavacek, 2014)
Ataques de protocolo	Son ataques de inundación que se aprovechan de la debilidad de un protocolo por su asimetría o por los espacios que se pueden dar es una conexión que pueden ser aprovechados por el atacante para inyectar tráfico malicioso a fin de causar saturación o consumo de recursos disponibles. (Ramos,2015)	Nivel Alto: de ser conocido el protocolo objetivo por parte del atacante y con qué tipo de paquete se puede generar la inundación planeada para que el sistema basado en el protocolo objetivo falle.	El ataque al protocolo TCP SYN. Este es un tipo de ataque bien conocido y generalmente no es efectivo contra las redes modernas. Funciona si un servidor asigna recursos después de recibir un SYN, pero antes de que haya recibido el ACK. Esto produce que por las sucesivas solicitudes SYN no se cuente con recursos para solicitudes legitimas produciendo denegación de servicio (Z. Shu,Y. Qian , 2013)
ataques de recurso físico	Consiste en un ataque a un recurso especifico de infraestructura; puede ser CPU, memoria, enrutador, switch. Cualquier elemento que pueda incidir directamente en el escenario de conectividad. (Ramos,2015)	Nivel Alto: requiere conocimiento de la infraestructura objetivo, realizar rastreos que pueden ser detectados y realizar pruebas ensayo error que pueden ser infructuosos.	El ataque BGP es realizado mediante suplantación de identidad en donde se pretende imitar al par BGP. Esto puede ser una suplantación basada en TCP que apunta al puerto BGP del enrutador o paquetes de BGP falsificados. Existe una percepción común de que el BGP es fácil de falsificar. Sin embargo, algunos análisis simples demuestran que los ataques falsificados dirigidos a

Ataque DoS	Descripción	Nivel de complejidad	Ejemplo
			BGP no son tan simples como la gente cree. (A. G. Fragkiadakis, E. Z. Tragos & I. G. Askoxylakis, 2013)
Ataque middleware	Se trata de la posibilidad de que un atacante coloque un procedimiento intermedio que valide todo lo que ocurre antes de llegar a sistema o dispositivo que emite la respuesta. Esto eleva exponencialmente los tiempos de respuesta (Ramos,2015)	Nivel Alto: Requiere de conocimiento de la infraestructura y de las fases de conexión de la infraestructura objetivo para colocar el middleware en el lugar donde sea mayor el tráfico o las solicitudes.	El atacante coloca una rutina intermedia de comprobación hash a cada solicitud; esto haría que la función generada trabaje en el peor caso de respuesta produciendo tiempos de respuesta altos en alguno de los procesos intermedios de la cadena de conexión. (Z. Shu,Y. Qian , 2013)
Ataque de aplicación	El atacante toma como objetivo una aplicación específica y explota una vulnerabilidad que no tuvo en cuenta el desarrollador del sistema en cuanto solicitudes masivas que no procesa debidamente generando indisponibilidad. (Ramos,2015)	Nivel medio: El atacante requiere tener conocimiento de vulnerabilidades de sistemas conocidos que puedan ser explotados. Se cuenta con la posibilidad de tener fuentes múltiples de consulta para efectuar este tipo de ataques en los que es variado el nivel de complejidad.	Basado en una vulnerabilidad conocida, el atacante explota la falla enviando solicitudes simultaneas que no son limitadas por el código del fabricante generando la interrupción del servicio. (W. Wang, Y. Sun, H. Li and Z. Han , 2013)

L. Anexo: Sectores de uso del estándar DMR

SECTOR	DESCRIPCION	CATEGORIAS DE EQUIPOS USADOS
Infraestructuras criticas	“Medición remota de magnitudes físicas y envío de esta información hacia el operador del sistema. Supervisión, Control y Adquisición de Datos. SCADA. Soluciones en telecomunicaciones para compañías de Oíl & Gas. Soluciones inalámbricas para aplicaciones de campo petrolíferos." (TAIT, 2015)	Aplicaciones, Infraestructura, radios móviles, radios portátiles, telemetría
Minero	“Los servicios de comunicaciones de datos y voz integradas digitales de DMR permiten a los clientes de minerales y energía tener supresión de ruido de fondo, rastreo GPS, reducción de hombre y funcionalidad de explosión para beneficios de seguridad para operaciones mineras, certificación IP67 y MIL-STD para proteger contra la inmersión en agua,	Aplicaciones, Infraestructura, radios móviles, radios portátiles, telemetría

SECTOR	DESCRIPCION	CATEGORIAS DE EQUIPOS USADOS
	polvo, calor y alta humedad y templado vidrio que resiste los arañazos. DMR le permite integrar tecnologías como Bluetooth para interactuar con dispositivos como el ritmo cardíaco y otros monitores biométricos. El seguimiento en tiempo real de esos sensores que informan a través de las radios digitales portátiles de los trabajadores de la mina significa que se podría incluso definir si una persona ha caído.” (TAIT, 2015)	
Seguridad y vigilancia	Sistema de radio DMR extendido, robusto y confiable, con capacidad de llamadas privadas, grupales, mensajes de texto y GPS, además de tener un sistema de gestión y control muy completo para dar trazabilidad.	Aplicaciones, Infraestructura, radios móviles, radios portátiles
Amateur	Se usa Tier 1 y Tier 2 para realizar enlaces aficionados	Aplicaciones, Infraestructura, radios móviles

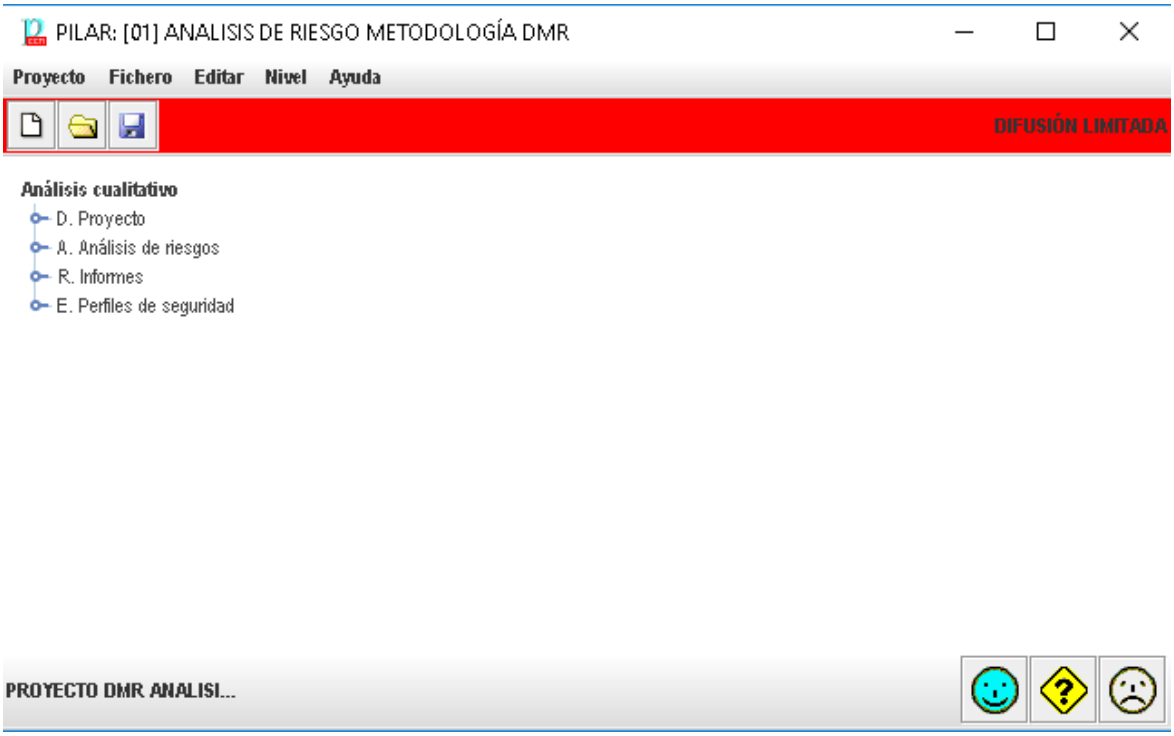
SECTOR	DESCRIPCION	CATEGORIAS DE EQUIPOS USADOS
	para establecer comunidades de comunicación.	
Construcción	Basado en la cobertura de señal, las comunicaciones entre el operador de grúa y tierra, y la vinculación de numerosas operaciones, subcontratistas y personal de seguridad en grupos de usuarios entre sí y la administración central dentro de una red. También existe el requisito de una comunicación confiable, clara e instantánea en ambientes extremadamente ruidosos y polvorientos, dentro de edificios y en espacios abiertos, sea cual sea el clima, y por supuesto, que los dispositivos de comunicación sean fáciles de usar, duraderos y resistentes. Poca utilización de servicios extendidos de datos	Aplicaciones, Infraestructura, radios móviles
Educación	solución rentable ideal para comunicaciones de radio	Aplicaciones, Infraestructura, radios móviles

SECTOR	DESCRIPCION	CATEGORIAS DE EQUIPOS USADOS
	dentro y fuera del campus; proporcionar comunicación instantánea en voz y texto entre equipos departamentales y funcionales para garantizar la seguridad y la gestión eficiente de escuelas, institutos y universidades, y se utilizan ampliamente en el sector educativo	
Salud	Proporciona comunicación instantánea en voz o datos a individuos, departamentos o grupos y ofrece una solución práctica y confiable en entornos de atención médica, ya sean cirugías, centros de salud u hospitales.	Aplicaciones, Infraestructura, radios móviles, radios portátiles, telemetría
Comercio	capacidad de llamadas privadas, grupales, mensajes de texto	radios móviles
Transporte	Sistema de radio DMR extendido, robusto y confiable, con capacidad de llamadas privadas, grupales, mensajes de texto y GPS,	Aplicaciones, Infraestructura, radios móviles, radios portátiles, telemetría

SECTOR	DESCRIPCION	CATEGORIAS DE EQUIPOS USADOS
	además de tener un sistema de gestión y control muy completo para dar trazabilidad.	
Servicios públicos	Sistema de radio DMR extendido, robusto y confiable, con capacidad de llamadas privadas, grupales, mensajes de texto y GPS, además de tener un sistema de gestión y control muy completo para dar trazabilidad.	Aplicaciones, Infraestructura, radios móviles, radios portátiles, telemetría
Energía	"Sistema de radio DMR extendido, robusto y confiable, con capacidad de llamadas privadas, grupales, mensajes de texto y GPS, además de tener un sistema de gestión y control muy completo para dar trazabilidad. Medición remota de magnitudes físicas y envío de esta información hacia el operador del sistema. Supervisión, Control y Adquisición de Datos. SCADA. Soluciones en	Aplicaciones, Infraestructura, radios móviles, radios portátiles, telemetría

SECTOR	DESCRIPCION	CATEGORIAS DE EQUIPOS USADOS
	telecomunicaciones para compañías de Oíl & Gas. Soluciones inalámbricas para aplicaciones de campo petrolíferos." (TAIT, 2015)	
Refinerías	DMR permite una comunicación instantánea y simultánea rentable con individuos y grupos de personas, asegurando un servicio confiable incluso cuando las líneas de comunicaciones por cable se vuelven inoperables por condiciones ambientales adversas o actos de sabotaje. Se usan pocas funcionalidades extendidas de datos	Aplicaciones, Infraestructura, radios móviles

M. Anexo: Parametrización inicial del software



N. Anexo: Lista de activos

id	Activo	Dimensión	Valoración	Descripción
1	FRQRADIO	D	MA	Son frecuencias contratadas a MINTIC por medio de un tercero. Son estrictamente reguladas y su afectación causa indisponibilidad total al sistema en fase 1.
2	SERVINTERNET	D	A	Los enlaces de internet son útiles para la conexión de

id	Activo	Dimensión	Valoración	Descripción
				repetidoras sitio a sitio. Son contratados a un proveedor de servicios de internet ISP y su afectación genera indisponibilidad del sistema en fase 2
3	ROUTER	D	A	Dispositivo necesario para el enrutamiento de redes hacia el centro de despacho. su afectación genera indisponibilidad del sistema en fase 2
4	ACCPOINTWIFI	D	A	Dispositivo necesario para brindar internet en zonas de complicado acceso en donde se encuentran ubicadas las receptoras. su afectación genera indisponibilidad del sistema en fase 2
5	SWITCH	D	A	Dispositivo necesario para brindar conectividad a equipos en cada fase a nivel LAN. su afectación genera indisponibilidad del sistema en fase 2 y 3.

id	Activo	Dimensión	Valoración	Descripción
6	FIREWALL	D	A	Dispositivo de seguridad usado para restringir conexiones entrantes y salientes. Su afectación genera indisponibilidad del sistema en fase 2 y 3
7	RDIOFRE	D	MA	Uso del Espectro radioeléctrico para la comunicación de radios. Su afectación causa indisponibilidad total al sistema en fase 1.
8	RADIODMR	D	A	Dispositivo final de comunicación DMR que permite el envío de paquetes de datos. Puede generar indisponibilidad por mal manejo, afectación por parte de atacante consumiendo recursos o por pérdida Afecta fase 1
9	REPETIDORADMR	D	MA	Elemento principal para la modulación de los paquetes de datos, brindar el canal para su transmisión y recepción para posterior envío a las demás fases. Su indisponibilidad

id	Activo	Dimensión	Valoración	Descripción
				afecta toda la cadena de conexión.
10	DUPLEXOR	D	A	Elemento de comunicación que aísla interferencias y permite simultaneidad en la transmisión y recepción de señales. Su indisponibilidad afecta fase 1
11	ANTENARX/TX	D	A	Elemento de comunicación que brinda cobertura que permite la transmisión y recepción de señales. Su indisponibilidad afecta fase 1
12	LAN	D	A	Conectividad local para los dispositivos en cada fase. Puede generar indisponibilidad en fase 2 y 3
13	CABLEADO	D	A	Elementos físicos de red que permiten la interconexión entre elementos. Presencia en toda la cadena de conexión
14	TRAMATCP	D	MA	Paquete de datos final enviado de la repetidora a las demás fases de conexión. El no contar con este se afectaría toda la cadena de conexión.

id	Activo	Dimensión	Valoración	Descripción
15	TDMA	D	A	Medio de transporte de señales. Su indisponibilidad afecta totalmente la fase 1
16	4FSK	D	A	Modulación de señales para ser enviadas por los slots TDMA. Su indisponibilidad no permitiría enviar paquetes de datos
17	Bluethoot	D	B	Tecnología que permite tener funcionalidades extendidas como actualización remota de firmware de terminales de radio. La indisponibilidad por denegación de servicio afectaría la capacidad de dicha tecnología.
18	GPS	D	A	Tecnología usada para ubicar equipos presentes en la red DMR. La indisponibilidad de esta afectaría esta capacidad
19	AES	D	A	Seguridad mejorada para la comunicación en general en todas las fases. Una mala configuración produciría denegación de servicio al imposibilitar abrir el paquete enviado en alguna de las fases de transporte.

id	Activo	Dimensión	Valoración	Descripción
20	PDP	D	MA	Considerado el insumo final producido por la fase 1 y su posterior envío por TCP. Sin este producto no hay datos que enviar.
21	PROTOCOLOTCP	D	A	Protocolo orientado a la conexión que permite establecer enlaces con los componentes de fase 1, 2 y 3. Su indisponibilidad presume falla a nivel de red
22	PAQDIGITALESRF	D	MA	Mensaje digital enviado por el canal que dispone la repetidora. Necesario para iniciar la preparación del paquete para que pase por las demás fases de conexión
23	PROTOCOLOUDP	D	M	Permite la validación de la condición de todos los elementos de la red DMR.
24	GEOREFER	D	A	la indisponibilidad de este Tipo de dato no permitiría referenciar geográficamente radios presentes en la red.
25	MENSTEXTO	D	A	la indisponibilidad de este Tipo de dato no permitiría notificar mensajes cortos entre

id	Activo	Dimensión	Valoración	Descripción
				terminales de radio y centro de despacho.
26	TELEMETRIA	D	A	la indisponibilidad de este Tipo de dato no permitiría la medición remota de magnitudes físicas y el posterior envío de la información hacia el operador del sistema
27	ANTIVIRUS	D	M	Puede generar indisponibilidad por una mala configuración o por ser vulnerado afectando la estación de trabajo
28	SOFTDESPACH	D	A	Puede generar indisponibilidad por una mala configuración, por vulnerabilidad o fallas de desarrollo.
29	SISTOERATIVO	D	A	Puede generar indisponibilidad por una mala configuración, por vulnerabilidad o fallas actualización.
30	MOTBASEDATOS	D	A	Puede generar indisponibilidad por una mala configuración, por vulnerabilidad o fallas de desarrollo.

id	Activo	Dimensión	Valoración	Descripción
31	SERVMONITOREO	D	A	Puede generar indisponibilidad por una mala configuración, fallas eléctricas o de componentes.
32	PC	D	A	Puede generar indisponibilidad por una mala configuración, fallas eléctricas o de componentes.
33	UPS	D	MA	Puede generar indisponibilidad por una mala instalación, fallas eléctricas o de componentes.
34	ESTACIONBASE	D	MA	Ubicación de la repetidora y de los componentes de fase1 y fase 2. Puede generar indisponibilidad por una mala configuración, fallas eléctricas o de componentes.
35	DATACENTER	D	MA	Ubicación de componentes de fase 2 y fase 3. Puede generar indisponibilidad por una mala configuración, fallas eléctricas o de componentes.
36	CENTRAL_MONITOREO	D	MA	Ubicación de radio operadores. Puede generar indisponibilidad por una mala configuración, fallas eléctricas o de componentes.

id	Activo	Dimensión	Valoración	Descripción
37	USERDESPACHADOR	D	A	Usuario inexperto o con fallas de inducción que puede generar interrupción de servicios
38	ADMRED	D	A	Usuario inexperto o que provoca errores por malas configuraciones de red y de dispositivos finales
39	ADMDMR	D	A	Usuario inexperto o que provoca errores por malas configuraciones de red DMR y de dispositivos de radio
40	USRRADIO	D	A	Riesgo alto por falta de capacitación o malas prácticas en el manejo del canal de datos que impiden la recepción de los mensajes enviados

O. Anexo: Levantamiento de activos

Capa	Nombre del Activo
[S.3rd] contratado a una tercera parte	1. [FRQRADIO] FRECUENCIAS DE RADIO 2. [SERVINTERNET] SERVICIO DE INTERNET PARA ENLACES
[COM] Redes de comunicaciones	[G1] Componentes de conectividad 3. [ROUTER] ROUTER 4. [ACCPOINTWIFI] ACCESS POINT WIFI 5. [SWITCH] SWITCH 6. [FIREWALL] FIREWALL 7. [RDIOFRE] RF [G3] Componentes de Infraestructura 8. [RADIODMR] RADIOS DMR 9. [REPETIDORADMR] REPETIDORA DMR 10. [DUPLEXOR] DUPLEXOR 11. [ANTENARX/TX] ANTENA RX/TX 12. [LAN] RED DE DATOS 13. [CABLEADO] CABLEADO
[Tech] Tecnologías o protocolos en DMR	14. [TRAMATCP] TRAMA DE DATOS TCP/IP 15. [TDMA] TDMA 16. [4FSK] 4FSK (MODULACIÓN CUARTO NIVEL) 17. [Bluethoot] Bluethoot 18. [GPS] GPS 19. [AES] AES

Capa	Nombre del Activo
	20. [PDP] PDP 21. [PROTCP] PROTOCOLO TCP 22. [PAQDIGITALESRF] PAQUETES DIGITALES RADIOFRECUENCIA DMR 23. [PROTUDP] PROTOCOLO UDP
[Dat] SERVICIOS DE DATOS	24. [MENSTEXTO] Mensaje de texto 25. [TELEMETRIA] Telemetría 26. [GEOREF] Georreferencia
[E] Equipamiento	[SW] Aplicaciones 27. [ANTIVIRUS] SOFTWARE ANTIVIRUS ESTACIONES-SERVIDOR 28. [SOFTDESPACH] SOFTWARE GESTION DMR DESPACHADOR 29. [SISTOERATIVO] SISTEMA OPERATIVO ESTACIONES-SERVIDOR 30. [MOTBASEDATOS] MOTOR BASE DE DATOS EVENTOS DE DATOS [PCS] Equipos Finales 31. [SERVMONITOREO] SERVIDOR MONITOREO 32. [PC] ESTACIÓN DE TRABAJO (PC) [AUX] Elementos auxiliares 33. [UPS] UPS
[L] Instalaciones	34. [ESTACIONBASE] ESTACIÓN BASE 35. [DATACENTER] DATACENTER 36. [CENTRAL_MONITOREO] CENTRAL_MONITOREO

Capa	Nombre del Activo
[P] Personal	37. [USERDESPACHADOR] DESPACHADOR MONITOREO 38. [ADMRED] Administrador de red interna 39. [ADMDMR] Administrador de infraestructura DMR 40. [USRRADIO] Usuario radio

P. Anexo: Lista activos en el dominio

DOMINIO	CAPA	ACTIVO	VALORACIÓN	DESCRIPCIÓN
[0PRESENCIAGRL] FASE 0 PRESENCIA EN TODA LA CADENA DE CONEXIÓN	[COM] Redes de comunicaciones	[LAN] RED DE DATOS	A	Conectividad local para los dispositivos en cada fase. Puede generar indisponibilidad en fase 2 y 3
		[CABLEADO] CABLEADO	A	Elementos físicos de red que permiten la interconexión entre elementos. Presencia en

DOMINIO	CAPA	ACTIVO	VALORACIÓN	DESCRIPCIÓN
				toda la cadena de conexión
	[TechyProt] Tecnologías o protocolos en DMR	[PROTTCP] PROTOCOLO TCP	A	Protocolo orientado a la conexión que permite establecer enlaces con los componentes de fase 1, 2 y 3. Su indisponibilidad presume falla a nivel de red
		PROTOCOLO UDP	M	Permite la validación de la condición de todos los elementos de la red DMR
	[Dat] SERVICIOS DE DATOS	[GEOREFER] Georreferencia	A	la indisponibilidad de este Tipo de dato no permitiría referenciar geográficament

DOMINIO	CAPA	ACTIVO	VALORACIÓN	DESCRIPCIÓN
				e radios presentes en la red.
		[MENSTEXTO] Mensaje de texto	A	la indisponibilidad de este Tipo de dato no permitiría notificar mensajes cortos entre terminales de radio y centro de despacho.
		[TELEMETRIA] Telemetría	A	la indisponibilidad de este Tipo de dato no permitiría la medición remota de magnitudes físicas y el posterior envío de la información hacia el

DOMINIO	CAPA	ACTIVO	VALORACIÓN	DESCRIPCIÓN
				operador del sistema
	[E] Equipamiento	[UPS] UPS	MA	Puede generar indisponibilidad por una mala instalación, fallas eléctricas o de componentes.
	capa: [P] Personal	[USERDESPACHADOR] DESPACHADOR MONITOREO	A	Usuario inexperto o con fallas de inducción que puede generar interrupción de servicios
		[ADMRED] Administrador de red interna	A	Usuario inexperto o que provoca errores por malas configuraciones de red y de dispositivos finales

DOMINIO	CAPA	ACTIVO	VALORACIÓN	DESCRIPCIÓN
		[ADMDMR] Administrador de infraestructura DMR	A	Usuario inexperto o que provoca errores por malas configuraciones de red DMR y de dispositivos de radio
		[USRRADIO] USUARIO RADIO	A	Riesgo alto por falta de capacitación o malas prácticas en el manejo del canal de datos que impiden la recepción de los mensajes enviados

DOMINIO	CAPA	ACTIVO	VALORACIÓN	DESCRIPCIÓN

[1RADIOFREQ] FASE 1 RADIOFRECUENCIA	[S.3rd] contratado a una tercera parte	[FRQRADIO] FRECUENCIAS DE RADIO	MA	Son frecuencias contratadas a MINTIC por medio de un tercero. Son estrictamente reguladas y su afectación causa indisponibilidad total al sistema en fase 1.
	[COM] Redes de comunicaciones	[ACCPOINTWIFI] ACCESS POINT WIFI	A	(1) Dispositivo necesario para brindar internet en zonas de complicado acceso en donde se encuentran ubicadas las receptoras. su afectación genera indisponibilidad del sistema en fase 2
		[RDIOFRE] RF	MA	(2) Uso del Espectro radioeléctrico para la comunicación de radios. Su afectación causa indisponibilidad

				total al sistema en fase 1.
		[RADIODMR] RADIOS DMR	A	(3) Dispositivo final de comunicación DMR que permite el envío de paquetes de datos. Puede generar indisponibilidad por mal manejo, afectación por parte de atacante consumiendo recursos o por pérdida Afecta fase 1
		[REPETIDORADMR] REPETIDORA DMR	MA	(4) Elemento principal para la modulación de los paquetes de datos, brindar el canal para su transmisión y recepción para posterior envío a las demás fases. Su indisponibilidad

				afecta toda la cadena de conexión.
		[DUPLEXOR] DUPLEXOR	A	(5) Elemento de comunicación que aísla interferencias y permite simultaneidad en la transmisión y recepción de señales. Su indisponibilidad afecta fase 1
		[ANTENARX/TX] ANTENA RX/TX	A	(6) Elemento de comunicación que brinda cobertura y que permite la transmisión y recepción de señales. Su indisponibilidad afecta fase 1
	[TechyProt] Tecnologías o protocolos en DMR	[TDMA] TDMA	A	Protocolo de transporte de señales. Su indisponibilidad afecta totalmente la fase 1

		[4FSK] 4FSK (MODULACIÓN CUARTO NIVEL)	A	Modulación de señales para ser enviadas por los slots TDMA. Su indisponibilidad no permitiría enviar paquetes de datos
		[Bluethoot] Bluethoot	B	Tecnología que permite tener funcionalidades extendidas como actualización remota de firmware de terminales de radio. La indisponibilidad por denegación de servicio afectaría la capacidad de dicha tecnología.
		[GPS] GPS	A	Tecnología usada para ubicar equipos presentes en la red DMR. La indisponibilidad de esta afectaría esta capacidad

		[PDP] PDP	MA	Considerado el insumo final producido por la fase 1 y su posterior envío por TCP. Sin este producto no hay datos que enviar.
		[PAQDIGITALESRF] PAQUETES DIGITALES RADIOFRECUENCIA DMR	MA	Mensaje digital enviado por el canal que dispone la repetidora. Necesario para iniciar la preparación del paquete para que pase por las demás fases de conexión
	[L] Instalaciones	[ESTACIONBASE] ESTACIÓN BASE	MA	Ubicación de la repetidora y de los componentes de fase1 y fase 2. Puede generar indisponibilidad por una mala configuración, fallas eléctricas o de componentes.

DOMINIO	CAPA	ACTIVO	VALORACIÓN	DESCRIPCIÓN
[2TCP/IP] FASE 2 ENLACES TCP/IP	[S.3rd] contratado a una tercera parte	[SERVINTERNET] SERVICIO DE INTERNET PARA ENLACES	A	Los enlaces de internet son útiles para la conexión de repetidoras sitio a sitio. Son contratadas a un proveedor de servicios de internet ISP y su afectación genera indisponibilidad del sistema en fase 2
	[COM] Redes de comunicaciones	[ROUTER] ROUTER	A	Dispositivo necesario para el enrutamiento de redes hacia el centro de despacho. su afectación genera indisponibilidad del sistema en fase 2

	[TechyProt] Tecnologías o protocolos en DMR	[TRAMATCP] PAQUETE DE DATOS DE RED	MA	Paquete de datos final enviado de la repetidora a las demás fases de conexión. El no contar con este se afectaría toda la cadena de conexión.
		[AES] AES	A	Seguridad mejorada para la comunicación en general en todas las fases. Una mala configuración produciría denegación de servicio al imposibilitar abrir el paquete enviado en alguna de las fases de transporte.

DOMINIO	**CAPA**	**ACTIVO**	**VALORACIÓN**	**DESCRIPCIÓN**

[3CENTDESPACHO] FASE 3 CENTRO DE DESPACHO	[COM] Redes de comunicaciones	[SWITCH] SWITCH	A	Dispositivo necesario para brindar conectividad a equipos en cada fase a nivel LAN. su afectación genera indisponibilidad del sistema en fase 2 y 3.
		[FIREWALL] FIREWALL	A	Dispositivo de seguridad usado para restringir conexiones entrantes y salientes. Su afectación genera indisponibilidad del sistema en fase 2 y 3
	[E] Equipamiento	[ANTIVIRUS] SOFTWARE ANTIVIRUS ESTACIONES-SERVIDOR	M	Puede generar indisponibilidad por una mala configuración o por ser vulnerado afectando la estación de trabajo
		[SOFTDESPACH] SOFTWARE	A	Puede generar indisponibilidad por una mala

		GESTION DMR DESPACHADOR		configuración, por vulnerabilidad o fallas de desarrollo.
		[SISTOERATIVO] SISTEMA OPERATIVO ESTACIONES-SERVIDOR	A	Puede generar indisponibilidad por una mala configuración, por vulnerabilidad o fallas actualización.
		[MOTBASEDATOS] MOTOR BASE DE DATOS EVENTOS DE DATOS	A	Puede generar indisponibilidad por una mala configuración, por vulnerabilidad o fallas de desarrollo.
		[SERVMONITOREO] SERVIDOR MONITOREO	A	Puede generar indisponibilidad por una mala configuración, fallas eléctricas o de componentes.
		[PC] ESTACIÓN DE TRABAJO (PC)	A	Puede generar indisponibilidad por una mala

				configuración, fallas eléctricas o de componentes.
	[L] Instalaciones	[DATACENTER] DATACENTER	MA	Ubicación de componentes de fase 2 y fase 3. Puede generar indisponibilidad por una mala configuración, fallas eléctricas o de componentes.
		[CENTRAL_MONITOREO] CENTRAL_MONITOREO	MA	Ubicación de radio operadores. Puede generar indisponibilidad por una mala configuración, fallas eléctricas o de componentes.

Q. Anexo: Funcionamiento de aplicación PILAR análisis de riesgo

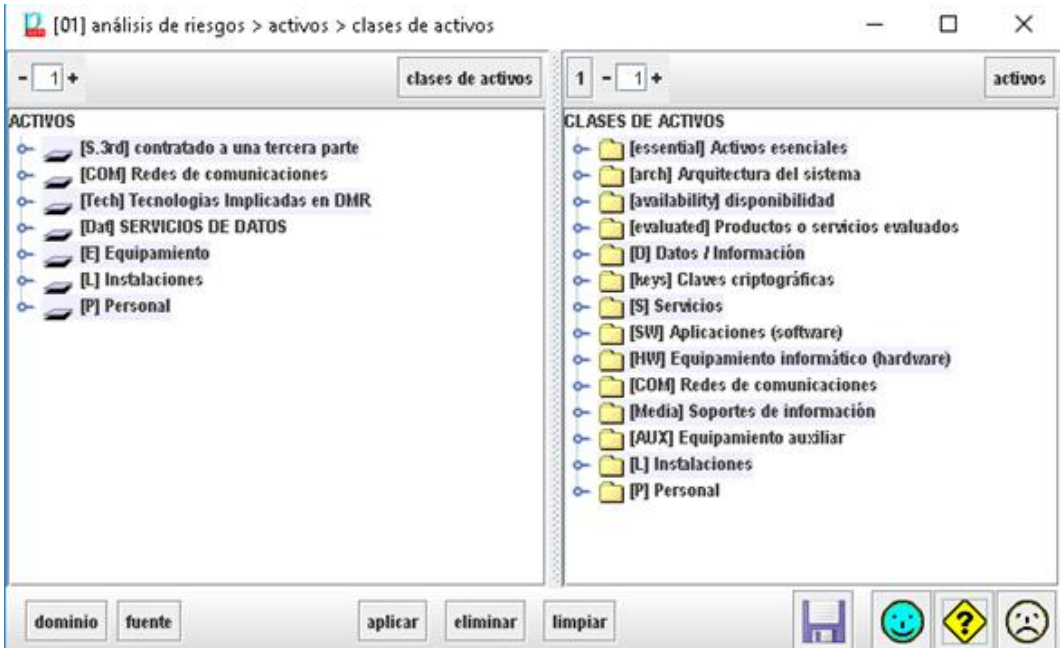
biblioteca [ME] Biblioteca INFOSEC (26.5.2012) (cM_71.p5)
código 01
nombre ANALISIS DE RIESGO METODOLOGÍA DMR
proyecto - clasificación DIFUSIÓN LIMITADA

dato	valor
Organización	ORGANIZACIÓN CON INFRAESTRUCTURA DMR
Descripción	EVALUAR SERVICIOS Y TECNOLOGÍAS IMPLICADAS EN LA CADENA DE CONEXIÓN DMR
Autor	SERGIO ALVAREZ-OSCAR URREA
Versión	1
Fecha	7/11/18
Responsable del Sistema	ORGANIZACIÓN CON INFRAESTRUCTURA DMR
Responsable de la Seguridad de la Información	EQUIPO DE INVESTIGACIÓN
Delegado de Protección de Datos	EQUIPO DE INVESTIGACIÓN

R. Anexo: Dominios de seguridad en la herramienta PILAR

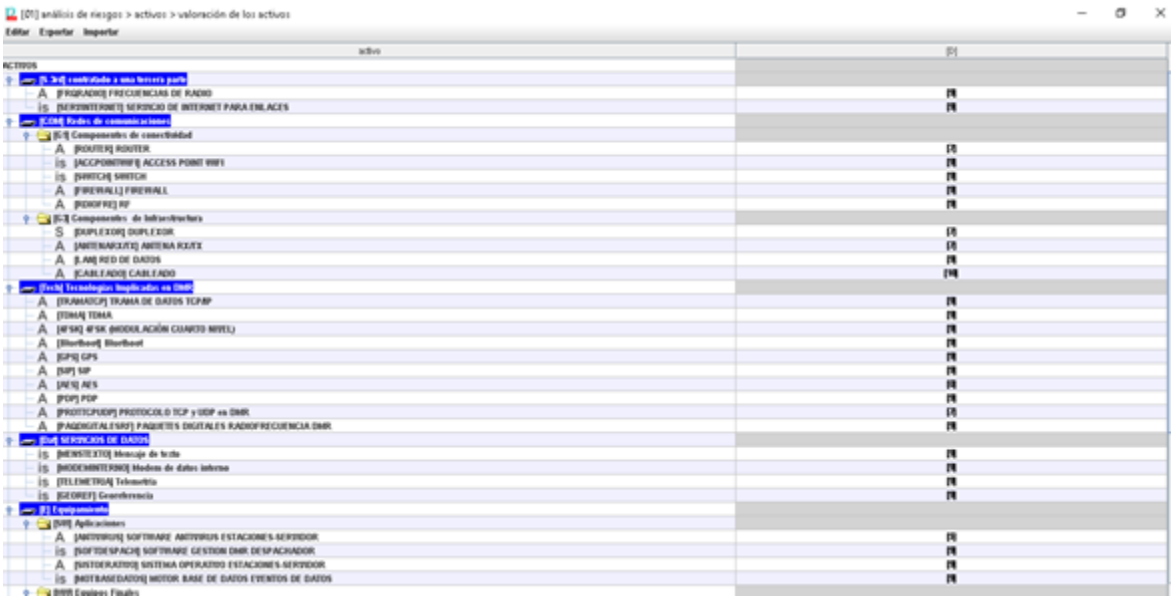
S. Anexo: Análisis de riegos en el proceso de identificación en la herramienta PILAR

T. Anexo: Análisis de riesgos en el proceso de clasificación de activos

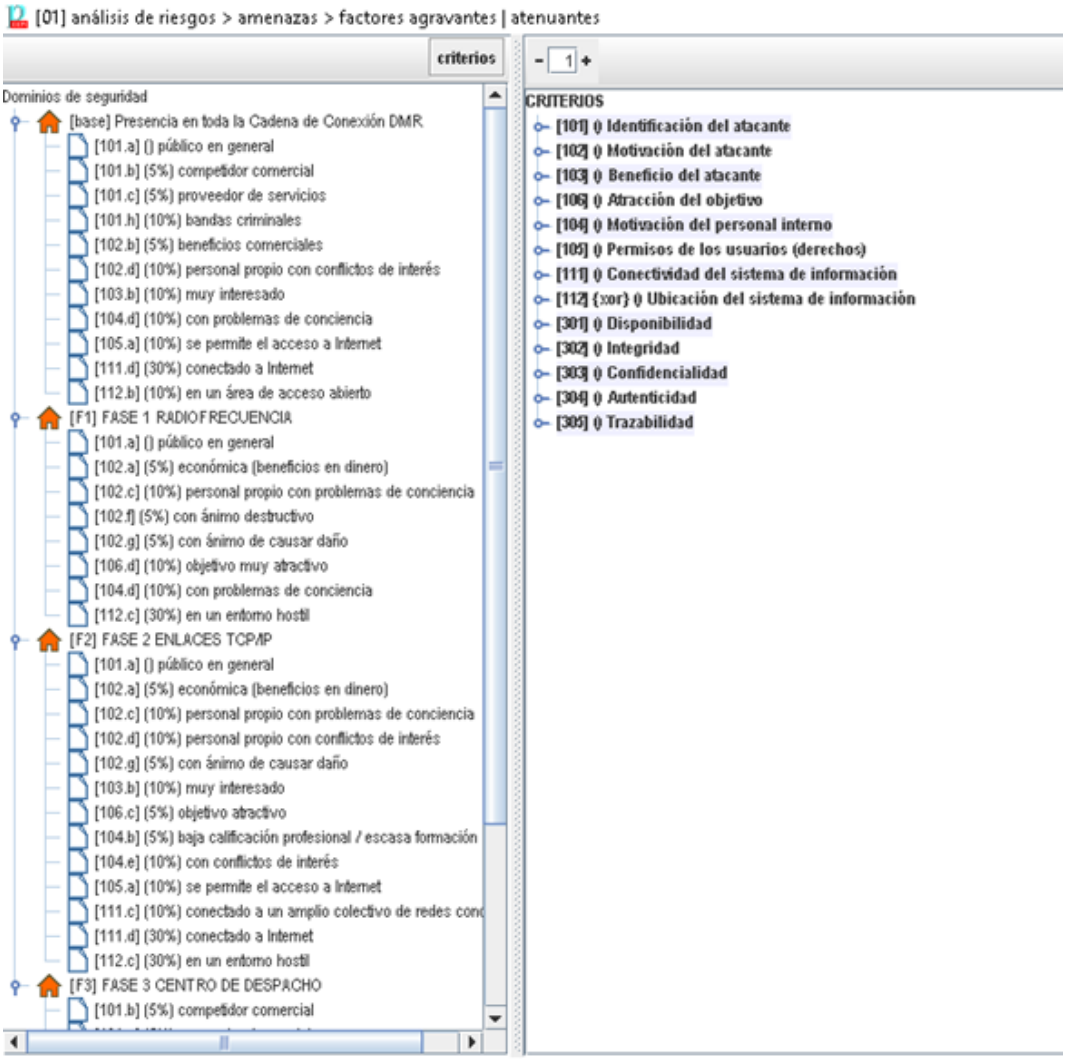


U. Anexo: Valoración de dominios en la herramienta PILAR

V. Anexo: Valoración de activos en la herramienta PILAR



W. Anexo: Amenazas y sus factores agravantes en la herramienta PILAR



X. Anexo: Amenazas de activos y valoración

Amenaza	**Probabilidad**	**Dimensión**
[FRQRADIO] FRECUENCIAS DE RADIO	M	MA
Amenaza	**Probabilidad**	**[D]**
[E.4] Errores de configuración	M	MA
[A.40] Incumplimiento (leyes, reglamentos, normas, ...)	M	A
[SERVINTERNET] SERVICIO DE INTERNET PARA ENLACES	M	MA
Amenaza	**Probabilidad**	**[D]**
[E.2] Errores del administrador del sistema / de la seguridad	M	A
[E.4] Errores de configuración	M	MA
[E.8] Difusión de software dañino	M	MA
[A.12] Análisis de tráfico	M	MA
[A.14] Interceptación de información (escucha)	M	MA

[A.24] Denegación de servicio	M	A
[A.40] Incumplimiento (leyes, reglamentos, normas, ...)	M	B
[ROUTER] ROUTER	M	MA
amenaza	probabilidad	[D]
[I.5] Avería de origen físico o lógico	M	A
[I.6] Corte del suministro eléctrico	M	T
[I.7] Condiciones inadecuadas de temperatura o humedad	M	T
[I.8] Fallo de servicios de comunicaciones	M	T
[E.2] Errores del administrador del sistema / de la seguridad	M	M
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M
[E.24] Caída del sistema por agotamiento de recursos	A	A
[A.7] Uso no previsto	M	M

[A.23] Manipulación del hardware	M	T
[A.24] Denegación de servicio	A	T
[ACCPOINTWIFI] ACCESS POINT WIFI	M	A
amenaza	probabilidad	[D]
[I.4.31] Jamming	M	A
[I.5] Avería de origen físico o lógico	M	A
[I.8] Fallo de servicios de comunicaciones	M	A
[E.2] Errores del administrador del sistema / de la seguridad	M	A
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M
[SWITCH] SWITCH	M	A
amenaza	probabilidad	[D]
[I.5] Avería de origen físico o lógico	M	A

[I.8] Fallo de servicios de comunicaciones	M	A
[E.2] Errores del administrador del sistema / de la seguridad	B	A
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	M
[FIREWALL] FIREWALL	M	MA
amenaza	probabilidad	[D]
[I.8] Fallo de servicios de comunicaciones	M	A
[E.2] Errores del administrador del sistema / de la seguridad	M	A
[E.4] Errores de configuración	A	A
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	A
[A.4] Manipulación de los ficheros de configuración	M	A
[A.24] Denegación de servicio	A	MA
[RDIOFRE] RF	A	MA

amenaza	probabilidad	[D]
[I.4.31] Jamming	A	MA
[I.8] Fallo de servicios de comunicaciones	M	A
[E.1] Errores de los usuarios	M	M
[E.24] Caída del sistema por agotamiento de recursos	M	MA
[A.5] Suplantación de la identidad	A	MA
[A.10] Alteración de secuencia	B	A
[A.14] Interceptación de información (escucha)	B	M
[A.19] Revelación de información	M	A
[A.24] Denegación de servicio	A	T
[A.40] Incumplimiento (leyes, reglamentos, normas, ...)	A	T
[RADIODMR] RADIOS DMR	M	A
amenaza	probabilidad	[D]

[I.5] Avería de origen físico o lógico	M	M
[I.5.3] Equipos de comunicaciones	M	M
[I.8] Fallo de servicios de comunicaciones	M	M
[E.1] Errores de los usuarios	B	M
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	A
[E.25] Pérdida de equipos	M	M
[A.5] Suplantación de la identidad	M	M
[REPETIDORADMR] REPETIDORA DMR	A	MA
amenaza	probabilidad	[D]
[I.5] Avería de origen físico o lógico	M	MA
[I.5.3] Equipos de comunicaciones	A	A
[I.6] Corte del suministro eléctrico	M	MA
[I.7] Condiciones inadecuadas de temperatura o humedad	M	MA

[I.8] Fallo de servicios de comunicaciones	M	MA
[E.2] Errores del administrador del sistema / de la seguridad	M	MA
[E.4] Errores de configuración	M	MA
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	MA
[E.24] Caída del sistema por agotamiento de recursos	M	MA
[A.23] Manipulación del hardware	M	MA
[A.25] Robo de equipos	M	T
[DUPLEXOR] DUPLEXOR	M	A
amenaza	probabilidad	[D]
[I.4] Contaminación electromagnética	M	M
[I.5] Avería de origen físico o lógico	M	A
[I.8] Fallo de servicios de comunicaciones	M	A

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M
[A.7] Uso no previsto	M	A
[A.23] Manipulación del hardware	M	A
[ANTENARX/TX] ANTENA RX/TX	M	MA
amenaza	probabilidad	[D]
[I.5] Avería de origen físico o lógico	M	A
[I.7] Condiciones inadecuadas de temperatura o humedad	M	T
[I.8] Fallo de servicios de comunicaciones	M	A
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M
[A.7] Uso no previsto	M	A
[A.23] Manipulación del hardware	M	A
[LAN] RED DE DATOS	A	MA
amenaza	probabilidad	[D]

[I.5] Avería de origen físico o lógico	M	A
[I.6] Corte del suministro eléctrico	M	T
[I.8] Fallo de servicios de comunicaciones	M	A
[E.2] Errores del administrador del sistema / de la seguridad	M	M
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M
[E.24] Caída del sistema por agotamiento de recursos	A	A
[A.7] Uso no previsto	M	A
[A.23] Manipulación del hardware	M	A
[A.24] Denegación de servicio	A	T
[A.26] Ataque destructivo	M	T
[CABLEADO] CABLEADO	B	M
amenaza	probabilidad	[D]
[N] Desastres naturales	B	B

[I.5.3] Equipos de comunicaciones	B	M
[TRAMATCP] PAQUETE DE DATOS DE RED	A	MA
amenaza	probabilidad	[D]
[E.9] Errores de [re-]encaminamiento	M	A
[A.10] Alteración de secuencia	M	A
[A.12] Análisis de tráfico	A	MA
[A.14] Interceptación de información (escucha)	M	M
[A.15] Modificación de la información	M	M
[A.18] Destrucción de la información	M	A
[A.24] Denegación de servicio	M	A
[TDMA] TDMA	A	MA
amenaza	probabilidad	[D]
[I.4] Contaminación electromagnética	A	A
[I.8] Fallo de servicios de comunicaciones	A	A

[E.10] Errores de secuencia	M	A
[E.24] Caída del sistema por agotamiento de recursos	M	MA
[A.18] Destrucción de la información	A	MA
[A.24] Denegación de servicio	A	T
[4FSK] 4FSK (MODULACIÓN CUARTO NIVEL)	M	A
amenaza	probabilidad	[D]
[E.10] Errores de secuencia	M	A
[A.24] Denegación de servicio	M	A
[Bluethoot] Bluethoot	A	A
amenaza	probabilidad	[D]
[A.5] Suplantación de la identidad	M	A
[A.8] Difusión de software dañino	M	A
[A.9] [Re-]encaminamiento de mensajes	M	A
[A.10] Alteración de secuencia	M	M

[A.14] Interceptación de información (escucha)	M	A
[A.15] Modificación de la información	M	M
[A.24] Denegación de servicio	A	M
[GPS] GPS	A	A
amenaza	probabilidad	[D]
[I.8] Fallo de servicios de comunicaciones	A	A
[E.24] Caída del sistema por agotamiento de recursos	M	A
[A.24] Denegación de servicio	A	A
[AES] AES	M	A
amenaza	probabilidad	[D]
[A.10] Alteración de secuencia	M	A
[A.12.3] Por personas externas	M	A
[PDP] PDP	A	MA
amenaza	probabilidad	[D]
[I.8] Fallo de servicios de comunicaciones	M	MA

[E.24] Caída del sistema por agotamiento de recursos	A	MA
[A.24] Denegación de servicio	A	T
[PROTTCP] PROTOCOLO TCP	A	A
amenaza	probabilidad	[D]
[I.8] Fallo de servicios de comunicaciones	M	A
[E.2] Errores del administrador del sistema / de la seguridad	M	M
[E.24] Caída del sistema por agotamiento de recursos	M	A
[A.7] Uso no previsto	M	M
[A.24] Denegación de servicio	A	A
[PAQDIGITALESRF] PAQUETES DIGITALES RADIOFRECUENCIA DMR	A	MA
amenaza	probabilidad	[D]
[I.4] Contaminación electromagnética	A	MA
[I.4.31] Jamming	A	MA

[E.24] Caída del sistema por agotamiento de recursos	A	MA
[A.12] Análisis de tráfico	A	MA
[A.24] Denegación de servicio	A	MA
[PROTUDP] PROTOCOLO UDP	A	B
amenaza	probabilidad	[D]
[E.18] Destrucción de la información	M	B
[A.6] Abuso de privilegios de acceso	A	B
[GEOREFER] Georreferencia	M	A
amenaza	probabilidad	[D]
[I.8.11] Interrupción accidental	M	A
[I.8.12] Interrupción deliberada por un agente externo	M	A
[I.8.13] Interrupción deliberada por un agente interno	M	A
[E] Errores y fallos no intencionados	M	A

[E.24] Caída del sistema por agotamiento de recursos	M	A
[A.7] Uso no previsto	M	A
[A.24] Denegación de servicio	M	A
[A.26] Ataque destructivo	B	M
[MENSTEXTO] Mensaje de texto	M	A
amenaza	probabilidad	[D]
[I.8.11] Interrupción accidental	M	A
[I.8.12] Interrupción deliberada por un agente externo	M	A
[I.8.13] Interrupción deliberada por un agente interno	M	A
[E] Errores y fallos no intencionados	M	A
[E.24] Caída del sistema por agotamiento de recursos	M	A
[A.7] Uso no previsto	M	A
[A.24] Denegación de servicio	M	A

[A.26] Ataque destructivo	M	A
[TELEMETRIA] Telemetría	A	A
amenaza	probabilidad	[D]
[I.8.11] Interrupción accidental	M	A
[I.8.12] Interrupción deliberada por un agente externo	M	A
[I.8.13] Interrupción deliberada por un agente interno	M	A
[E] Errores y fallos no intencionados	M	M
[E.24] Caída del sistema por agotamiento de recursos	A	A
[A.7] Uso no previsto	A	M
[A.24] Denegación de servicio	M	A
[A.26] Ataque destructivo	B	A
[ANTIVIRUS] SOFTWARE ANTIVIRUS ESTACIONES-SERVIDOR	A	MA
amenaza	probabilidad	[D]

[E.4] Errores de configuración	M	B
[E.21] Errores de mantenimiento / actualización de programas (software)	M	M
[A.24] Denegación de servicio	A	MA
[A.24.2] Saturación de los recursos software	M	M
[SOFTDESPACH] SOFTWARE GESTION DMR DESPACHADOR	A	M
amenaza	probabilidad	[D]
[E] Errores y fallos no intencionados	M	M
[E.4] Errores de configuración	M	M
[E.20] Vulnerabilidades de los programas (software)	M	M
[E.21] Errores de mantenimiento / actualización de programas (software)	A	M
[E.24] Caída del sistema por agotamiento de recursos	M	M

[SISTOERATIVO] SISTEMA OPERATIVO ESTACIONES-SERVIDOR	M	A
amenaza	probabilidad	[D]
[E.4] Errores de configuración	M	M
[E.20] Vulnerabilidades de los programas (software)	M	A
[E.21] Errores de mantenimiento / actualización de programas (software)	M	M
[E.24] Caída del sistema por agotamiento de recursos	MB	M
[A.6] Abuso de privilegios de acceso	M	M
[A.22] Manipulación de programas	M	M
[A.24] Denegación de servicio	M	M
[MOTBASEDATOS] MOTOR BASE DE DATOS EVENTOS DE DATOS	M	A
amenaza	probabilidad	[D]
[E.4] Errores de configuración	M	M

[E.20] Vulnerabilidades de los programas (software)	M	A
[E.21] Errores de mantenimiento / actualización de programas (software)	B	M
[E.24] Caída del sistema por agotamiento de recursos	M	M
[A.3] Manipulación de los registros de actividad (log)	B	M
[A.4] Manipulación de los ficheros de configuración	MB	A
[A.6] Abuso de privilegios de acceso	M	A
[A.22] Manipulación de programas	M	M
[A.24] Denegación de servicio	M	A
[SERVMONITOREO] SERVIDOR MONITOREO	M	A
amenaza	probabilidad	[D]
[I.5] Avería de origen físico o lógico	M	A
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	A

[E.24] Caída del sistema por agotamiento de recursos	M	A
[A.4] Manipulación de los ficheros de configuración	M	A
[A.7] Uso no previsto	M	A
[A.11] Acceso no autorizado	M	A
[A.18] Destrucción de la información	B	A
[PC] ESTACIÓN DE TRABAJO (PC)	A	MA
amenaza	probabilidad	[D]
[N.1] Fuego	B	T
[N.2] Daños por agua	B	A
[I.4] Contaminación electromagnética	M	M
[I.5] Avería de origen físico o lógico	M	A
[I.6] Corte del suministro eléctrico	M	T
[I.7] Condiciones inadecuadas de temperatura o humedad	M	T

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M
[E.24] Caída del sistema por agotamiento de recursos	A	A
[E.25] Pérdida de equipos	A	T
[A.6] Abuso de privilegios de acceso	M	M
[A.7] Uso no previsto	M	M
[A.11] Acceso no autorizado	M	M
[A.23] Manipulación del hardware	M	A
[A.24] Denegación de servicio	A	T
[A.25] Robo de equipos	A	T
[A.26] Ataque destructivo	M	T
[UPS] UPS	M	M
amenaza	probabilidad	[D]
[I.5.2] Hardware	M	M
[I.6] Corte del suministro eléctrico	M	M
[ESTACIONBASE] ESTACIÓN BASE	M	MA

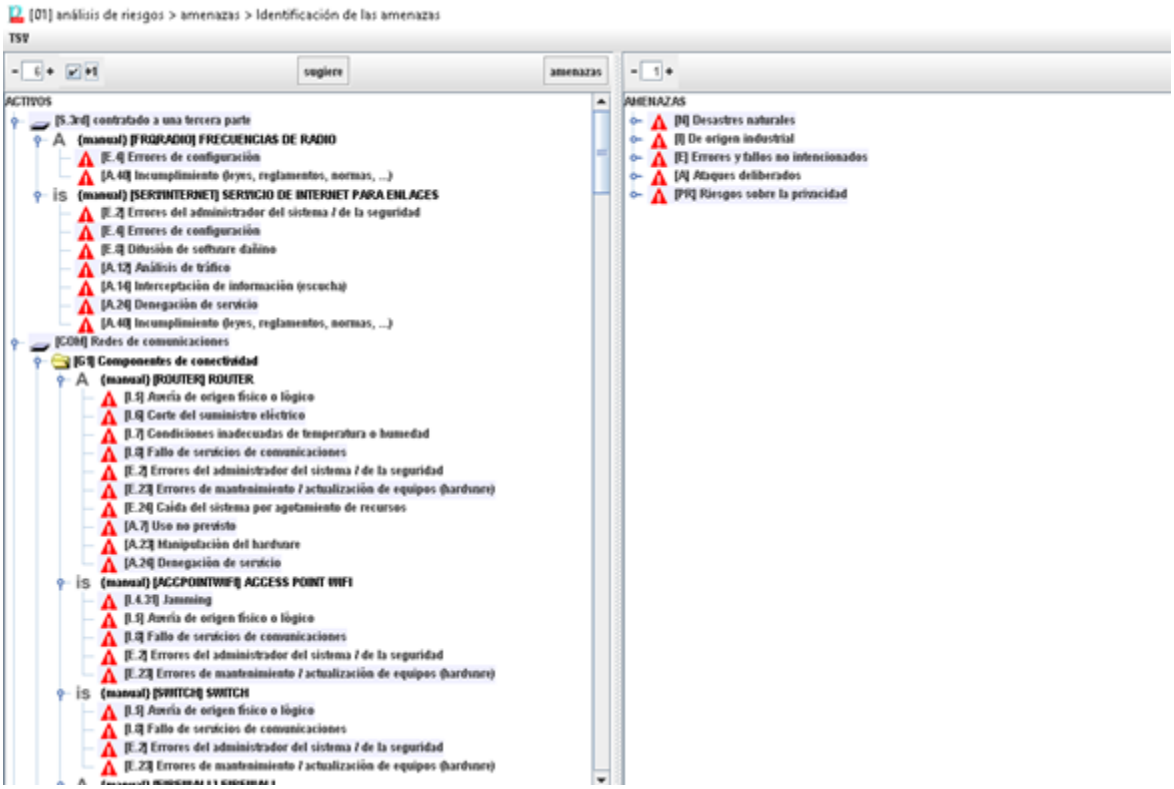
amenaza	probabilidad	[D]
[N] Desastres naturales	MB	A
[I.4] Contaminación electromagnética	M	MA
[I.6] Corte del suministro eléctrico	M	T
[I.7] Condiciones inadecuadas de temperatura o humedad	M	T
[E.25] Pérdida de equipos	M	T
[A.6] Abuso de privilegios de acceso	M	M
[A.7] Uso no previsto	M	M
[A.23] Manipulación del hardware	M	A
[A.25] Robo de equipos	M	T
[A.26] Ataque destructivo	M	T
[DATACENTER] DATACENTER	M	MA
amenaza	probabilidad	[D]
[N.1] Fuego	M	T
[N.2] Daños por agua	M	T

[I.4] Contaminación electromagnética	B	M
[A.6] Abuso de privilegios de acceso	M	M
[A.7] Uso no previsto	M	M
[A.26] Ataque destructivo	B	T
[A.27] Ocupación enemiga	M	T
[CENTRAL_MONITOREO] CENTRAL_MONITOREO	M	MA
amenaza	probabilidad	[D]
[N.1] Fuego	M	T
[N.2] Daños por agua	M	T
[I.4] Contaminación electromagnética	B	M
[A.6] Abuso de privilegios de acceso	B	M
[A.7] Uso no previsto	B	M
[A.26] Ataque destructivo	B	T
[A.27] Ocupación enemiga	M	T
[USERDESPACHADOR] DESPACHADOR MONITOREO	M	A
amenaza	probabilidad	[D]

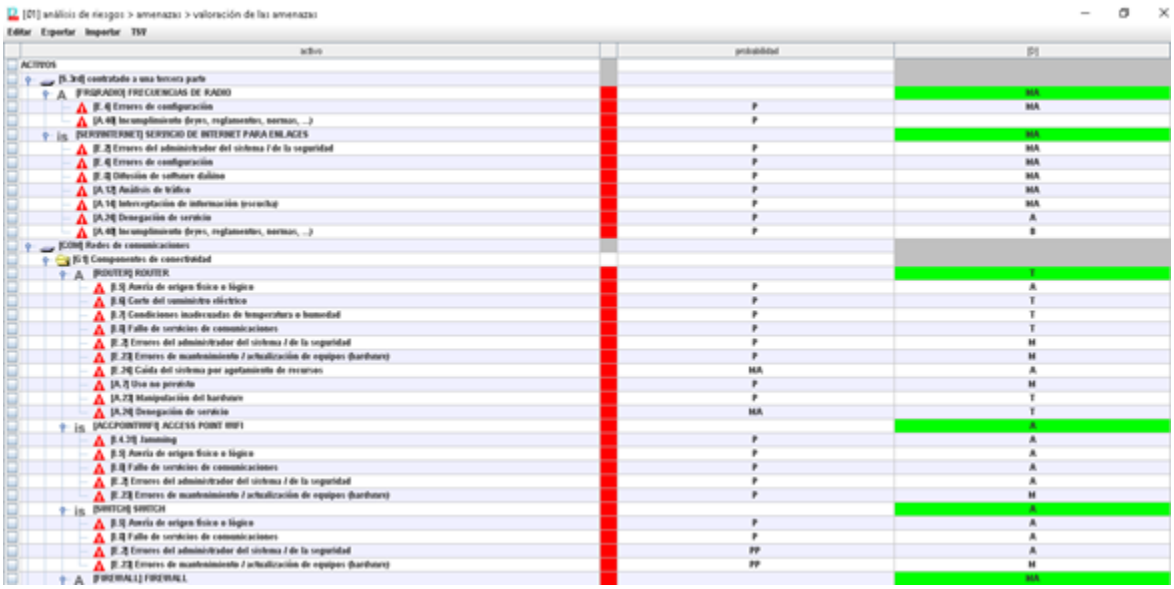
[E.28] Indisponibilidad del personal	M	A
[A.30] Ingeniería social (picaresca)	M	A
[ADMRED] Administrador de red interna	A	MA
amenaza	probabilidad	[D]
[E.2] Errores del administrador del sistema / de la seguridad	A	MA
[E.28] Indisponibilidad del personal	M	M
[A.30] Ingeniería social (picaresca)	B	MA
[ADMDMR] Administrador de infraestructura DMR	M	MA
amenaza	probabilidad	[D]
[E.2] Errores del administrador del sistema / de la seguridad	M	MA
[E.21] Errores de mantenimiento / actualización de programas (software)	M	MA
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	MA

[E.28] Indisponibilidad del personal	M	M
[A.30] Ingeniería social (picaresca)	B	A
[USRRADIO] USUARIO RADIO	M	A
amenaza	probabilidad	[D]
[E.18] Destrucción de la información	M	B
[E.28] Indisponibilidad del personal	M	M
[A.18] Destrucción de la información	M	M
[A.28] Indisponibilidad del personal	M	A
[A.29] Extorsión	M	M
[A.30] Ingeniería social (picaresca)	M	M

Y. Anexo: Identificación de amenazas en la herramienta PILAR



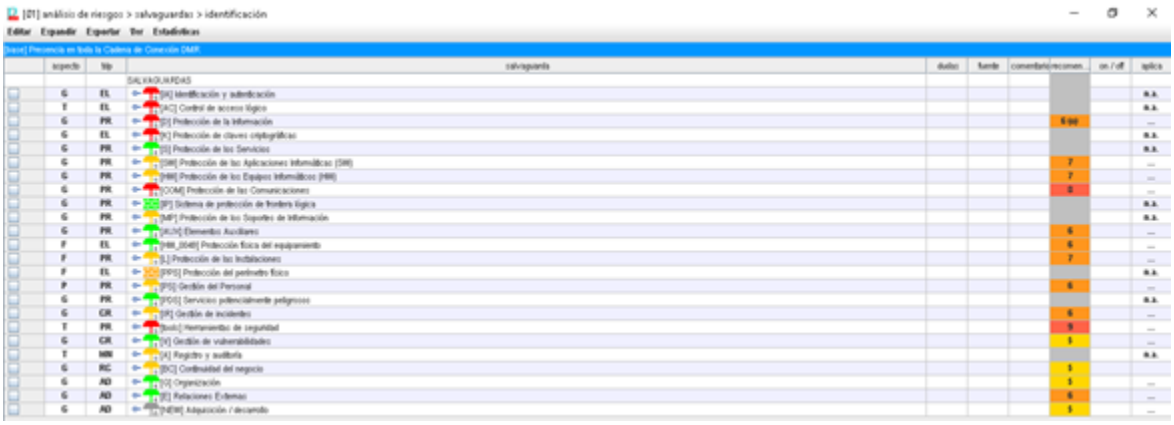
Z. Anexo: Valoración de amenazas en la herramienta PILAR



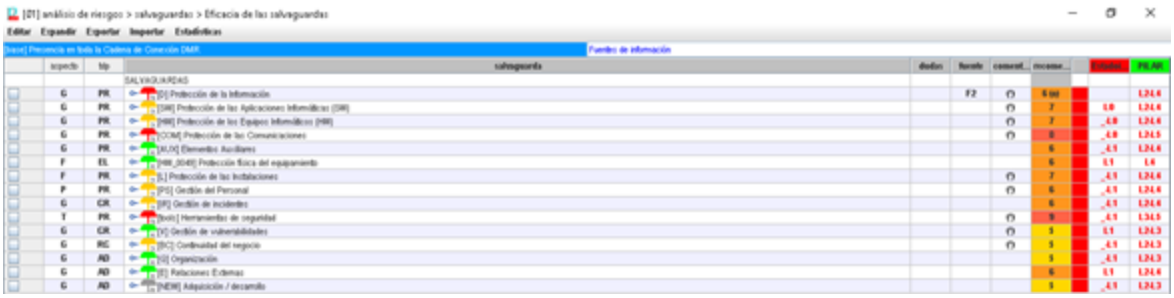
AA. Anexo: Evaluación según la probabilidad de ocurrencia en la herramienta PILAR

AB. Anexo: Evaluación según el impacto a la disponibilidad de la transmisión de datos en la herramienta PILAR

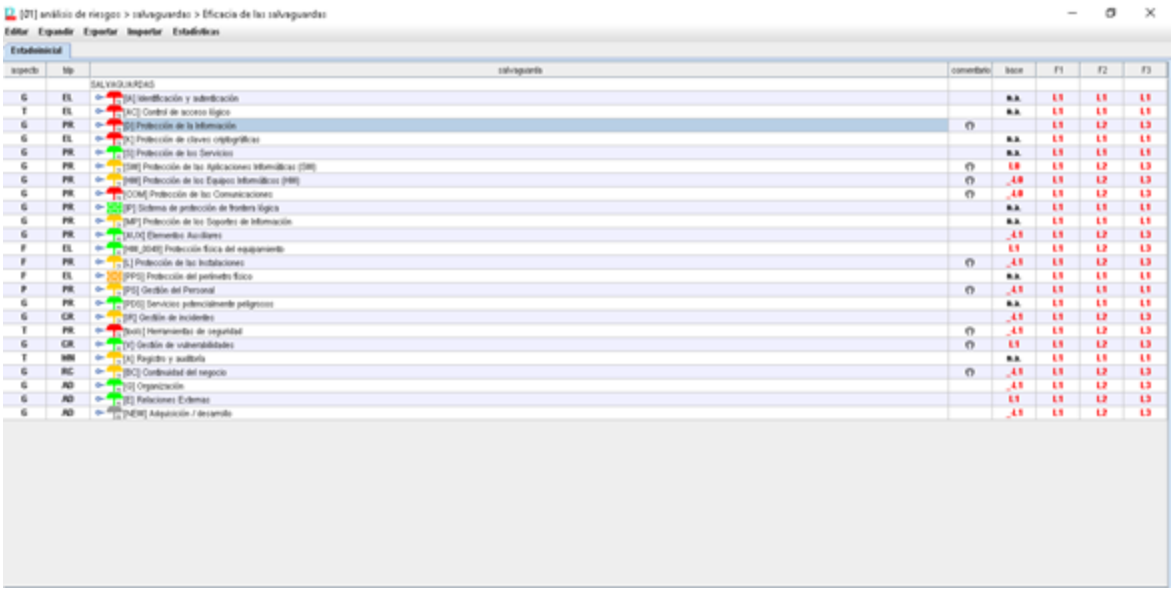
AC. Anexo: Identificación de salvaguardas en la herramienta PILAR



AD. Anexo: Valoración estado inicial y madurez de las salvaguardas en la herramienta PILAR



AE. Anexo: Valoración de salvaguardas y estado de madurez en la herramienta PILAR



AF. Anexo: Salva guardas por dominio

DOMINIO DE SEGURIDAD	CÓDIGO	SALVAGUARDA	VALORACIÓN	POTENCIAL	OBJETIVO FINAL
[0PRESENCIAGRL] FASE 0 PRESENCIA EN TODA LA CADENA DE CONEXIÓN	HW	Protección de los Equipos Informáticos (HW)	A	L0	L2-L4
	HW.SC	Se aplican perfiles de seguridad	A	L0	L3-L4
	HW. cont	Aseguramiento de la disponibilidad	M	L0	L2-L4
	HW.cont.1	Se dimensiona holgadamente y se planifica la adquisición de repuestos	M	L0	L4
	COM	Protección de las Comunicaciones	A	L0	L2-L5
	COM.SC	Se aplican perfiles de seguridad	A	L0	L4-L5
	COM.cont	Aseguramiento de la disponibilidad	M	L0	L2-L4
	COM.cont.1	Se identifican y evitan "puntos únicos de	M	L0	L4

DOMINIO DE SEGURIDAD	CÓDIGO	SALVAGUARDA	VALORACIÓN	POTENCIAL	OBJETIVO FINAL
		fallo" (SPF-Single Point of Failure)			
	COM.DS	Segregación de las redes en dominios	M	L0	L3-L4
	AUX	Elementos Auxiliares	M	L1	L2-L4
	AUX.start	Instalación	M	L1	L4
	AUX.wires	Protección del cableado	M	L1	L3-L4
	AUX.8	Se prevén medidas frente a todos los problemas graves identificados en el análisis de riesgos	M	L1	L4
	HW_0049	Protección física del equipamiento	M	n.a.	L4
	PS	Gestión del Personal	M	L1	L2-L4
	PS.8	Procedimientos de prevención y reacción	M	L1	L4
	PS.8.2	frente a phishing	M	L1	L4
	PS.8.3	frente a extorsión	M	L1	L4
	PS.8.4	frente a ataques de ingeniería social	M	L1	L4

DOMINIO DE SEGURIDAD	CÓDIGO	SALVAGUARDA	VALORACIÓN	POTENCIAL	OBJETIVO FINAL
	IR	Gestión de incidentes	M	L1	L2-L4
	IR.3	Contención del incidente	M	L1	L3-L4
	IR.3.3	Se suspenden cautelarmente los trabajos en el sistema afectado	M	L1	L4
	IR.3.4	Se aísla cautelarmente el sistema afectado	M	L1	L4
	tools	Herramientas de seguridad	M	n.a.	L3-L4
	tools.IDS	IDS/IPS: Herramienta de detección / prevención de intrusión	M	n.a.	L3-L4
	tools.traffic	Herramienta de monitorización de tráfico	M	n.a.	L3-L4
	E	Relaciones Externas	M	L1	L2-L4
	E.1	Acuerdos para intercambio de información y software	M	L1	L3-L4

Dominio de seguridad	CÓDIGO	SALVAGUARDA	VALORACIÓN	POTENCIAL	OBJETIVO FINAL
[1RADIOFREQ] FASE 1 RADIOFRECUENCIA	S	Protección de los Servicios	M	L1	L2-L4
	S.1	Prestación de los servicios	M	L1	L2-L4
	S.SC	Se aplican perfiles de seguridad	M	L1	L3-L4
	S.2	Servicios subcontratados	M	L1	L2-L4
	S.2.6	Continuidad de operaciones	M	L1	L3-L4
	HW	Protección de los Equipos Informáticos (HW)	A	L1	L2-L4
	HW.SC	Se aplican perfiles de seguridad	A	L1	L3-L4
	HW.cont	Aseguramiento de la disponibilidad	M	L1	L2-L4
	HW.cont.1	Se dimensiona holgadamente y se planifica la adquisición de repuestos	M	L1	L4

	COM	Protección de las Comunicaciones	A	L1	L2-L5
	COM.SC	Se aplican perfiles de seguridad	A	L1	L4-L5
	COM.cont	Aseguramiento de la disponibilidad	M	L1	L2-L4
	COM.cont.1	Se identifican y evitan "puntos únicos de fallo" (SPF-Single Point of Failure)	M	L1	L4
	COM.aut	Autenticación del canal	M	L1	L2-L4
	COM.aut.4	{xor} Mecanismo de autenticación	M	L1	L3-L4
	COM.aut.4.3	2 factores: token + contraseña	M	n.s.	L3-L4
	COM.aut.4.4	2 factores: token + certificados	M	n.s.	L3-L4
	COM.aut.4.5	2 factores: contraseña de un solo uso (OTP) con token	M	n.s.	L3-L4
	COM.aut.4.6	2 factores: contraseña de un solo uso (OTP) por canal separado	M	n.s.	L4

	COM.wifi	Seguridad Wireless (WiFi)	A	L1	L3-L4
	COM.wifi.4	Se eliminan las claves por defecto en tarjetas y puntos de accesos antes de su despliegue	A	L1	L4
	COM.wifi.6	Se deshabilitan los protocolos de gestión no esenciales	A	L1	L4
	COM.DS	Segregación de las redes en dominios	M	L1	L3-L4
	AUX	Elementos Auxiliares	M	L1	L2-L4
	AUX.cont	Aseguramiento de la disponibilidad	M	L1	L3-L4
	AUX.cont.2	Continuidad de operaciones	M	L1	L3-L4
	AUX.AC	Climatización	M	L1	L3-L4
	AUX.wires	Protección del cableado	M	L1	L3-L4
	AUX.7	Se disponen medidas frente a posibles robos	M	L1	L4

	HW_0049	Protección física del equipamiento	M	L1	L4
	L	Protección de las Instalaciones	M	L1	L2-L4
	L.6	Protección frente a desastres	M	L1	L3-L4
	L.6.6	Se ha previsto protección frente a contaminación electromagnética	M	L1	L4
	IR	Gestión de incidentes	M	L1	L2-L4
	IR.3	Contención del incidente	M	L1	L3-L4
	IR.3.3	Se suspenden cautelarmente los trabajos en el sistema afectado	M	L1	L4
	IR.3.4	Se aísla cautelarmente el sistema afectado	M	L1	L4
	tools	Herramientas de seguridad	M	L1	L3-L4
	tools.IDS	IDS/IPS: Herramienta de detección /	M	L1	L3-L4

		prevención de intrusión			
	tools.conf	Herramienta de chequeo de configuración	M	L1	L3-L4
	tools.traffic	Herramienta de monitorización de tráfico	M	L1	L3-L4
	E	Relaciones Externas	M	L1	L2-L4
	E.1	Acuerdos para intercambio de información y software	M	L1	L3-L4

Dominio de seguridad	CÓDIGO	SALVAGUARDA	VALORACIÓN	POTENCIAL	OBJETIVO FINAL
Dominio de seguridad: [2TCP/IP] FASE 2 ENLACES TCP/IP	K	Protección de claves criptográficas	A	L1	L2-L4

	K.comms	Protección de claves de comunicaciones	A	L1	L2-L4
	K.comms.8	{xor} Almacenamiento de las claves	A	L1	L4
	S	Protección de los Servicios	M	L1	L2-L4
	S.1	Prestación de los servicios	M	L1	L2-L4
	S.SC	Se aplican perfiles de seguridad	M	L1	L3-L4
	HW	Protección de los Equipos Informáticos (HW)	A	L2	L2-L4
	HW.SC	Se aplican perfiles de seguridad	A	L2	L3-L4
	HW.cont	Aseguramiento de la disponibilidad	M	L2	L2-L4
	HW.cont.1	Se dimensiona holgadamente y se planifica la adquisición de repuestos	M	L2	L4
	COM	Protección de las Comunicaciones	A	L2	L2-L5
	COM.SC	Se aplican perfiles de seguridad	A	L2	L3-L5

	COM.cont	Aseguramiento de la disponibilidad	M	L2	L2-L4
	COM.cont.1	Se identifican y evitan "puntos únicos de fallo" (SPF-Single Point of Failure)	M	L2	L4
	COM.wifi	Seguridad Wireless (WiFi)	A	L2	L3-L4
	COM.wifi.4	Se eliminan las claves por defecto en tarjetas y puntos de accesos antes de su despliegue	A	L2	L4
	COM.wifi.6	Se deshabilitan los protocolos de gestión no esenciales	A	L2	L4
	COM.DS	Segregación de las redes en dominios	M	L2	L3-L4
	IR	Gestión de incidentes	M	L2	L2-L4
	IR.3	Contención del incidente	M	L2	L3-L4
	IR.3.3	Se suspenden cautelarmente los trabajos en el sistema afectado	M	L2	L4

	IR.3.4	Se aísla cautelarmente el sistema afectado	M	L2	L4
	tools	Herramientas de seguridad	M	L2	L2-L4
	tools.conf	Herramienta de chequeo de configuración	M	L2	L3-L4
	E	Relaciones Externas	M	L2	L2-L4
	E.1	Acuerdos para intercambio de información y software	M	L2	L3-L4

Dominio de seguridad	CÓDIGO	SALVAGUARDA	VALORACIÓN	POTENCIAL	OBJETIVO FINAL
Dominio de seguridad: [3CENTDESPACHO] FASE 3 CENTRO DE DESPACHO	SW	Protección de las Aplicaciones Informáticas (SW)	A	L3	L2-L4
	SW.SC	Se aplican perfiles de seguridad	A	L3	L3-L4
	HW	Protección de los Equipos Informáticos (HW)	A	L3	L2-L4

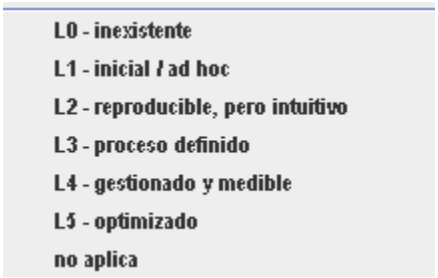
	HW.SC	Se aplican perfiles de seguridad	A	L3	L3-L4
	HW.cont	Aseguramiento de la disponibilidad	M	L3	L2-L4
	HW.cont.1	Se dimensiona holgadamente y se planifica la adquisición de repuestos	M	L3	L4
	COM	Protección de las Comunicaciones	A	L3	L2-L5
	COM.SC	Se aplican perfiles de seguridad	A	L3	L3-L5
	COM.cont	Aseguramiento de la disponibilidad	M	L3	L2-L4
	COM.cont.1	Se identifican y evitan "puntos únicos de fallo" (SPF-Single Point of Failure)	M	L3	L4
	COM.wifi	Seguridad Wireless (WiFi)	A	L3	L3-L4
	COM.wifi.4	Se eliminan las claves por defecto en tarjetas y puntos de accesos antes de su despliegue	A	L3	L4

	COM.wifi.6	Se deshabilitan los protocolos de gestión no esenciales	A	L3	L4
	COM.DS	Segregación de las redes en dominios	M	L3	L3-L4
	AUX	Elementos Auxiliares	M	L3	L2-L4
	AUX.wires	Protección del cableado	M	L3	L3-L4
	HW_0049	Protección física del equipamiento	M	L3	L3-L4
	L	Protección de las Instalaciones	A	L3	L2-L4
	L.6	Protección frente a desastres	A	L3	L3-L4
	L.6.2	Protección frente a incendios	A	L3	L3-L4
	L.6.3	Protección frente a inundaciones	A	L3	L3-L4
	IR	Gestión de incidentes	M	L3	L2-L4
	IR.3	Contención del incidente	M	L3	L3-L4
	IR.3.3	Se suspenden cautelarmente los	M	L3	L4

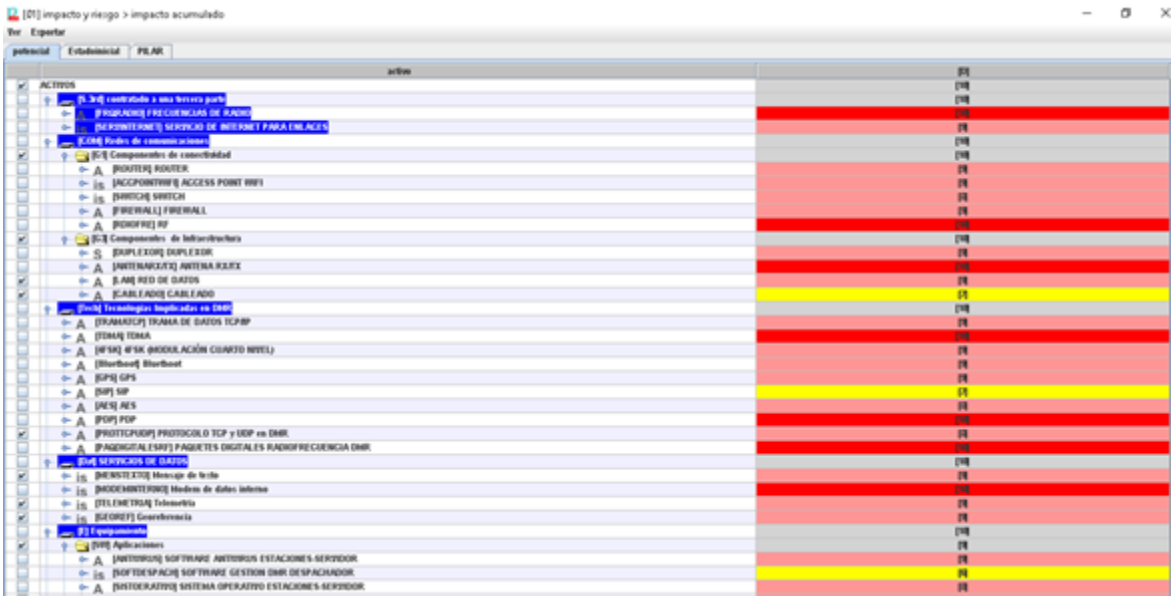
		trabajos en el sistema afectado			
	IR.3.4	Se aísla cautelarmente el sistema afectado	M	L3	L4
	tools	Herramientas de seguridad	M	L3	L2-L4
	tools.IDS	IDS/IPS: Herramienta de detección / prevención de intrusión	M	L3	L3-L4
	tools.conf	Herramienta de chequeo de configuración	M	L3	L3-L4
	tools.traffic	Herramienta de monitorización de tráfico	M	L3	L2-L4
	V	Gestión de vulnerabilidades	M	L3	L2-L4
	tools.V	Herramienta de análisis de vulnerabilidades	M	L3	L3-L4
	E	Relaciones Externas	M	L3	L2-L4
	E.1	Acuerdos para intercambio de	M	L3	L3-L4

		información y software			

AG. Anexo: Nivel de madurez de la salvaguarda en la herramienta PILAR

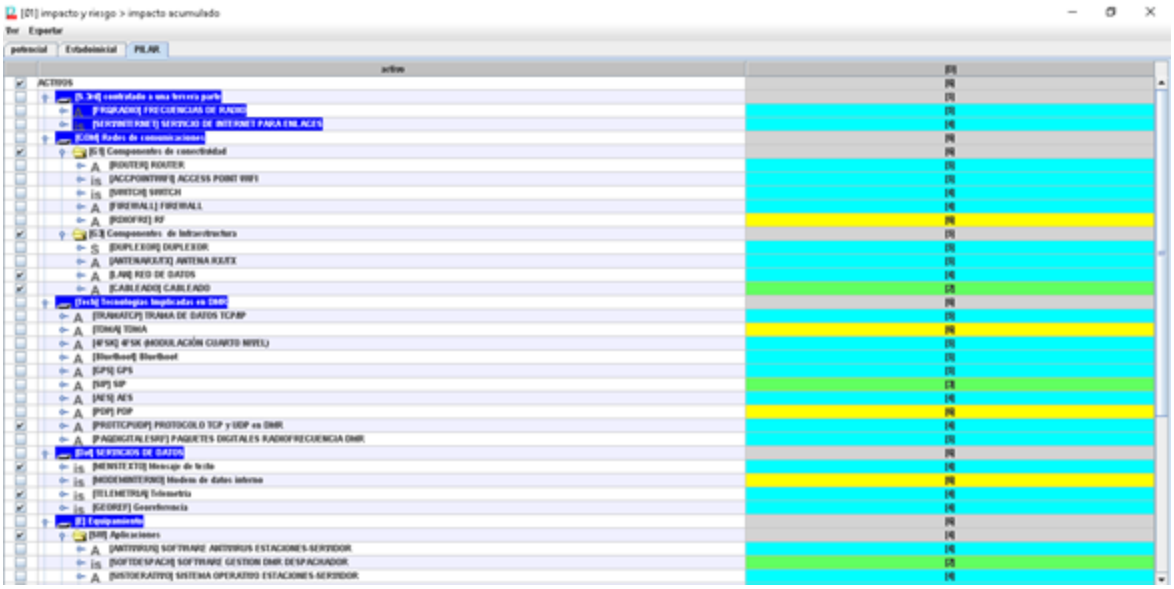


AH. Anexo: Impacto que tienen las amenazas en los activos en la herramienta PILAR

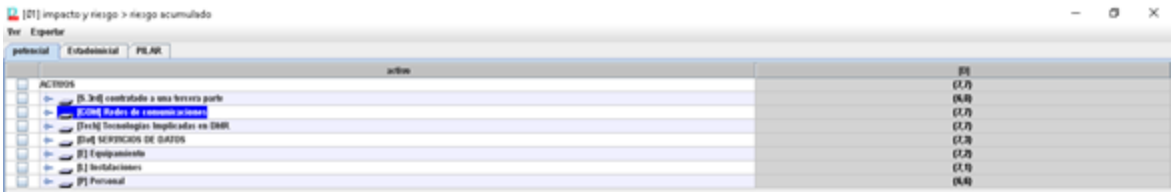


AI. Anexo: Nivel y leyenda de acuerdo con el impacto en la herramienta PILAR

AJ. Anexo: Activos relacionados con las salvaguardas en la herramienta PILAR

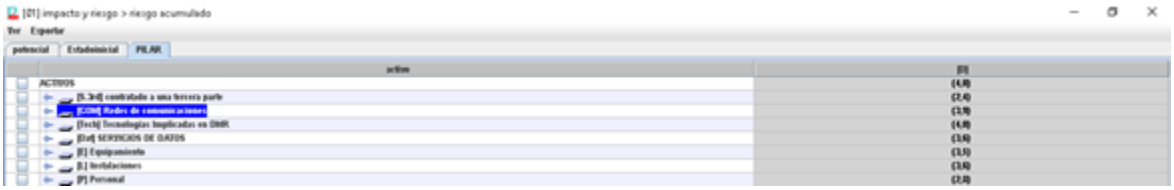


AK. Anexo: Calculo del riesgo de cada capa de activos en la herramienta PILAR

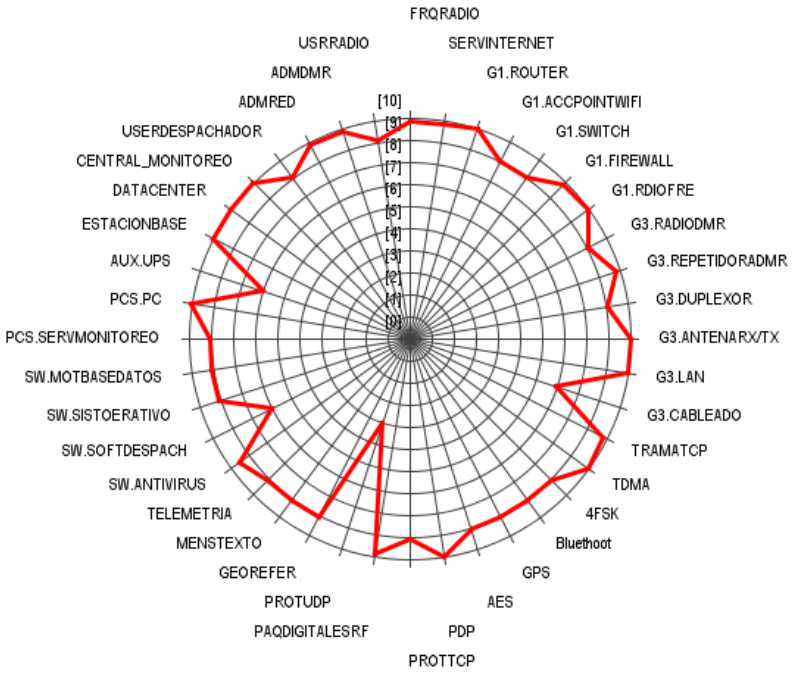


AL. Anexo: Nivel de criticidad en la herramienta PILAR

AM. Anexo: Controles aplicados a cada capa de activos en la herramienta PILAR



AN. Anexo: Impacto acumulado en la herramienta PILAR



AO. Anexo: Impacto potencial

ACTIVO	IMPACTO POTENCIAL
[S.3rd] contratado a una tercera parte	
[FRQRADIO] FRECUENCIAS DE RADIO	MA
[SERVINTERNET] SERVICIO DE INTERNET PARA ENLACES	A
[COM] Redes de comunicaciones	
[G1] Componentes de conectividad	MA
[ROUTER] ROUTER	M
[ACCPOINTWIFI] ACCESS POINT WIFI	M
[SWITCH] SWITCH	M
[FIREWALL] FIREWALL	A
[RDIOFRE] RF	MA
[G3] Componentes de Infraestructura	MA
[RADIODMR] RADIOS DMR	A
[REPETIDORADMR] REPETIDORA DMR	MA
[DUPLEXOR] DUPLEXOR	M
[ANTENARX/TX] ANTENA RX/TX	A
[LAN] RED DE DATOS	A
[CABLEADO] CABLEADO	M
[TechyProt] Tecnologías o protocolos en DMR	
[TRAMATCP] PAQUETE DE DATOS DE RED	MA
[TDMA] TDMA	A
[4FSK] 4FSK (MODULACIÓN CUARTO NIVEL)	A
[Bluethoot] Bluethoot	B
[GPS] GPS	A
[AES] AES	M

[PDP] PDP	MA
[PROTTCP] PROTOCOLO TCP	A
[PAQDIGITALESRF] PAQUETES DIGITALES RADIOFRECUENCIA DMR	MA
[PROTUDP] PROTOCOLO UDP	B
[Dat] SERVICIOS DE DATOS	
[GEOREFER] Georreferencia	A
[MENSTEXTO] Mensaje de texto	A
[TELEMETRIA] Telemetría	A
[E] Equipamiento	
[SW] Aplicaciones	A
[ANTIVIRUS] SOFTWARE ANTIVIRUS ESTACIONES-SERVIDOR	B
[SOFTDESPACH] SOFTWARE GESTION DMR DESPACHADOR	M
[SISTOERATIVO] SISTEMA OPERATIVO ESTACIONES-SERVIDOR	A
[MOTBASEDATOS] MOTOR BASE DE DATOS EVENTOS DE DATOS	A
[PCS] Equipos Finales	A
[SERVMONITOREO] SERVIDOR MONITOREO	A
[PC] ESTACIÓN DE TRABAJO (PC)	A
[AUX] Elementos auxiliares	M
[UPS] UPS	M
[L] Instalaciones	
[ESTACIONBASE] ESTACIÓN BASE	MA
[DATACENTER] DATACENTER	MA
[CENTRAL_MONITOREO] CENTRAL_MONITOREO	MA
[P] Personal	

[USERDESPACHADOR] DESPACHADOR MONITOREO	A
[ADMRED] Administrador de red interna	A
[ADMDMR] Administrador de infraestructura DMR	A
[USRRADIO] USUARIO RADIO	A

AP. Anexo: Riego potencial

Activo	Riesgo potencial
[S.3rd] contratado a una tercera parte	
[FRQRADIO] FRECUENCIAS DE RADIO	A
[SERVINTERNET] SERVICIO DE INTERNET PARA ENLACES	A
[COM] Redes de comunicaciones	
[G1] Componentes de conectividad	MA
[ROUTER] ROUTER	A
[ACCPOINTWIFI] ACCESS POINT WIFI	M
[SWITCH] SWITCH	M
[FIREWALL] FIREWALL	MA
[RDIOFRE] RF	MA
[G3] Componentes de Infraestructura	MA
[RADIODMR] RADIOS DMR	M
[REPETIDORADMR] REPETIDORA DMR	MA
[DUPLEXOR] DUPLEXOR	M
[ANTENARX/TX] ANTENA RX/TX	A
[LAN] RED DE DATOS	MA
[CABLEADO] CABLEADO	M
[TechyProt] Tecnologías o protocolos en DMR	

[TRAMATCP] PAQUETE DE DATOS DE RED	MA
[TDMA] TDMA	MA
[4FSK] 4FSK (MODULACIÓN CUARTO NIVEL)	M
[Bluethoot] Bluethoot	M
[GPS] GPS	A
[AES] AES	M
[PDP] PDP	MA
[PROTTCP] PROTOCOLO TCP	A
[PAQDIGITALESRF] PAQUETES DIGITALES RADIOFRECUENCIA DMR	MA
[PROTUDP] PROTOCOLO UDP	B
[Dat] SERVICIOS DE DATOS	
[GEOREFER] Georreferencia	M
[MENSTEXTO] Mensaje de texto	M
[TELEMETRIA] Telemetría	A
[E] Equipamiento	
[SW] Aplicaciones	M
[ANTIVIRUS] SOFTWARE ANTIVIRUS ESTACIONES-SERVIDOR	M
[SOFTDESPACH] SOFTWARE GESTION DMR DESPACHADOR	M
[SISTOERATIVO] SISTEMA OPERATIVO ESTACIONES-SERVIDOR	M
[MOTBASEDATOS] MOTOR BASE DE DATOS EVENTOS DE DATOS	M
[PCS] Equipos Finales	MA
[SERVMONITOREO] SERVIDOR MONITOREO	M
[PC] ESTACIÓN DE TRABAJO (PC)	MA
[AUX] Elementos auxiliares	M

[UPS] UPS	M
[L] Instalaciones	
[ESTACIONBASE] ESTACIÓN BASE	MA
[DATACENTER] DATACENTER	MA
[CENTRAL_MONITOREO] CENTRAL_MONITOREO	MA
[P] Personal	
[USERDESPACHADOR] DESPACHADOR MONITOREO	M
[ADMRED] Administrador de red interna	MA
[ADMDMR] Administrador de infraestructura DMR	A
[USRRADIO] USUARIO RADIO	M

Bibliografía

Hussain, A., Saqib, N. A., Qamar, U., Zia, M., & Mahmood, H. (2014). Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks. Journal of Communications and Networks, 16(4), 397–406. https://doi.org/10.1109/JCN.2014.000069

Onali, T., Sole, M., & Giusto, D. D. (2011). DMR networks for health emergency management: A case study. 2011 7th International Wireless Communications and Mobile Computing Conference, 2151–2156. https://doi.org/10.1109/IWCMC.2011.5982867

Secure Land Communications. (2018). Visible body: SIRDEE. Spain. Recuperado de https://www.securelandcommunications.com

Tetrapol Forum. (2018). Visible body: Tetrapol. Recuperado de http://www.tetrapol.com/

Deepak, B. R., Bharathi, P. S., & Kumar, D. (2017). Radio frequency anti-jamming capability improvement for cognitive radio networks: An evolutionary game theoretical approach. 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN), 1–6. https://doi.org/10.1109/ICSCN.2017.8085719

Cave, M., Doyle, C., & Webb, W. (2007). Essentials of modern spectrum management. New York: Cambridge; New York: Cambridge University Press.

Gottwalt, F., Chang, E., & Dillon, T. (2019). Analysis of feature selection techniques for correlation-based network anomaly detection doi:10.1007/978-3-319-98776-7_2 Retrieved from www.scopus.com

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 92, 178-188. doi: 10.1016/j.future.2018.09.063

Wankhede, S. B. (2019). Study of network-based DOS attacks doi:10.1007/978-981-13-0776-8_58 Retrieved from www.scopus.com

Kong, S., Application, F., & Data, P. (2011). (12) United States Patent, 2(12), 12–15. https://doi.org/10.1016/j.(73)

Informe técnico sobre los beneficios de DMR 1, 1–14. Retrieved from www.dmrassociation.org

Loukas, G., & Oke, G. (2008). Protection against Denial of Service Attacks: A Survey. The Computer Journal, 0(0), 60–78. https://doi.org/10.1093/comjnl/bxh000

Benet, M. (2014). Vulnerabilidad en sistemas DMR. Retrieved from https://www.securityartwork.es/2014/12/10/vulnerabilidad-en-sistemas-dmr/

Arif, S., Hassan, S., Nisar, K., Habbal, A., Omar, H., & Ismail, M. (2013). A holistic approach in developing an ensemble mobile peer-to-peer computing. Proceedings - 5th International

Conference on Computational Intelligence, Communication Systems, and Networks, CICSyN 2013, 311–315. https://doi.org/10.1109/CICSYN.2013.12

Hlavacek, D., & Chang, J. M. (2014). A layered approach to cognitive radio network security: A survey. Computer Networks, 75(PartA), 414–436. https://doi.org/10.1016/j.comnet.2014.10.001

Lin, S., Chen, C., Wu, E. H., Chan, C., & Jou, E. (2016). A New e-Bus System Using Two-Way Government Radio Networks, (January).

Múnera Salazar, L. E., & Cadavid, A. N. (2010). Agrupamiento mediante Q-análisis. Sistemas & Telemática, 14(37), 45–56. https://doi.org/10.18046/syt.v14i37.2241

Kumarasamy, S., & Shankar, G. A. (2012). An Active Defense Mechanism for TCP SYN flooding attacks. ArXiv.Org, 1–6.

Astorza, V. A. de. (2017). Análisis de la seguridad y proceso de la auditoría de señales. Retrieved from https://riunet.upv.es/handle/10251/86818

Borja, M. F. (2011). Análisis de tráfico con Wireshark, 52.

García, D., & Ruiz, J. (2017). Análisis y Gestión de Riesgos en el Marco del SGSI, Basado en la Metodología MAGERIT y Apoyado en un API Web para su Ejecución. Retrieved from http://repository.udistrital.edu.co/bitstream/11349/6813/1/Documento Proyecto Grado.pdf%0Ahttp://repository.udistrital.edu.co/handle/11349/6813

Association, DMR. (2009). Benefits and features of DMR White Paper, 1–22.

Picod, J., Lebrun, A., & Demay, J. (2014). Bringing Software Defined Radio to the Penetration Testing Community. Black Hat USA, 2014, 1–7. Retrieved from https://www.youtube.com/watch?v=hZJDdz6kVJ4

Britos, A., & Daniel, J. (2010). Captura Distribuida Y Procesamiento Estadístico Índice General.

Trotta, A., Di Felice, M., Bedogni, L., Bononi, L., & Panzieri, F. (2015). Connectivity recovery in post-disaster scenarios through Cognitive Radio swarms. Computer Networks, 91, 68–89. https://doi.org/10.1016/j.comnet.2015.07.017

Kaushik, S. S., & Deshmukh, P. P. R. (2011). Detection of Attacks in an Intrusion Detection System, 2(3), 982–986.

Kouwen, A., Scanlon, M., Raymond Choo, K. K., & Le-Khac, N. A. (2018). Digital forensic investigation of two-way radio communication equipment and services. Digital Investigation, 26, S77–S86. https://doi.org/10.1016/j.diin.2018.04.007

Coy Abondano, J. A., Proyectos, M. en G. de, & jcoyabo@eafit.edu.co. (2016). Diseño de una Oficina de Dirección de Proyectos (PMO) para la empresa SERACIS LTDA., que pertenece al sector de la Vigilancia y Seguridad Privada, 1–35. Retrieved from https://repository.eafit.edu.co/handle/10784/8719#.WimljkqWaUk

López, R. (2017). Escuela Especializada en Ingenería ITCA-FEPADE / REVISTA TECNOLÓGICA N° 10. ENERO -DICIEMBRE 2017 C. Ataques a través de Bases de Datos, 10, 13–19.

Alcaraz, C., Rom, R., & Rubio, J. E. (2017). Estado y Evolución de la Detección de Intrusiones en los Sistemas Industriales, (Jnic), 1–20.

ETSI. (2013). Etsi tr 102 398, 1, 1–70.

Specification, T. (2017). ETSI TS 102 361-3 - Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems; Part 3: DMR data protocol, 5, 1–57.

Martin, L., Christophe, B., Suignard, E., Picault, A., & Edf, R. (n.d.). From Co- Toward Multi-Simulation of Smart Grids based on HLA and FMI Standards : A Telecontrol Case Study Based on Real World, 6(413427), 1–20.

Carter, J., Grommon, E., & Harris, P. (2016). From conceptual to operational: Over-the-air-programming of land mobile radios. Physical Communication, 19, 18–29. https://doi.org/10.1016/j.phycom.2016.01.007

Ramos Varón Antonio Angel. (2015). Hacking práctico de redes wifi y radiofrecuencia. (RA-MA, Ed.). MADRID, ESPAÑA.

Moulad, L., Belhadaoui, H., Rifi, M. (2018). Implementation of an Hierarchical Hybrid Intrusion Detection Mechanism in Wireless Sensor Network Based on Energy Management. (2019) Advances in Intelligent Systems and Computing, 756, Pp. 360-377, 613, 91337. https://doi.org/10.1007/978-3-319-60744-3

Khamphakdee, N., Benjamas, N., & Saiyod, S. (2014). Improving intrusion detection system based on Snort rules for network probe attack detection. 2014 2nd International Conference on Information and Communication Technology, ICoICT 2014, 69–74. https://doi.org/10.1109/ICoICT.2014.6914042

T. H. Ptacek and T. N. Newsham. (1998). Insertion, evasion, and denial of service: Eluding network intrusion detection. Secure Networks, Inc., Suite 330, 1201 5th Street S.W, Calgary, Alberta, Canada.

Gramajo, A. (2005). Introducción a conceptos de IDS y técnicas avanzadas con Snort. Networks.

Burningham, J. S. (2015). Introduction to Digital Mobile Radio (DMR). Qst, 99(10), 30.

Consejo Superior de Administración Electrónica. (2012). MAGERIT - versión 3.0, 42. Retrieved from http://administracionelectronica.gob.es/ctt/resources/Soluciones/184/Area descargas/Libro-III-Guia-de-Tecnicas.pdf?idIniciativa=184&idElemento=87&idioma=en

Amutio, M., Candau Javier, & Mañas José. (2012). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método, 127.

Retrieved from https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Allen, C., Feltheimer, A., & Helliwell, J. (n.d.). MAKING THE RIGHT CHOICE : TO SOLVE CRITICAL MACHINE-TO-MACHINE MAKING THE RIGHT CHOICE

Security Art Work. (2014). Vulnerabilidad en sistemas DMR - Security Art Work. [online] Available at: https://www.securityartwork.es/2014/12/10/vulnerabilidad-en-sistemas-dmr/

Indicador de disponibilidad. (2018). Retrieved from https://www.zabbix.com/

Loukas, G., & Oke, G. (2008). Protection against Denial of Service Attacks: A Survey. The Computer Journal, 0(0), 60–78. https://doi.org/10.1093/comjnl/bxh000

Qaddus, A. (2016). Real Time Performance Analysis of Digital Mobile Radio (DMR) and APCO Project 25 (P-25) Radio Systems in Land Mobile Radio (LMR) Systems, 8(3), 49–55.

Tobergte, D. R., & Curtis, S. (2013). Sistemas de Detección de Intrusos. Journal of Chemical Information and Modeling, 53(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Villal, A. (2002). Sistemas de Detección de Intrusos, 1–22.

Zurutuza, U. (2004). Sistemas de detección de intrusos. Chungar, 36(2), 67. https://doi.org/10.4067/S0717-73562004000200016

Luz, R. R. (2005). Sistemas de radiocomunicaciones. Retrieved from https://books.google.com.co/books?id=uNISCgAAQBAJ

Kaushik, S. & Deshmukh (2011). Detection of Attacks in an Intrusion Detection System, 2(3), 982–986.

Telefónica, F. (2011). Smart Cities: un primer paso hacia la internet de las cosas: Fundación Telefónica. Retrieved from https://books.google.com.co/books?id=wZLmCgAAQBAJ

Byun, S. S. (2016). TCP over scarce transmission opportunity in cognitive radio networks. Computer Networks, 103, 101–114. https://doi.org/10.1016/j.comnet.2016.03.026

GStavroulakis, P. (2007). Terrestrial Trunked Radio - TETRA. Vasa. https://doi.org/10.1177/1363460706060719

Abascal Blanco, Á. J. (2016). Tesis: Plataforma de soporte a toma de decisiones frente a situaciones de emergencias en Smart Cities .

Richard Heady, George Luger, Arthur Maccabe, and M. S. (2011). The architecture of a Network Level Intrusion Detection System. Technical Report CS90–20, University of New Mexico,

Konyavskiy, V., Epishkina, A., & Korotin, A. (2016). The Design of Integrity Monitoring and Reliability Verification System for Critical Information, Transmitted in Automatic Train

Signaling System, Based on DMR-RUS Radio Channel. Procedia Computer Science, 88, 318–323. https://doi.org/10.1016/j.procs.2016.07.442

Autor, L. A. N., Rodriguez, Y., Tutores, W., & Artiles, M. C. (2012). Universidad Central “ Marta Abreu ” de Las Villas Facultad de Matemática , Física y Computación.

Fernández Castaño, F., & Santiago Segura, M. J. (2011). Universidad de Granada. Actas del congreso Internacional sobre Migraciones en Andalucía.

Sistemas, C. I. D. E. (2014). UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO.

Bennett, D. M. (2014). Vulnerabilidad en sistemas DMR. British Journal of Psychiatry, 205(01), 76–77. https://doi.org/10.1192/bjp.205.1.76a

Blaze (2010). Why(SpecialAgent) Johnny(Still) Can’tEncrypt: ASecurity Analysisofthe APCOProject25Two-WayRadioSystem. Folia Endocrinol.Jap., 51(8), 661–675.

Belaustegui, A. (2007). VTIID Área de Informática indicador de disponibilidad. Cadiz.

NTC ISO 31000. (2011). NORMA TÉCNICA NTC-ISO COLOMBIANA 31000 GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES E: RISK MANAGEMENT. PRINCIPLES AND GUIDELINES CORRESPONDENCIA: esta norma es una adopción idéntica (IDT) por traducción de la norma, (571). Retrieved from https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

TAIT. (2015). DMR INTRODUCTION.

Ashdail Raindondi Perez. (2013). ESTUDIO DE IMPLEMENTACIÓN DE SISTEMAS DE 410 MHZ Y 430 MHZ.

Dorosz, P. K. P. (2003). Intrusion Detection Systems (IDS) Part I - (network intrusions; attack symptoms; IDS tasks; and IDS architecture). Retrieved from http://techgenix.com/intrusion_detection_systems_ids_part_i__network_intrusions_attack_symptoms_ids_tasks_and_ids_architecture/

Edward G. Amoroso. (1999). Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, and Response , 1st Edition, Intrusion.Net Books.

Cadena Muñoz, E., Eslava Blanco, H. J., & Franco Calderón, J. A. (2015). Gestión del espectro radioeléctrico en Colombia. Revista Tecnura, 19(45), 159. https://doi.org/10.14483/udistrital.jour.tecnura.2015.3.a12

Baldini G. (JRC-IPSC). (2010). Report of the workshop on " Interoperable communications for Safety and Security " Workshop jointly organized by. https://doi.org/10.2788/19075

Stahlberg, M. (2000). Radio jamming attacks against two popular mobile networks. Helsinki University of Technology Seminar on Network Security, 1–20. https://doi.org/10.1007/s12630-010-9354-9

Verisign. (2015). Verisign Distributed Denial of Service Trends Report, 4(1), 1–8. Retrieved from https://www.verisign.com/assets/report-ddos-trends-Q32015.pdf

Utilities Telecom Council. (2015). ANNUAL REVIEW the Wind is at our backs

Superintendencia de vigilancia. (2009). Super Vigilancia limitará uso de equipos de interceptación por parte de empresas de Seguridad Privada. Retrieved from https://www.supervigilancia.gov.co/publicaciones/1711/supervigilancia--limitara--uso-de-equipos-de-interceptacion--por-parte--de-empresas-de-seguridad-privada/

José María López Piñero. (1992). Los indicadores bibliométricos y la evaluación de la actividad médico-científica: la aplicación de los indicadores.

Javier Culebra Hernández. (2017). CURSO DE FORMACIÓN DMR.

Maria, Tsirka.(2016). IDS PORTAL. Retrieved from http://idsportal.cs.teiath.gr/index.php/en/

Centro Criptológico Nacional. (2018). Software EAR / PILAR Risk analysis and management tools. Retrieved from https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar/pilar.html

TS, E. (octubre de 2017). www.dmrassociation.org. Obtenido de https://www.dmrassociation.org/

Digital, I. C. (2014). www.inetec.net. Obtenido de inetec.net: http://www.inetec.net/productos/hytera-dmr/hytera-serie-pd6/

Castro, J. (24 de noviembre de 2014). *larepublica.net*. Obtenido de larepublica.net: https://www.larepublica.net/noticia/que_es_el_espectro_radioelectrico

Z. Shu, Y. Qian and S. Ci, "On physical layer security for cognitive radio networks," in IEEE Network, vol. 27, no. 3, pp. 28-33, May-June 2013. doi:10.1109/MNET.2013.6523805

A. G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 428-445, First Quarter 2013.