SEGURIDAD DE LA INFORMACIÓN EN UNA RED DE SENSORES PARA RADIOLOCALIZACIÓN EN APLICACIONES DE VIGILANCIA DEL ESPECTRO ELECTROMAGNÉTICO

Vladimir Francesco Pérez Quintero

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLIN

2019

SEGURIDAD DE LA INFORMACIÓN EN UNA RED DE SENSORES PARA RADIOLOCALIZACIÓN EN APLICACIONES DE VIGILANCIA DEL ESPECTRO ELECTROMAGNÉTICO

Vladimir Francesco Pérez Quintero

Trabajo de grado para optar al título de Maestría en Tecnologías de la Información y la Comunicación

Director

Álvaro Enrique Ospina Sanjuan

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLIN

2019

DECLARACIÓN ORIGINALIDAD

"Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad". Art. 82 Régimen Discente de Formación Avanzada, Universidad Pontificia Bolivariana.

FIRMA AUTOR (ES) _____

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

Amenaza Externa: Amenaza que se origina fuera de una organización.

Amenaza Interna: Amenaza que se origina en una organización.

Análisis de Riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo NTC-ISO /IEC 27001.

Antispam: Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

Antivirus: Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Aplicaciones engañosas: Las aplicaciones engañosas son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.

Banda de frecuencias asignada: Banda de frecuencias en el interior de la cual se autoriza la emisión de una estación determinada; la anchura de esta banda es igual a la anchura de banda necesaria más el doble del valor absoluto de la tolerancia de frecuencia. Cuando se trata de estaciones espaciales, la banda de frecuencias asignada incluye el doble del desplazamiento máximo debido al efecto

Doppler que puede ocurrir con relación a un punto cualquiera de la superficie de la Tierra.

Bandas de frecuencias: Agrupamiento o conjuntos de ondas radioeléctricas con límite superior e inferior definidos explícitamente. Para los propósitos del Cuadro Nacional se definen ocho grandes bandas, a saber: VLF, LF, MF, HF, VHF, UHF, SHF y EHF. Estas a su vez están subdividas cada una de ellas en otras más pequeñas llamadas sub-bandas.

Caballo de Troya: Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de Troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

Canal radioeléctrico: Par de frecuencias radioeléctricas discretas, una para transmisión y otra para recepción, o de una frecuencia para transmisión y recepción, según el modo de operación.

Certificado: Los sistemas criptográficos utilizan este archivo como prueba de identidad. Contiene el nombre del usuario y la clave pública.

Confidencialidad: Propiedad de la información que determina que esté disponible a personas autorizadas.

Disponibilidad: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

Contraseña: Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña.

Emisión: Producción de una señal en una puerta de entrada de una línea de transmisión o en un punto de un medio de transmisión.

Espectro Electromagnético: Es el conjunto de todas las frecuencias de emisión de los cuerpos de la naturaleza. Comprende un amplio rango que va desde ondas cortas, ondas medias o intermedias y ondas largas.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Exploits o Programas intrusos: Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

Firewall: Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Firma digital o electrónica: Es el valor numérico que se adhiere a un mensaje de datos y que utiliza un procedimiento matemático conocido vinculado a la clave del iniciador y al texto del mensaje para determinar que este valor se haya obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no haya sido modificado después de efectuada la transformación.

Frecuencia asignada: Centro de la banda de frecuencias asignada a una estación.

Gusanos: Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, a diferencia de un Virus.

Hackear: Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar.

Información: Inteligencia o conocimiento capaz de ser representado en formas adecuadas para comunicación, almacenamiento o procesamiento.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos.

Interferencia: Es la interconexión que permite a cualquiera de los operadores interconectados, cursar el tráfico de otros operadores a la red del operador interconectante, siempre que no se contravenga el reglamento para cada servicio. El solo servicio portador entre dos redes no se considera interconexión indirecta.

Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para

Nodo: Es el elemento de red, ya sea de acceso o de conmutación, que permite recibir y reenrutar las comunicaciones.

Ondas radioeléctricas u ondas hertzianas: Ondas electromagnéticas, cuya frecuencia se fija convencionalmente por debajo de 3000 GHz, que se propagan por el espacio sin guía artificial.

Penetración: Indicador del cubrimiento de un servicio de telecomunicaciones respecto de la población.

Phishing: Método más utilizado por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Riesgo: El riesgo es el efecto de la incertidumbre sobre los objetivos.

Rootkits: Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final.

Señal: Fenómeno físico, una o más de cuyas características varían para representar información.

Sistema de detección de intrusos: Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Sistema de prevención de intrusos: Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing.

Spyware o Software Espía: El software espía consta de un paquete de software que realiza un seguimiento y envía información confidencial o personal a terceros. La información personal es información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de las personas no desearía compartir con otras, como detalles bancarios, números de tarjetas de créditos y contraseñas. Terceros puede hacer referencia a sistemas remotos o partes con acceso local.

Tecnologías de la Información (TI): Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.

Telecomunicación: Se entiende por telecomunicaciones toda transmisión, emisión o recepción de signos, señales, escritos y sonidos, datos o información de cualquier naturaleza, por hilo, radio, medios visuales u otros sistemas electromagnéticos.

UIT: Unión Internacional de Telecomunicaciones.

Usuario: Persona o máquina delegada por un cliente para utilizar los servicios y/o facilidades de una red de telecomunicaciones. En el contexto de los servicios de telecomunicación: un ser humano que utiliza un servicio. En un contexto técnico: un ser humano, una entidad o un proceso.

Virus: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario.

Vulnerabilidad: Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.

Xtell: Es un sistema de mensajería cliente - servidor, permite enviar mensajes desde un cliente usando el comando xtell a un servidor corriendo el servidor xtelld. Puede ser usado en remplazo de otros comandos comunes como write.

RESUMEN

El proyecto de Colciencias “Desarrollo de Capacidades Tecnológicas en Comprobación Técnica del Espectro” se enfoca en la tarea de Identificación de Transmisores, concepto establecido en la recomendación de la UIT ITU-R SM.1600 (Sm & Spectrum, 2012). Una vez se ha sensado el espectro y se han radiolocalizado los transmisores de interés, debe identificarse plenamente a los transmisores pudiendo determinar si son legales o ilegales. Esta etapa es crucial para poder efectivamente imponer sanciones y demostrar la autoría de una transmisión ilegal. Adicionalmente cobra cada vez mayor importancia y complejidad teniendo en cuenta que hay un gran número de dispositivos que pueden ser usados sin licencias o certificaciones lo cual dificulta su identificación, que las bandas son compartidas por múltiples tecnologías y que las quejas de interferencia son difíciles de resolver para el ente regulador (Sm & Spectrum, 2012) .

Este trabajo de grado dispone puntualmente analizar diversos esquemas de seguridad que permitan garantizar que la información procedente de diferentes sensores o nodos observadores, cumplen con requisitos de seguridad mínimos que garanticen al centro de fusión que va a procesar información real y fidedigna. El proyecto de investigación se encuentra enmarcado dentro del proyecto “Desarrollo de Capacidades Tecnológicas en Comprobación Técnica del Espectro”, aprobado por Colciencias en la convocatoria 652 y desarrollado al interior del grupo de investigación GIDATI.

Para este trabajo de grado, se partirá de una arquitectura de red previamente MTIC.UPB-FPDG_1 6 de 33 definida conformada por una red de sensores o nodos observadores con capacidades heterogéneas (unos pueden medir tiempos de llegada en las señales recibidas, otros pueden medir ángulos de llegada, otros pueden medir ambos parámetros), y un centro de fusión encargado de mezclar toda la información recibida por parte de los sensores y procesarla adecuadamente con el fin único de identificar posibles transmisiones ilegales. Con la arquitectura previamente definida en el marco del proyecto, así como los nodos y el centro de fusión, dentro de las actividades nos concentramos puntualmente en determinar las características de transmisión que deben tener las señales transmitidas por los nodos observadores al centro de fusión con el fin de que la información llegue fielmente.

INTRODUCCIÓN

Mediante el presente trabajo se propone un grupo de métodos para minimizar el impacto de las vulnerabilidades de seguridad para los nodos sensores del prototipo del sistema de sensado de espectro en el proyecto “Desarrollo de Capacidades Tecnológicas en Comprobación técnica del espectro”, apoyándose en la búsqueda bibliográfica del estado del arte donde condensaremos las mejores prácticas para el sistema de nodo de sensores, definiendo, aplicando y dejando documentado esta investigación.

CAPITULO 1

Búsqueda bibliográfica de ataques y defensas en redes de sensores

Los radios definidos por software SDR han tenido una evolución acelerada llegando a convertirse en una herramienta invaluable para la educación e investigación en el sector de las telecomunicaciones, ya que nos da la capacidad de desarrollar rápidamente los prototipos y algoritmos necesarios para la investigación. En su interior podemos encontrar los componentes de arquitectura necesarios para realizar los algoritmos así como los sensores necesarios para obtener las capturas de información de la radiofrecuencia, incorporando conversores análogo-digital ADC, conversores digital-análogo, FPGA, hardware para radio y una modularidad de programación de paquetes, apoyada por una comunidad de conocimiento como GNU Radio[1]. Esta evolución en los dispositivos SDR, ha significado de facto posicionarse como el dispositivo seleccionado por las universidades y compañías para realizar la gran mayoría de investigaciones, gracias al soporte de una amplia gama de actividades relacionadas con las telecomunicaciones, dentro las diferentes familias de dispositivos que soportan estas capacidades encontramos los USRP ETTUS N200/N210, ZedBoard w, NooElec NESDR y la familia de los ETTUS USRP E300.

Las características diferenciadoras de los dispositivos SDR[2] son:

- Hardware asequible con el suficiente poder de cómputo para operar a través de un amplio rango de portadoras de frecuencia y anchos de banda, incluyendo dentro de su diseño, la portabilidad del dispositivo.

- Disponibilidad de ambientes de desarrollo de software que proveen tecnologías de comunicación para el control de la plataforma SDR, enriquecidos por los conjuntos de módulos, algoritmos, características y facilidades para tomar rápidamente la curva de aprendizaje sobre las tecnologías.

- Soporte entre el hardware SDR y software especializado de computación, dando la capacidad de desarrollar modelos basados en software y experimentados en el mundo real en tiempo real.

- Capacidad de interacción de estudiantes con las últimas tecnologías de telecomunicaciones como lo podemos ver en las redes de última generación G5[3].

Dentro de las familias de SDR podemos ver las siguientes características de hardware en los SDR:

	Ettus USRP N200/N210	ZedBoard w/ Xilinx Zynq-7000 FPGA & AD-FMCOMMS5-EBZ	NooElec NESDR Mini SDR USB Stick	Ettus USRP E300
Interface to host Computer	Gigabit Ethernet	Dual FMC Connectors	USB 2.0	AXI4-MM interface to an embedded dual-core ARM Cortex-A9 processor
RF front-end Instantaneous bandwidth RF frequency coverage	USRP daughterboards 25–50 MHz DC to 6 GHz (determined by daughterboard)	Integrated RFIC 56 MHz 70 MHz to 6 GHz	Integrated RFIC 3.2 MHz 24 to 1766 MHz	Integrated RFIC 56 MHz 70 MHz to 6 GHz
MIMO	1 × 1 per unit, up to 8 × 8 using multiple units	4 × 4	N/A	2 × 2
Full duplex	Yes	Yes	Rx only	Yes
ADC	Dual 14-bit 100 MS/s	Dual/quad 12-bit 61.44 MS/s	8-bit 3.2 MS/s	Dual/quad 12-bit 61.44 MS/s
DAC	Dual 16-bit 400 MS/s	Dual/quad 12-bit 61.44 MS/s	None	Dual/quad 12-bit 61.44 MS/s
FPGA RFNoC-compatible Cost	Xilinx Spartan 3A DSP No $$	Xilinx Zynq-7000 No $$$	None No $	Xilinx Zynq-7000 Yes $$$$

Fig. 1 Características del hardware SDR

El campo de las telecomunicaciones por radio están regidas por entes territoriales para la administración del espectro electromagnético, algunas de estas agencias administradoras son la Agencia Nacional del Espectro (ANE) en Colombia o la Federal Communication Comission (FCC) en Estados Unidos, entre otras; estas agencias se encargan de repartir el espectro electromagnético mediante licencias otorgadas para su funcionamiento, en las cuales implementan restricciones de uso de tecnología para los servicios a ser proveídos, estas restricciones hacen que muchos de los desarrollos que se quieran realizar sean movidos a bandas de frecuencia para la que no se necesitan licenciamiento, aunque en muchas ocasiones, estos desarrollo toman prestado frecuencias ociosas en el espectro licenciado generando interferencias sobre las bandas licenciadas. Hay tecnologías como la Cognitive Radio[4] que se encarga de evitar interferencias en las bandas licenciadas y de hacer un uso más eficiente del espectro electromagnético, pero en todas las situaciones donde se haga uso de bandas sin el respectivo

licenciamiento, las entidades reguladoras están en la obligación de entrar a controlar la situación del espectro radioeléctrico [ERE], esta es una tarea compleja y de gran responsabilidad que involucra no solamente la asignación de frecuencias y la coordinación de estas asignaciones con los países vecinos, sino que trae nuevos retos derivados de los nuevos usos del espectro y las nuevas tecnologías; el uso del espectro en el largo plazo; la promoción de las actividades de investigación en tecnologías de radio; el monitoreo permanente de los diferentes servicios; y la adaptación de los parámetros de radio propagación a las condiciones locales.

La gestión de ERE involucra, como una de sus partes, los sistemas de monitoreo de espectro, que buscan detectar posibles violaciones de la regulación existente, así como otras tareas propias de la gestión, como limpieza (frequency Clearance), ubicación de emisiones no permitidas, entre otras. Igualmente, los operadores móviles utilizan sistemas similares en sus operaciones de ajuste y despliegue de nuevos sitios para garantizar que estén libres de interferencias.

Las capacidades que brindan los SDR descritos en la figura 1 *Características del hardware SDR* facilitan la gestión del ERE, ya que introducen la capacidad de movilidad de las antenas. En américa latina es ampliamente utilizada la suite TESMonitor, esta suite tiene muchas características pero dentro de sus desventajas encontramos una baja resolución del mecanismo de Radio-Determinación (Direction Finding), que se basa en servomotor con antena directiva y no es utilizable en unidades móviles, lo que le resta competitividad a la herramienta y abre el campo de investigación para las necesidades regionales incorporando ciertas tareas del monitoreo del ERE que difieren considerablemente de las de otros países, lo que hace que surjan necesidades específicas que no suelen ser de norma en los sistemas internacionales.

Este es el campo que se encarga el proyecto global de seguridad que brinda el proyecto apoyado por el GIDATI, el cual busca brindar *disponibilidad* e *integridad* a las comunicaciones en el espectro electromagnético, pero de las mismas capacidades de transmisión y recepción de los SDR lo convierten automáticamente en una amenaza frente a atacantes externos que quieran *capturar el sistema*, afectando directamente la disponibilidad e integridad y añadiendo la amenaza de confidencialidad en caso de que el sistema sea comprometido y usado para otros fines. A fin de tener un producto competitivo, se deben resolver las siguientes amenazas y vulnerabilidades[5] para los sistemas de monitoreo del ERE apoyados en los SDR:

- Adversial atack: El objetivo del ataque es generar un modelo de ataque el cual ha sido cuidadosamente diseñado para encontrar las entradas que hacen que la máquina o su operación falle.

- Selfish attack: El objetivo del atacante es conseguir más espectro electromagnético para el mismo, evitando que los otros compitan por el uso de los canales, ocupando los canales por los que ellos han dejado de competir.

- Malicius attack: El objetivo es crear interferencias para los otros competidores, esto no significa necesariamente que el atacante obtenga beneficios del ataque, se trata de simplemente generar pérdidas para los demás.

Los ataques generados al sistema de gestión del ERE pueden ser *directos*, donde el objetivo es denegar el servicio o generar repudio en las comunicaciones o *indirectos* mediante violaciones de políticas o rompimiento de regulaciones, estas últimas con consecuencias legales por el incumplimiento de acuerdos. Estos ataques se orientan en vulnerar la información circulante en los sistemas, ya sea afectando la confidencialidad, la integridad o la disponibilidad.

Como parte del desarrollo de estrategias de defensa, en 1995 la British Standar[6], pública la norma BS 7799-1:1995 para ayudar a las empresas a administrar la seguridad de la información. Esta norma tenía una estructuración sencilla y no permitía forma de certificación de cumplimiento, ni establecía como conseguirla. A partir de esta norma se han realizado las siguientes actualizaciones:

- En 1999 se publica la revisión de la norma BS 7799-2:1999 incorporando los requisitos para implantar un sistema de gestión de la seguridad.

- En el 2000 la Internacional Estándar ISO publica la ISO/IEC 17799:2000, básicamente una transcripción del estándar británico.

- En el 2002 la British Standar publica la BS 7799-2:2002, la cual permitió la certificación de empresas mediante una entidad certificadora en el Reino Unido y otros países.

- En el 2005 se publica la ISO/IEC 27001:2005 apareciendo la ISO 27001 como estándar internacional la cual es certificable y se revisa la ISO 17799 dando lugar a la creación de la norma ISO/IEC 27001:2005.

- En 2007 se renombra la ISO 17799, pasando a ser la ISO 27002:2005.

- En 2007 se realiza una revisión, publicando la ISO/IEC 27001:2007.

- En 2009 se publica un documento de modificaciones llamado ISO 27001:2007/1M:2009.

- En 2013 se publica la versión actual ISO/IEC 27001:2013.

El proyecto “Desarrollo de Capacidades Tecnológicas en Comprobación Técnica del Espectro” , aprobado por Colciencias en la convocatoria 652 y desarrollado al interior del grupo de investigación GIDATI no es ajeno a las vulnerabilidades presentes en todo sistema de información, por lo tanto, se incorpora un análisis de riesgos tecnológicos apoyados en un marco de evaluación de la familia ISO-NTC 27000, usando para la norma ISO-NTC 27005, las cuales incluyen actividades expuestas en la figura 2 [7]:

Fig. 2 Proceso de evaluación de riesgo

Esta evaluación de riesgos se apoya en un análisis de vulnerabilidades, ejecutando la herramienta de análisis de vulnerabilidades *Nessus, seleccionada entre varias opciones disponibles*. Esta herramienta evalúa lo dispositivos y clasifica las vulnerabilidades encontradas según una lista llamada “vulnerabilidades conocidas y exposiciones” o por su término en inglés “*Common Vulnerabilities and Exposures” CVE*, la cual es mantenida por *The Mitre Corporation*, una organización financiada por los *Estados Unidos de Norteamérica* a través de la *División Nacional para la Cyberseguridad*. Esta lista es actualizada constante mente con las nuevas vulnerabilidades descubiertas y sirve como referencia para entender y comprender la forma de abordar la vulnerabilidad detectada.

El ejercicio de evaluación de riesgos define los planes de acción para los controles asociados a los dispositivos que participan en el sistema, previniendo el compromiso (hackeo) del mismo, brindando la confidencialidad, integridad y disponibilidad necesaria para su correcto funcionamiento, evitando que se puedan llevar a cabo Adversial, Selfish, Malicius Atacks desde el sistema.

1.1 Planteamiento del problema

1.1.1 Problema

La vigilancia del espectro electromagnético implica realizar tareas de identificación de transmisores para la imposición de las correspondientes sanciones. A pesar de que desde las tecnologías de comunicaciones inalámbricas existen variadas técnicas para implementar las tareas de vigilancia del espectro así como de identificación de transmisores, todas ellas pueden fallar si la información que los nodos sensores envían al centro de fusión es alterada o sustituida. Esto implica que es necesario implementar técnicas de seguridad de la información en los nodos sensores.

1.1.2 Justificación

La gestión del espectro es una labor de gran importancia y responsabilidad que comprende la asignación y coordinación de frecuencias con países vecinos, la asignación de frecuencias a nuevos servicios y usuarios del espectro, el análisis prospectivo del uso del espectro electromagnético, el monitoreo de los servicios que hacen uso del espectro, la detección de posibles violaciones y la ubicación de emisiones no permitidas.

Esta labor ha sido implementada de diversas formas a través del tiempo, existen algunas técnicas de comunicaciones inalámbricas clásicas y otras más novedosas que permiten hacerlo con mayor o menor precisión. Sin embargo, en los países de América Latina y otros países en vías de Desarrollo existen ciertas particularidades que hacen que la implementación difiera notablemente de otros países del mundo, y que por lo tanto, los métodos mundialmente estandarizados no puedan ser utilizados de forma directa. Dentro de esas particularidades se encuentran sus terrenos y climas, sus características económicas que hacen que no sea viable para el ente regulador adquirir equipos exageradamente costosos como los usados por países desarrollados.

Ante esta necesidad la ITU en sus recomendaciones ITU K. 83 y ITU.K 91 (esta última aún no publicada) establece la posibilidad de implementar equipos de gestión del espectro de menor costo y precisión, con adaptaciones técnicas a las condiciones y necesidades particulares de los países en vías de desarrollo.

Es así como dentro del programa de sensado de espectro ("Desarrollo de Capacidades Tecnológicas en Comprobación Técnica del Espectro," n.d.), se pretende generar un prototipo de un sistema con capacidades de sensado del espectro y radiolocalización de fuentes transmisoras. Este prototipo debe contar con características de seguridad en las transmisiones que se realicen entre los nodos observadores y el centro de fusión. En la actualidad hay amplias investigaciones sobre implementación de esquemas de seguridad de la información para tecnologías de sensores similares a la deseada, como RFID o NFC. Estos trabajos sirven como base para el aprendizaje e identificación de los esquemas que se requieren implementar sobre la red de sensores de particular interés dentro del programa de investigación de Colciencias en el cual nos enmarcamos.

En el mundo se cuenta con otros equipos de muy alta precisión utilizados en países desarrollados, que cuentan con todos los requerimientos técnicos y de precisión requeridos por la ITU, así mismo con sus propias características de seguridad. Sin embargo, estos son equipos muy costosos, que como se mencionó antes, no aplican para su directa utilización en algunos países en vías de desarrollo. Adicionalmente, debido a que se trata de tecnología de punta, los fabricantes de estos equipos utilizan esquemas propietarios que no liberan al público y por tanto no es fácil determinar los esquemas de seguridad que ellos implementan. Es necesario entonces, hacer un análisis para el prototipo particular de interés que se está desarrollando al interior del proyecto de esta investigación "Seguridad de la Información en una red de sensores para radiolocalización en aplicaciones de vigilancia del espectro electromagnético".

1.2 Objetivos

Proponer un grupo de métodos para minimizar el impacto de las vulnerabilidades de seguridad para los nodos sensores del prototipo del sistema de sensado de espectro en el proyecto "Desarrollo de Capacidades Tecnológicas en Comprobación técnica del espectro", con el fin de garantizar al centro de fusión el procesamiento de señales fidedignas para sus labores de Identificación de Transmisores.

1.2.1 Objetivo específico 1

Definir las vulnerabilidades de mayor impacto a la que está expuesta la información enviada por los nodos sensores en un prototipo de un sistema de gestión de espectro, con base en estudios previos realizados sobre estándares en tecnologías similares (como RFID).

1.2.2 Objetivo específico 2

Implementar las técnicas de seguridad de la información que protejan ante las vulnerabilidades del sistema en los escenarios previamente seleccionados.

1.2.3 Objetivo específico 3

Realizar un informe final que exponga el plan de seguridad para asegurar el nodo de sensores del sistema de sensado del espectro. Desarrollo bibliográfico de la metodología de evaluación de riesgo

1.3 Desarrollo bibliográfico de la metodología de evaluación de riesgo

La metodología descrita en la norma ISO-NTC/IEC 27005[8], se ocupa de la gestión de riesgos para apoyar las necesidades del sistema de gestión de seguridad de la información descritos en la ISO-NTC/IEC 27001 y describen un método iterativo en busca de la mejora continua, para el desarrollo del análisis de riesgos se hacen las siguientes definiciones.

1.3.1 Amenaza

Es la causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

1.3.2 Vulnerabilidad

Es la debilidad de un activo o control que puede ser explotada por una o más amenazas.

1.3.3 Riesgo

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

1.3.4 Activo de información

Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, discos duros, bases de datos, etc.) que tenga valor para la organización.

1.3.5 Impacto

El costo para la empresa de un incidente, que puede o no ser medido en términos financieros.

1.3.6 Probabilidad

Es la medida cuantitativa por medio de la cual podemos obtener la frecuencia de ocurrencia de un evento, para pronosticar en un momento dado puede ocurrir.

1.3.7 Confidencialidad

Es una propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado a dicha información.

1.3.8 Disponibilidad

Propiedad de la información de estar accesible en el momento que es requerida por una entidad autorizada.

1.3.9 Integridad

Propiedad de la información de estar libre de alteraciones o modificaciones no autorizadas.

1.3.10 Incidente

Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

1.3.11 Evento

Suceso que ocurre de acuerdo a una condición o serie de condiciones dadas.

1.3.12 Riesgo residual

Es el riesgo que remanente luego del tratamiento del riesgo.

1.3.13 Aceptación del riesgo

Decisión informada de asumir un riesgo concreto.

1.3.14 Evasión del riesgo

Es la decisión de eliminar completamente la fuente del riesgo.

1.3.15 Transferencia de riesgo

Es la decisión de ceder el riesgo a un proveedor que esté en capacidad de gestionarlo.

1.3.16 Actividades del análisis de riesgos

En la tabla 1 definimos las actividades del análisis de riesgos.

Nº	Actividad	Normas y/o controles
01	Identificación de activos	Se debe realizar un inventario de los activos de información, los cuales serán incluidos dentro del alcance de la evaluación del riesgo.
02	Valoración de activos	Los activos deben ser clasificados de acuerdo a su importancia en la cadena de valor de la organización, teniendo en cuenta: El valor real del activo y el impacto categorizado.
03	Identificación de las amenazas	Para cada activo listado en el inventario se deben identificar las posibles amenazas que puedan afectar la integridad, disponibilidad o confidencialidad de la información. Para identificar las amenazas se debe de tener en cuenta si existe alguna vulnerabilidad la cual pueda ser aprovechada por dicha amenaza, de no ser así, la amenaza será despreciable y no se tendrá en cuenta.
04	Evaluación de la probabilidad de amenaza	De acuerdo a diferentes factores como la revisión de incidentes, estadísticas de amenazas, experticia de los usuarios y los propietarios de los activos, se debe valorar la probabilidad de ocurrencia de las amenazas identificadas.

05	Identificación de los controles existentes	Se requiere identificar todos los controles implementados (Existentes y planificados), y evaluar la efectividad de los mismos. **Nota**: No todos los controles establecidos son de carácter técnico; algunos son de índole operativa o registro físico.
06	Identificación de las consecuencias	Se deben definir las consecuencias que generaría para la organización la perdida de confidencialidad, integridad y disponibilidad de la información para cada uno de los activos.
07	Valoración del impacto.	El impacto es el resultado del análisis y valoración de las consecuencias, el cual se expresará en términos cuantitativos y cualitativos.
08	Estimación de niveles de riesgo	Se deben estimar los niveles de riesgo teniendo en cuenta la probabilidad de ocurrencia de un escenario (vulnerabilidad – amenaza – impacto) para los activos de la organización. Riesgo= Amenaza X Impacto

Tabla 1 Actividades del análisis de riesgos

1.3.17 Gestión del riesgo

En la tabla 2, definimos las actividades para realizar la gestión del riesgo.

Nº	**Actividad**	**Normas y/o controles**
01	Nivel de Riesgo aceptable	Se debe definir el nivel de riesgo que la Organización está dispuesta a asumir y declarar éste como riesgo aceptable.
02	Definir tratamiento	Se debe seleccionar el tratamiento que se dará al riesgo que no sea aceptable. Se deben implementar controles que permitan evitar, Reducir o Transferir el riesgo.

		Evitar: Se hace uso de controles los cuales reduzcan la probabilidad de ocurrencia de la amenaza que genera el riesgo. Reducir: Se hace uso de controles los cuales disminuyan el impacto que generaría el riesgo en caso de materializarse. Transferir: Se hace uso de controles que traspasen el riesgo a una tercera parte, de este modo reducir la responsabilidad sobre dicho riesgo.
03	Plan de tratamiento	Se debe llevar a cabo un plan de tratamiento de riesgos definiendo los controles y actividades a realizar, responsables, recursos necesarios, registros de control y cambios que ocurran en las actividades.

Tabla 2 Gestión del riesgo

1.3.18 Estimación del nivel de riesgo

Se debe de estimar el nivel del riesgo, haciendo uso de la estimación de la probabilidad de amenaza y la estimación del impacto, Estas definiciones las podremos encontrar a continuación.

1.3.18.1 Asignación de valores método cuantitativo

1.3.18.1.1 Probabilidad

En la tabla 3 definimos la probabilidad de ocurrencia de los eventos de riesgo.

Frecuencia	Rango	Valor	Cálculo
Muy Alta	1 vez al día	100%	5
Alta	1 vez a la semana	75%	4
Media	1 vez cada mes	50%	3
Baja	1 vez cada 6 meses	25%	2
Muy Baja	1 vez cada año	5%	1

Tabla 3 Probabilidad de ocurrencia

1.3.18.1.2 Impacto

En la tabla 4 definimos los criterios de evaluación del impacto.

VALOR	CRITERIO	DESCRIPCIÓN
5	Muy Alto	La divulgación no autorizada de la información que contiene o gestiona el activo impacta fuertemente la operación y la imagen o la estabilidad de la organización
4	Alto	La divulgación no autorizada de la información que contiene o gestiona este activo impacta negativamente la operación.
3	Medio	La divulgación no autorizada de la información que contiene o gestiona este activo impacta negativamente la operación parcialmente.
2	Bajo	La divulgación no autorizada de la información que contiene o gestiona este activo impacta negativamente algún proceso o actividad de la operación.
1	Muy bajo	La divulgación no autorizada de la información que contiene o gestiona este activo no impacta negativamente la operación.

Tabla 4 Confidencialidad

1.3.18.1.3 Disponibilidad

En la tabla 5 definimos los criterios de evaluación de disponibilidad.

VALOR	CRITERIO	DESCRIPCIÓN
5	Muy Alto	Si el activo no se encuentra disponible afecta la totalidad de la operación y la imagen o la estabilidad de la organización
4	Alto	Si el activo no se encuentra disponible afecta la totalidad de la operación.
3	Medio	Si el activo no se encuentra disponible afecta en un 50% la totalidad de la operación.
2	Bajo	Si el activo no se encuentra disponible afecta en un 25% la totalidad de la operación.
1	Muy bajo	Si el activo no se encuentra disponible afecta mínimamente la totalidad de la operación.

Tabla 5 Disponibilidad

1.3.18.1.4 Integridad

En la tabla 6 definimos los criterios de evaluación de integridad

VALOR	CRITERIO	DESCRIPCIÓN
5	Muy Alto	Si se altera la información que maneja este activo impacta negativamente la operación y daña la imagen de la organización

4	Alto	Si se altera la información que maneja este activo impacta negativamente la operación.
3	Medio	Si se altera la información que maneja este activo impacta negativamente la operación parcialmente.
2	Bajo	Si se altera la información que maneja este activo impacta negativamente algún proceso o actividad de la operación.
1	Muy bajo	Si se altera la información que maneja este activo no impacta negativamente la operación.

Tabla 6 Integridad

1.3.18.1.5 Estimación niveles de riesgo

En la tabla 7 definimos la matriz de riesgos usada para la evaluación.

Probabilidad					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	Impacto				

Tabla 7 Matriz de nivel de riesgo

1.3.18.2 Niveles de riesgo

En la tabla 8 definimos los criterios de clasificación del riesgo.

CRITICO (No aceptable)	Implementación de plan de mejora y seguimiento. Se deben implementar nuevos controles de prevención; para reducir la probabilidad de ocurrencia; de protección, para disminuir el impacto que genera, o traspasar dicho riesgo por medio de pólizas, por medios propios, tercerización u otras opciones disponibles.
ALTO (No Aceptable)	Implementación de plan de mejora y seguimiento. Se debe tomar medidas para bajar la severidad del riesgo; si es posible, fortalecer y mejorar controles existentes o implementar nuevos controles.
MEDIO (Aceptable)	Se pueden tomar medidas para bajar la severidad; si es posible, se deben conservar y mejorar controles.
BAJO (Aceptable)	La entidad puede asumir el riesgo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

Tabla 8 Apetito de riesgo

1.3.18.3 Lineamientos para el tratamiento del riesgo

En la tabla 9 definimos los criterios para el tratamiento del riesgo.

Severidad	Consideración	Medidas de respuesta
Crítico	El riesgo es inaceptable	Se deben implementar nuevos controles de prevención; para reducir la probabilidad de ocurrencia, para disminuir el impacto que genera, o traspasar dicho riesgo por medio de pólizas, tercerización u otras opciones disponibles.
Alto	El riesgo es importante	Se debe tomar medidas para bajar la severidad del riesgo; si es posible, fortalecer y mejorar controles

		existentes o implementar nuevos controles.
Medio	El riesgo es tolerable	Se pueden tomar medidas para bajar la severidad; si es posible, se deben conservar y mejorar controles.
Bajo	El riesgo es aceptable	La entidad puede asumir el riesgo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

Tabla 9 Lineamientos para el tratamiento del riesgo

1.3.19 Gestión del riesgo

Las actividades de gestión de riesgo se activan cuando:

a) Por periodo definido de revisión de los riesgos

b) Por cualquier cambio que afecte a la gestión de la seguridad como cambios en la organización, alcance del sistema de gestión de seguridad, los activos incluidos, la tecnología, procesos, objetivos del negocio, amenazas, eficacia de controles, eventos externos como requisitos legales, reglamentarios, contractual, entre otros.

c) Del resultado de la revisión técnica, (mínimo una vez cada año), escaneo de vulnerabilidades de red, equipos y aplicaciones de la compañía.

1.3.19.1 Identificación de riesgos

Es requerido ejecutar la identificación de riesgos dadas las siguientes situaciones:

a) Revisión periódica de los riesgos identificados.

b) Cambios en la organización, por ejemplo, cambio de sede, cambio de centro almacenamiento de información sensible, cambio centro alterno de datos, cambios en la tecnología, cambios en la reglamentación o requisitos contractuales, cambios en la operación, cambios en la tecnología, cambios proveedores, cambios en usuarios de terceras partes, entre otros.

c) Cambios en los activos críticos de la organización

d) Gestión de la capacidad

e) Eventos en el monitoreo de las operaciones

f) Eventos identificados que afecten la continuidad del negocio

g) Revisión riesgo aceptable y residual

1.3.19.2 Tratamiento de los riesgos

Dentro del tratamiento del riesgo tenemos las siguientes alternativas para los riesgos no aceptado y aceptados.

1.3.19.2.1 Riesgos no Aceptados

Emplear una o varias de estas alternativas:

1. Aplicar los controles apropiados, esto implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección).

2. Evitar el riesgo, tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, buen diseño, planificación previa o eliminación (Diseñar procesos de negocio con enfoque al riesgo).

3. Transferir a otras partes los riesgos asociados con el negocio. (Reducir su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Es así como por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

Se debe de generar un plan para el tratamiento del riesgo, la persona responsable de hacer seguimiento al plan trazado. El Resumen de tratamiento de riesgos debe ser revisado de forma periódica. Si el tratamiento de riesgo no supera las expectativas de nivel de riesgo aceptable, se debe definir un nuevo plan de tratamiento, y así sucesivamente hasta lograr un nivel aceptado de riesgo.

1.3.19.2.2 Riesgos Aceptados

Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de aceptación de riesgos. Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el responsable acepta la pérdida residual probable, elaborando planes de contingencia para su manejo.

CAPITULO 2

Implementar las técnicas de seguridad de la información que protejan ante las vulnerabilidades del sistema

En este capítulo desarrollaremos la ejecución del análisis de riesgo definido en la búsqueda bibliográfica realizada, incorporando las variables, parámetros y dos escenarios, así como su metodología para la evaluación de la medición de los riesgos expuestos, recolectando los resultados.

1.4 Caracterización del sistema

1.4.1 Escenario Inicial

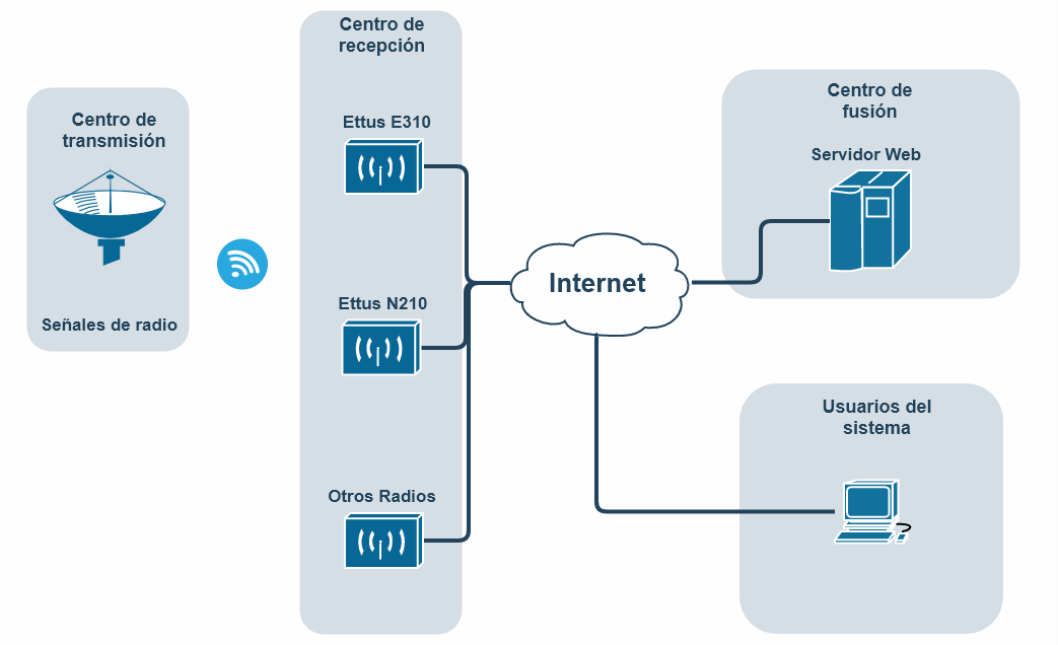

Fig. 3 Escenario inicial

1.4.2 Antenas receptoras

1.4.2.1 Radio Ettus E310

El Ettus E310 es un dispositivo portable que ofrece una plataforma de radio definido por software diseñado para el trabajo en campo. Tiene unas antenas transceiver flexibles 2x2 MIMO AD9361 desde un dispositivo analógico que provee hasta 56 Mhz de ancho de banda instantáneo, con periodos desde 70 MHZ hasta 6 Ghz para cubrir múltiples bandas de interés. Los bancos de filtros RF aumenta la selectividad tanto en la transmisión como en la recepción.

El procesador de banda base usa el Xilinx Zynq 7020 SoC para entregar al FPGA una computación acelerada combinada con la capacidad de operación autónoma que es habilitada por el procesador ARM dual-core, figura 4. El USRP E310 incluye un rico juego de periféricos, un receptor GPS integrado para el conocimiento de la ubicación y la sincronización del tiempo, como también dos puertos USB para expandir el almacenamiento I/O y las comunicaciones externas del dispositivo. Los usuarios pueden rápidamente crear prototipos, desplegando diseños móviles con aplicaciones embebidas en un tamaño, peso y consumo reducidos.

La serie USRP Embebida usa un framework abierto para crear distribuciones de Linux personalizadas para las necesidades específicas de la aplicación. El sistema operativo está preinstalado con el software API UHD con una variedad de herramientas de terceros como GNU radio. Incorpora soporte para el framework RFNoC FPGA, este habilita la computación determinística para el procesamiento en tiempo real y procesamiento de las señales de ancho de banda, su diseño físico lo podemos ver en la figura 5 y figura 6.

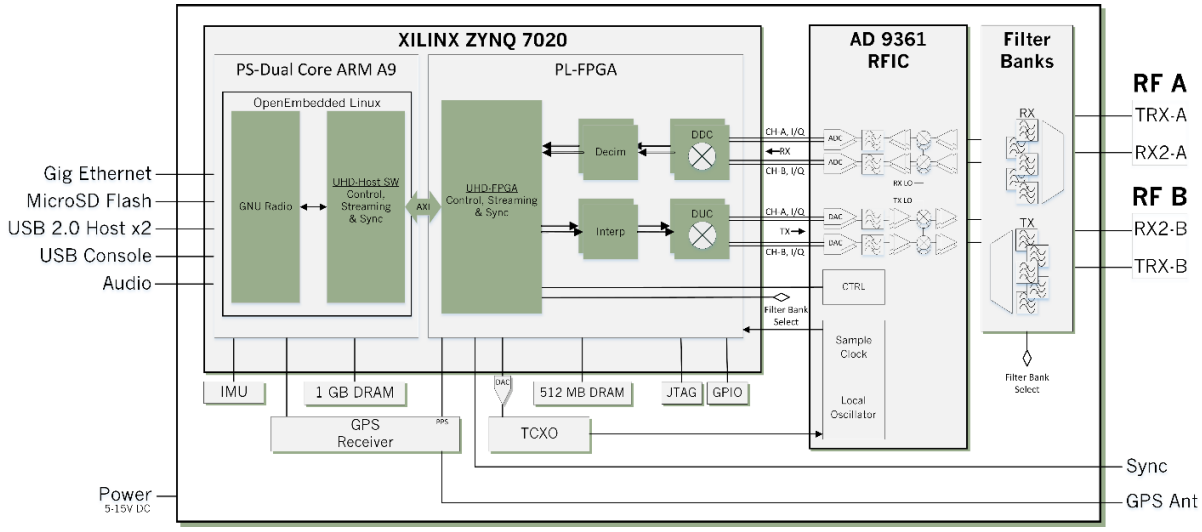

Fig. 4 Diagrama lógico Ettus 310

Fig. 5 Ettus 310 vista frontal

Fig. 6 Ettus 310 Vista trasera

1.4.2.2 Radio Ettus N210

El USRP N210 provee un alto procesamiento de ancho de banda y rango dinámico. Está dirigido para aplicaciones de comunicaciones demandantes de rápido desarrollo. La arquitectura del producto incluye un Xilinx Spartan 3ª-DSP 3400 FPGA, 100 MS/s con doble ADC y un puerto Gigabit Ethernet para transmitir información desde y hacia los equipos de procesamiento, figura 7. El diseño modular permite al USRP N210 operar desde los 6 Ghz, mientras que el puerto de expansión permite al N210 sincronizarse y ser utilizado en una configuración MIMO. Un módulo opcional GPSDO puede ser añadido para sincronizar los relojes con un 0.001 ppm del estándar GPS mundial. El dispositivo puede transmitir hasta 50 MS/s hacia los equipos de aplicación. Los usuarios pueden implementar funciones personalizadas en el FPGA con al procesador de 32 bits RISC incluido en la board. El FPGA ofrece el potencial de procesar 100 MS/s en ambas direcciones y su firmware puede ser recargado por medio de la tarjeta de red, su forma física la podemos en la figura 8.

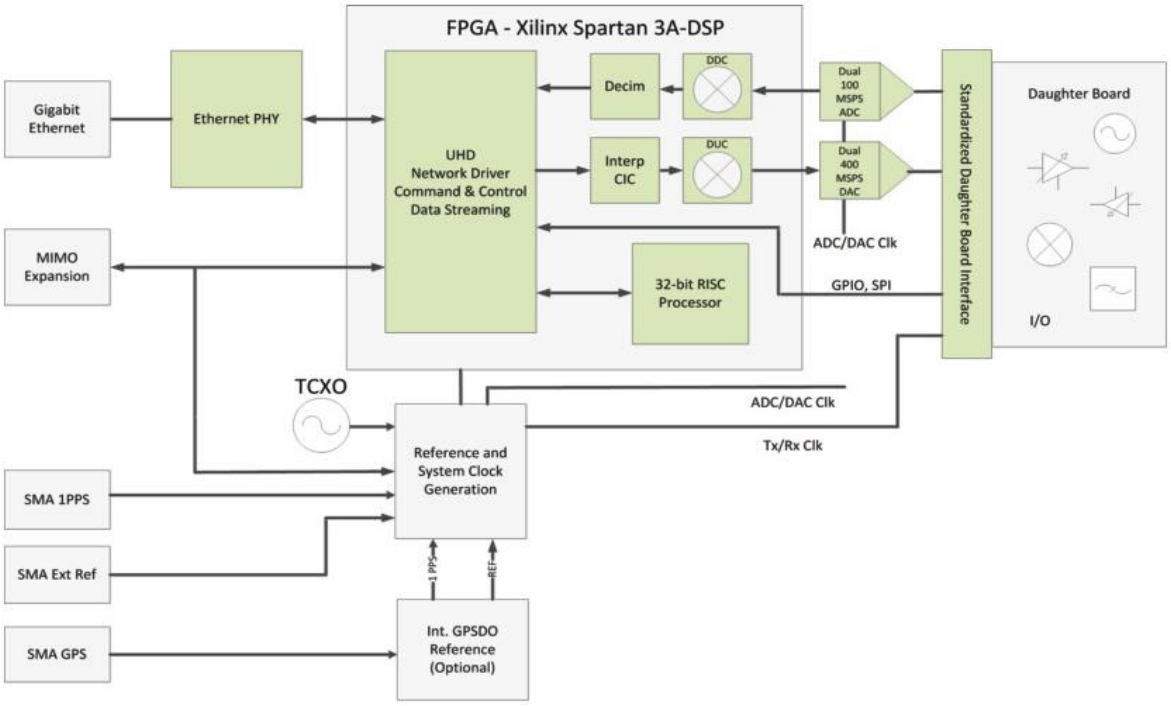

Fig. 7 Diagrama lógico Ettus N210

Fig. 8 Vista frontal Ettus N210

1.4.2.3 Otros Radios

Estos dispositivos son de apoyo para la triangulación de la señal, pueden ser USRP Ettus N210 o E310 descritos anteriormente.

1.4.3 Servidor WEB

Los servidores web son los encargados de entregar herramientas en línea para apoyar la lógica de negocio de la red de sensores en el proyecto TES-RDFS,

recolectando la información suministrada por las antenas receptoras y procesándolas para obtener la información.

1.4.4 Internet

Internet es una red global de computadores y otros dispositivos, los cuales proveen información y comunicación con cualquier otro dispositivo que tenga acceso a la red de internet.

1.4.5 Estación de trabajo

Es cualquier dispositivo que se pueda conectar al servicio web mediante internet, estos pueden ser computadores de sobremesa, portátiles, tablets, entre otros.

1.4.6 Usuario

Es la persona a la cual se le ha concedido derecho de ingreso al aplicativo de monitoreo de radiofrecuencia.

1.4.7 Señales de radio

Es el uso de un espectro entre 3Khz y 300 Ghz para el envío de comunicaciones haciendo uso de ondas electromagnéticas.

1.4.8 Centro de recepción

Es el recinto destinado para la recepción de señales de radio, este recinto puede ser móvil o estacionario.

1.4.9 Centro de fusión

Es el recinto destinado para el funcionamiento de los servidores del aplicativo TES-RDFS, contiene todas las características necesarias para los servicios de soporte de la infraestructura, como energía continua, sistemas de refrigeración, protección de los medios.

1.4.10 Centro de usuarios

Es el recinto destinado para la conexión de las estaciones de trabajo, gracias a el acceso por internet puede ser cualquier locación.

1.4.11 Centro de transmisión

Es el recinto donde se genera la transmisión de radiofrecuencia.

1.5 Evaluación de riesgo

La evaluación de riesgo se ha desarrollado en el documento anexo “Informe de riesgos” teniendo en cuenta el escenario inicial descrito anteriormente. A continuación, se describe los aspectos importantes del informe de riesgos.

1.5.1 Identificación de amenaza

Las amenazas a evaluar están definidas en la norma *NTC-ISO 27035*[9] acorde con las recomendaciones *NTC-ISO 27005*[8]. Existe una relación directa entre amenaza y vulnerabilidad, en el sentido de que si una amenaza no existe la vulnerabilidad tampoco. Estas amenazas están descritas en la tabla 10 Modelado de amenazas.

Tipo	Amenaza
Desastre Natural	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Fenómenos meteorológicos
	Inundación
Disturbios sociales	Paro laboral de los trabajadores de terceros
	Criminal de la computación
	Espionaje industrial
	Terrorismo
	Conmoción nacional
	Conmoción internacional
Daño Físico	Fuego
	Daño por agua
	Contaminación
	Accidente importante
	Destrucción del equipo o los medios
	Polvo, corrosión, congelamiento
Fallas de infraestructura	Falla en el sistema de suministro de agua o de aire acondicionado
	Pérdida de suministro de energía
	Falla en el equipo de telecomunicaciones
Perturbación por radiaciones	Radiación electromagnética
	Radiación térmica

	Impulsos electromagnéticos
Falla técnica	Falla del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Malware	Instalación de virus
	Instalación de backdoor
	Instalación de Rootkits
	Instalación de troyanos
	Instalación de keyloggers
	Instalación de Driver-by downloads
	Instalación de Adware
	Botnets
	Instalación de Roge software
	Instalación de Randsonwere
	Instalación de spyware
Ataque técnico	Fuerza bruta
	Spoofing
	Local file inclusión LFI
	Remote file inclusión RFI
	Cross site request forgery CSRF
	Ghost domain name
	Denegación de servicio DoS y DDoS
	Web defacement
	Inyección Sql Sqli, XMLi,JSONi
	Cross site scripting XSS
	Explotación de vulnerabilidad conocida
Violación de reglas	Uso no autorizado del equipo
	Copia fraudulenta del software
	Uso de software falso o copiado
	Corrupción de los datos
Compromiso de las funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal
Exposición de información	Interceptación de señales de interferencia comprometedoras

	Espionaje remoto
	Escucha subrepticia
	Hurto de medios o documentos
	Hurto de equipo
	Recuperación de medios reciclados o desechados
	Divulgación
	Datos provenientes de fuentes no confiables
	Manipulación con hardware
	Manipulación con software
	Detección de la posición
Contenido peligroso	Phishing
	Spam
	Ingeniería social
	Scam
	Porno
Otras amenazas	Amenazas no clasificadas en las anteriores categorías

Tabla 10 Modelado de amenazas

1.5.2 Valoración de activos

Se tiene unificado la valoración de los activos de información con la valoración que se hace en la evaluación de riesgos en cuanto a la confidencialidad, integridad y disponibilidad, para el costo de económico del activo de información se desarrolla una escala de costos como valor cuantitativo, finalmente para el valor cualitativo se desarrolla una escala desde la percepción del valor del activo de información como podemos ver en las tablas 11, 12,y 13 para la confidencialidad, disponibilidad e integridad respectivamente, así como el valor cualitativo y cuantitativo, tablas 14 y 15, estos son:

VALOR	CRITERIO	DESCRIPCIÓN
5	Muy Alto	La divulgación no autorizada de la información que contiene o gestiona el activo impacta fuertemente la operación y la imagen o la estabilidad de la organización
4	Alto	La divulgación no autorizada de la información que contiene o gestiona este activo impacta totalmente la operación del ítem
3	Medio	La divulgación no autorizada de la información que contiene o gestiona este activo impacta negativamente parcialmente la

		operación
2	Bajo	La divulgación no autorizada de la información que contiene o gestiona este activo impacta negativamente algún proceso o actividad de la operación.
1	Muy Bajo	La divulgación no autorizada de la información que contiene o gestiona este activo no impacta negativamente la operación.

Tabla 11 Valoración de confidencialidad

VALOR	CRITERIO	DESCRIPCIÓN
5	Muy Alto	Si el activo no se encuentra disponible afecta la totalidad de la operación y la imagen o la estabilidad de la organización
4	Alto	Si el activo no se encuentra disponible afecta la totalidad de la operación del ítem
3	Medio	Si el activo no se encuentra disponible afecta en un 50% la totalidad de la operación.
2	Bajo	Si el activo no se encuentra disponible afecta en un 25% la totalidad de la operación.
1	Muy bajo	Si el activo no se encuentra disponible afecta mínimamente la operación.

Tabla 12 Valoración de la disponibilidad

VALOR	CRITERIO	DESCRIPCIÓN
5	Muy Alto	Si se altera la información que maneja este activo impacta negativamente la operación y daña la imagen de la organización
4	Alto	Si se altera la información que maneja este activo impacta totalmente la operación ítem
0	Medio	Si se altera la información que maneja este activo impacta negativamente la operación parcialmente.
2	Bajo	Si se altera la información que maneja este activo impacta negativamente algún proceso o actividad de la operación.
1	Muy bajo	Si se altera la información que maneja este activo no impacta negativamente la operación.

Tabla 13 Valoración de la integridad

VALOR	DESCRIPCIÓN
1	0 a 1.000.000
2	1.000.001 a 5.000.000
3	5.00.001 a 10.000.000
4	10.000.001 a 20,000,000
5	20,000,001 o MAS

Tabla 14 Valoración cuantitativo

ESCALA	VALOR
Muy Bajo: MB	1
Bajo:B	2
Medio:M	3
Alto:A	4
Muy Alto: MA	5

Tabla 15 Valoración cualitativa

El ejercicio completo de valoración la encontramos en el ***análisis de riesgos (anexo) pág. 3*** en el apartado de valoración de activos, figura 9, incluyendo 13 activos de información.

Informe de valoración de activos Matrixtech

Seguridad de la información

En el siguiente informe se presenta la valoración de los activos de información de la organización de una escala 1 a 4. De igual manera se evalua el activo en cuanto a la confidencialidad, la integridad y la disponibilidad, representando este análisis el valor que tiene el activo para la organización.

Escala	Valor	Descripción
Muy Bajo: MB	1	0 a 1.000.000
Bajo:B	2	1.000.001 a 20.000.000
Medio:M	3	20.00.001 a 50.000.000
Alto:A	4	50.000.001 0 mas

Id	Activo	Descripción	Tipo	Confi	Inte	Disp	Valor Ccial	Valor Cuantitativo	Valor Cualitativo	Propietario	Responsable	Ubicación
1	Antenas transmisoras TX	Hardware	Enclousure	1	1	1	1	1	MB	GIDATI	GIDATI	Medellin
2	Radio Ettus E310	Hardware	Enclousure	4	3	3	3	3,2	M	GIDATI	GIDATI	Medellin
3	Radio Ettus N210	Hardware	Enclousure	4	3	3	3	3,2	M	GIDATI	GIDATI	Medellin
4	Otros Radios	Hardware	Enclousure	4	3	3	3	3,2	M	GIDATI	GIDATI	Medellin

Fig. 9 Informe de valoración de activos

1.5.3 Identificación de vulnerabilidades

En la valoración de activos hemos identificado los componentes principales que queremos proteger como podemos ver en la figura 3, estos son los radios *Ettus e310* y *Ettus N210*, así como el *Servidor web* del *centro de fusión*. Las evaluaciones de los radios se exponen en el presente trabajo y el análisis del

servidor web *será llevado a cabo en otra investigación* que está desarrollando el GIDATI.

Para los activos de información de los radios definidos por software, se revisó el hardware, el software, los datos y la infraestructura física que contiene los dispositivos. En la identificación de vulnerabilidades de software se hizo uso de herramientas de análisis de vulnerabilidades; para realizar el análisis del hardware se hizo observaciones directas sobre el sistema y para las instalaciones físicas se ha entrevistado a los interesados.

Este análisis define el riesgo inherente del sistema de vigilancia del espectro electromagnético, es el riesgo intrínseco del sistema sin tener en cuenta los controles que operen sobre él y no pueden ser eliminados, como ejemplo de riesgo inherente podemos tomar un sistema es susceptible de infectarse con virus, aunque se puede mitigar, el sistema sigue siendo susceptible de una afectación por software malicioso debido a la naturaleza del sistema informático y su riesgo inherente. Este análisis lo encontramos en el ***informe de riesgo inherente,*** figura 10, donde se evalúa 190 vulnerabilidades contra 13 activos de información.

Análisis de riesgo inherente

Seguridad de la información

Id Hallazgo	Tipo Dispositivo	Amenaza	Vulnerabilidad	Prob	Confi	Integ	Disp	Riesgo	Tratamiento
1	Hardware	Desastre Natural	Los equipos pueden ser afectados por inun	1	1	3	3	2	Aceptable

Id Act	Activo	Descripción	Tipo Activo	Ubicación	Impacto Cuant	Impacto Cualitativo
3	Radio Ettus N210	Hardware	Enclousure	Medellin	3	Bajo
2	Radio Ettus E310	Hardware	Enclousure	Medellin	3	Bajo
4	Otros Radios	Hardware	Enclousure	Medellin	3	Bajo

Id Hallazgo	Tipo Dispositivo	Amenaza	Vulnerabilidad	Prob	Confi	Integ	Disp	Riesgo	Tratamiento
2	Terceros	Disturbios sociales	El equipo puede ser comprometido por esp	5	5	5	5	25	No Aceptable

Id Act	Activo	Descripción	Tipo Activo	Ubicación	Impacto Cuant	Impacto Cualitativo
3	Radio Ettus N210	Hardware	Enclousure	Medellin	3	Bajo
4	Otros Radios	Hardware	Enclousure	Medellin	3	Bajo

Fig. 10 Análisis de riesgo inherente

1.5.4 Análisis del control

Para el riesgo inherente, se realizó una evaluación de los posibles controles que nos permitan mitigar las vulnerabilidades y reevaluando el riesgo para identificar como queda el riesgo después de aplicar controles, figura 11, a esta evaluación se le conoce como riesgo residual, el cual debe quedar dentro de nuestro apetito de riesgo, definido en el punto 5.4.2 y descrito en el punto 5.4.1.5 del presente documento. El análisis del control lo encontramos en los *Planes de acción en gestión de riesgo tecnológico y riesgo residual,* proponiendo 160 controles.

Planes de acción en gestión de riesgo tecnológico y riesgo residual
Seguridad de la información

Universidad Pontificia Bolivariana 80 años

Id Hallazgo 1	Tipo Hardware				Amenazas	Desastre Natural							
Id Control 1					Vulnerabilidades	Los equipos pueden ser afectados por inundaciones							
Responsable GIDATI					Situación Actual	Los equipos de radio definido por software SDR no son resistentes al agua							
					Acción	Ubicarlos sobre piso falso, fuera del alcance de tuberias hidricas							
Act Id	Activo	Prob	Confi	Integ	Dispo	Fecha	Estado	Imp Cuantivo	Riesgo	Riesgo residual	Imp Cualitativo	Riesgo Inherente	Tratamiento Residual
3	Radio Ettus N210	1	1	1	3	16/11/2017	Implementado	3	2	2	Medio	Aceptable	Aceptable
4	Otros Radios	1	1	1	3	16/11/2017	Implementado	3	2	2	Medio	Aceptable	Aceptable
2	Radio Ettus E310	1	1	1	3	16/11/2017	Implementado	3	2	2	Medio	Aceptable	Aceptable
Id Hallazgo 2	Tipo Terceros				Amenazas	Disturbios sociales							
Id Control 2					Vulnerabilidades	El equipo puede ser comprometido por espionaje industrial							
Responsable GIDATI					Situación Actual	El equipo puede ser accedido para obtener sus secretos							
					Acción	Cifrar el contenido de la instalación de SO							
Act Id	Activo	Prob	Confi	Integ	Dispo	Fecha	Estado	Imp Cuantivo	Riesgo	Riesgo residual	Imp Cualitativo	Riesgo Inherente	Tratamiento Residual
2	Radio Ettus E310	1	5	5	5	17/11/2017	No Implementado	3	25	5	Medio	No Aceptable	Aceptable
3	Radio Ettus N210	1	5	5	5	17/11/2017	No Implementado	3	25	5	Medio	No Aceptable	Aceptable
4	Otros Radios	1	5	5	5	17/11/2017	No Implementado	3	25	5	Medio	No Aceptable	Aceptable

Fig. 11 Planes de acción en gestión de riesgo tecnológico y residual[1]

1.5.5 Determinación de la probabilidad

Para la estimación de la probabilidad nos basamos en el conocimiento previo o juicio de experto, valorando cuantitativamente la probabilidad conforme la tabla 16.

Probabilidad de Ocurrencia

Frecuencia	Rango	Valor	Calculo
Muy Alta	1 vez al día	100%	5
Alta	1 vez a la semana	75%	4
Media	1 vez cada mes	50%	3
Baja	1 vez cada 6 meses	25%	2
Muy Baja	1 vez cada año	5%	1

Tabla 16 Probabilidad de ocurrencia

Esta tabla fue usada en la probabilidad del riesgo inherente y el plan de acción para evaluar el riesgo residual.

[1] La información presentada se encuentra descrita en ***análisis de riesgos (anexo)***

1.5.6 Análisis de impacto

El impacto se ha definido como el promedio de la confidencialidad, la integridad y la disponibilidad y su valor comercial:

Impacto = prom(prom(C + I + D), valor cuantitativo)

El impacto es usado en la evaluación de riesgos priorizando los planes de acción para mitigar los riesgos en el plan de acción, esta fórmula ha sido incorporada en la consulta que se hace a la base de datos de riesgos como podemos ver en la figura 12.

```
Controles.Disponibilidad,
Controles.Fecha,
Controles.Estado,
round(([Valoracion activos].confidencialidad+[Valoracion activos].integridad+[Valoracion activos].disponibilidad)/3) AS ImpCuantivo,
round(([Hallazgos].Confidencialidad+[Hallazgos].Integridad+[Hallazgos].Disponibilidad)/3)*[Hallazgos].[Probabilidad de Ocurrencia],0) AS Riesgo
round(((Controles.Confidencialidad+Controles.Integridad+Controles.Disponibilidad)/3)*Controles.[Probabilidad],0) AS [Riesgo residual],
IIf(ImpCuantivo>3,"Alto",IIf(ImpCuantivo>2,"Medio",IIf(ImpCuantivo>1,"Bajo","Muy Bajo"))) AS ImpCualitativo, IIf([Riesgo]>8,"No Aceptabl
```

Fig. 12 Fórmula de impacto

1.5.7 Determinación del riesgo

La *Determinación del riesgo* se realiza teniendo en cuenta la probabilidad de amenaza y el promedio del riesgo en sus componentes de confidencialidad, integridad y disponibilidad. Este cálculo se hace en antes y después de los controles para determinar si el control ha sido efectivo, figura 13 y 14, esto lo podemos identificar en el informe de riesgo inherente:

Análisis de riesgo inherente
Seguridad de la información

Id Hallazgo	Tipo Dispositivo	Amenaza	Vulnerabilidad		Prob	Confi	Integ	Disp	Riesgo	Tratamiento
1	Hardware	Desastre Natural	Los equipos pueden ser afectados por inun		1	1	3	3	2	Aceptable
Id Act	Activo	Descripción	Tipo Activo	Ubicación					Impacto Cuant	Impacto Cualitativo
3	Radio Ettus N210	Hardware	Enclousure	Medellin					3	Bajo
2	Radio Ettus E310	Hardware	Enclousure	Medellin					3	Bajo
4	Otros Radios	Hardware	Enclousure	Medellin					3	Bajo
Id Hallazgo	Tipo Dispositivo	Amenaza	Vulnerabilidad		Prob	Confi	Integ	Disp	Riesgo	Tratamiento
2	Terceros	Disturbios sociales	El equipo puede ser comprometido por esp		5	5	5	5	25	No Aceptable
Id Act	Activo	Descripción	Tipo Activo	Ubicación					Impacto Cuant	Impacto Cualitativo
3	Radio Ettus N210	Hardware	Enclousure	Medellin					3	Bajo
4	Otros Radios	Hardware	Enclousure	Medellin					3	Bajo
2	Radio Ettus E310	Hardware	Enclousure	Medellin					3	Bajo

Fig. 13 Determinación del riesgo inherente

El cálculo se repite en el plan de acción y riesgo residual.

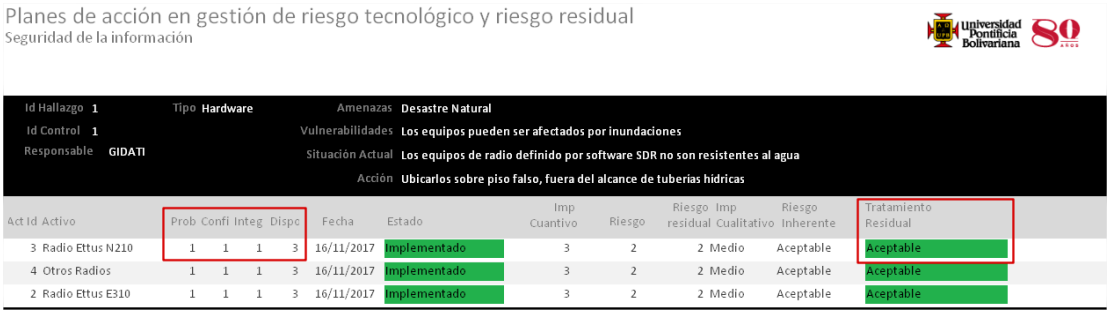

Fig. 14 Determinación del riesgo residual

1.5.8 Controles de remediación

Los controles de remediación se enuncian en el capítulo Planes de acción en gestión del riesgo tecnológico y residual, figura 15; Este plan indica que se debe hacer para mitigar el riesgo.

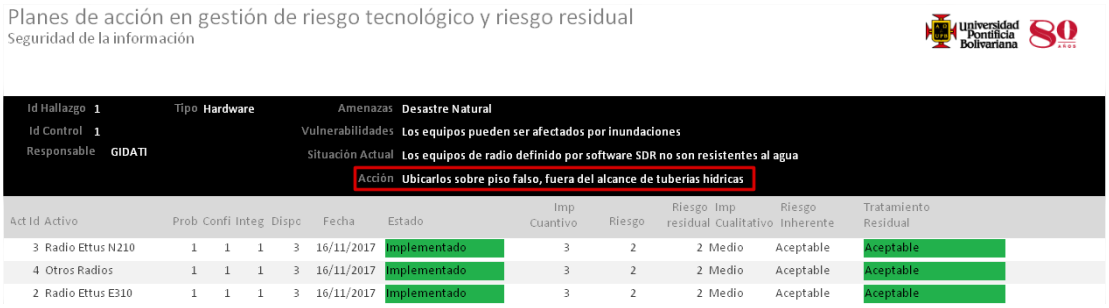

Fig. 15 Controles de remediación

1.6 Análisis de vulnerabilidades

El escaneo de vulnerabilidades ha sido apoyado con la herramienta *Nessus 6.9.3* cuyo informe se puede encontrar en los anexos como Ettut_310_nntjfd.pdf. En el sistema, se ha creado un perfil para la evaluación, configurando los siguientes ítems de evaluación:

1.6.1 Fuerza Bruta

Para la configuración de la herramienta se define los parámetros para la evaluación de ataque por fuerza bruta como podemos ver en la figura 16 Configuración de fuerza bruta.

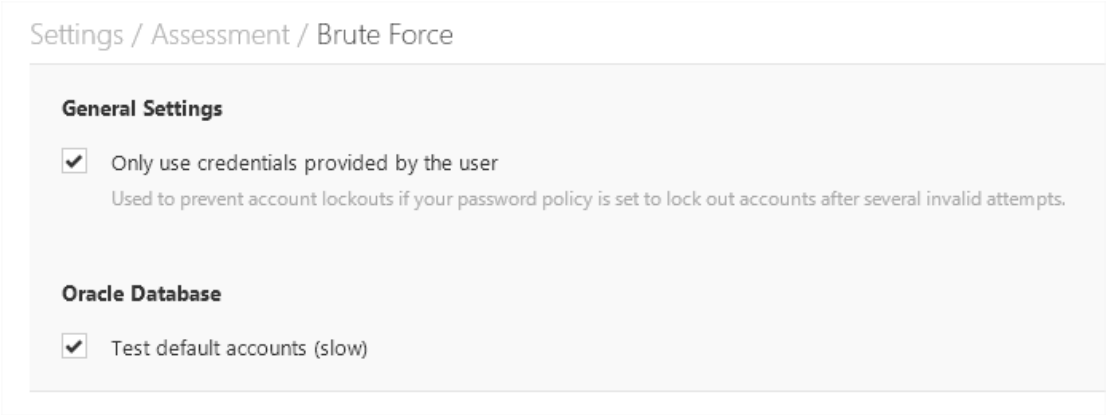

Fig. 16 Configuración de fuerza bruta

1.6.2 Plugins activados

A continuación, se muestran los Plugins habilitados para el escaneo de vulnerabilidades en la figura 17.

ENABLED	Backdoors	108
ENABLED	CentOS Local Security Checks	2326
ENABLED	CGI abuses	3567
ENABLED	CGI abuses : XSS	632
DISABLED	CISCO	779
DISABLED	Databases	513
ENABLED	Debian Local Security Checks	4553
ENABLED	Default Unix Accounts	159

ENABLED	Denial of Service	109
ENABLED	DNS	149
DISABLED	F5 Networks Local Security Checks	456
ENABLED	Fedora Local Security Checks	10788
ENABLED	Firewalls	180
ENABLED	FreeBSD Local Security Checks	3537
ENABLED	FTP	247
ENABLED	Gain a shell remotely	280

ENABLED	General	231
ENABLED	Gentoo Local Security Checks	2390
DISABLED	HP-UX Local Security Checks	1984
DISABLED	Huawei Local Security Checks	17
ENABLED	Incident Response	44
DISABLED	Junos Local Security Checks	157
DISABLED	MacOS X Local Security Checks	1014
DISABLED	Mandriva Local Security Checks	3139

ENABLED	Misc.	1350
DISABLED	Mobile Devices	63
ENABLED	Netware	14
DISABLED	Oracle Linux Local Security Checks	2443
DISABLED	OracleVM Local Security Checks	336
DISABLED	Palo Alto Local Security Checks	38
ENABLED	Peer-To-Peer File Sharing	82
ENABLED	Policy Compliance	45

ENABLED	Red Hat Local Security Checks	4199
ENABLED	RPC	37
DISABLED	SCADA	281
ENABLED	Scientific Linux Local Security Checks	2212
ENABLED	Service detection	423
ENABLED	Settings	79
DISABLED	Slackware Local Security Checks	930
DISABLED	SMTP problems	135

ENABLED	SNMP	33
DISABLED	Solaris Local Security Checks	3904
DISABLED	SuSE Local Security Checks	9578
ENABLED	Ubuntu Local Security Checks	3560
DISABLED	VMware ESX Local Security Checks	112
ENABLED	Web Servers	994

Fig. 17 Plugins activados

Ejecutamos el perfil que hemos configurado en la herramienta, obteniendo los siguientes resultados, figura 18.

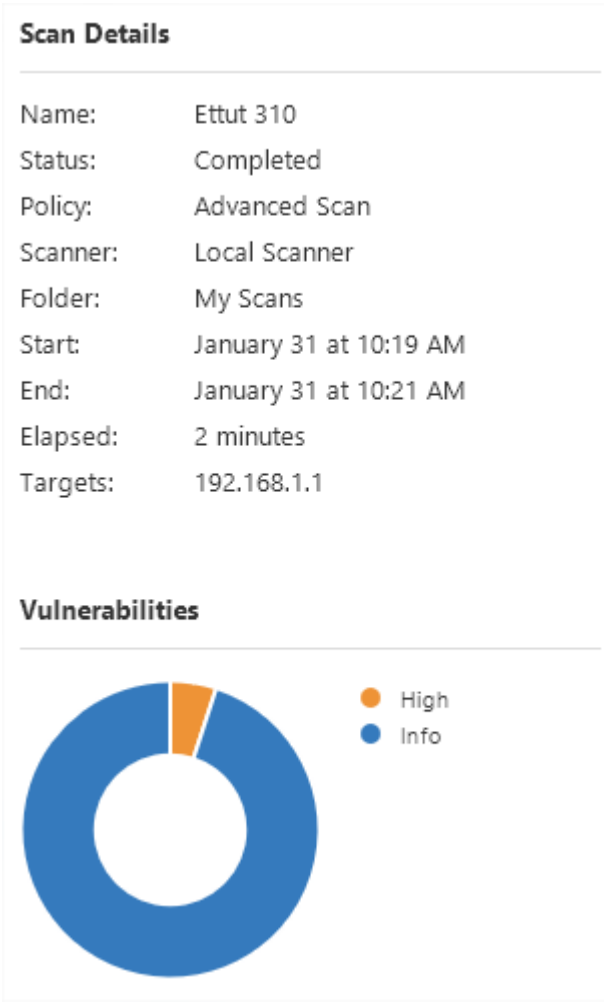

Fig. 18 Perfil de la herramienta

192.168.1.1

Scan Information

Start time:	Tue Jan 31 10:19:08 2017
End time:	Tue Jan 31 10:21:17 2017

Host Information

IP:	192.168.1.1
MAC Address:	00:80:2f:21:42:b4
OS:	Linux Kernel 3.14.2-xilinx (armv7l)

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	0	0	27	28

Fig. 19 Resumen de ejecución del perfil

En el sistema operativo encontramos que existe una vulnerabilidad alta, figura 19, por la cual se podría detener el servicio de captura de información de la señal de radio, ya que existe una vulnerabilidad identificada como “Network Time Protocol Daemon (ntpd) read_mru_list() Remote DoS”, asi como 27 vulnerabilidades informativas existentes debido configuraciones por defecto que trae el dispositivo, aunque las vulnerabilidades informativas no representan riesgo en sí, se puede mejorar la configuración para que no despliegue la información adicional que entrega el sistema. Es importante configurar correctamente los servicios de SSH, puesto que la configuración por defecto está diseñada para que los usuarios puedan acceder fácilmente al dispositivo.

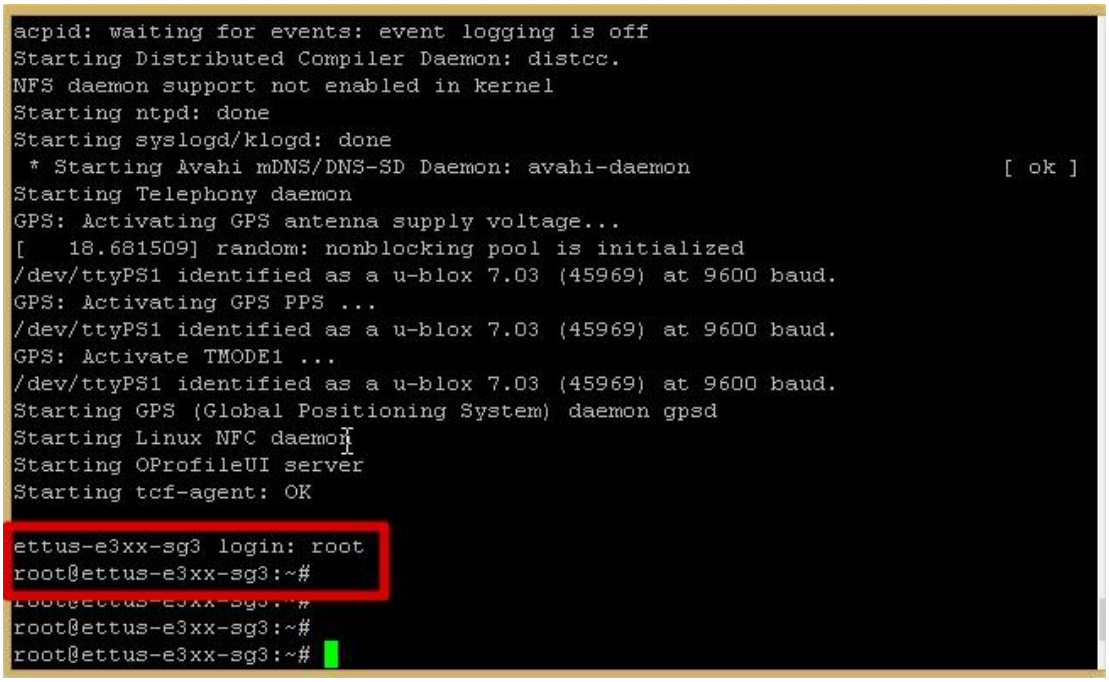

Fig. 20 Login sin password

En la figura 20, vemos que se puede ingresar escribiendo el usuario root sin contraseña, al ingresar se nota la usencia del banner de bienvenida también conocido como MOTD Message Off The Day, por sus siglas en ingles, donde se debería informar la confidencialidad del sistema, la propiedad y las normatividad que rigen al sistema; este es comportamiento en el sistema es consecuente con el estado de desarrollo del proyecto y su riesgo inherente, donde no hemos entrado a definir las directivas de seguridad, con el análisis de este comportamiento queda expresa la necesidad de definir las *lineas base* de configuración del sistema.

Como ejercicio adicional a la herramienta de escaneo de vulnerabilidades y a la inspección directa del dispositivo, se ha comprobado con comandos especiales de escaneo de puertos para obtener información adicional que orienten la busqueda de vulnerabilidades, mostradas en la figura 21.

Fig. 21 Escaneo de puertos

Con esta información se ha verificado la existencia de vulnerabilidades conocidas sobre estos servicios reportados; Encontramos que el puerto SSH contiene varias vulnerabilidades, frente a los algoritmos que ofrece para la comunicación, la falta de fortaleza en las contraseñas y el puerto funcionando en el número standard.

Encontramos al servicio de llamado de procedimiento remoto en el puerto 111, procedemos a revisar los servicios registrados con rpcinfo, figura 22.

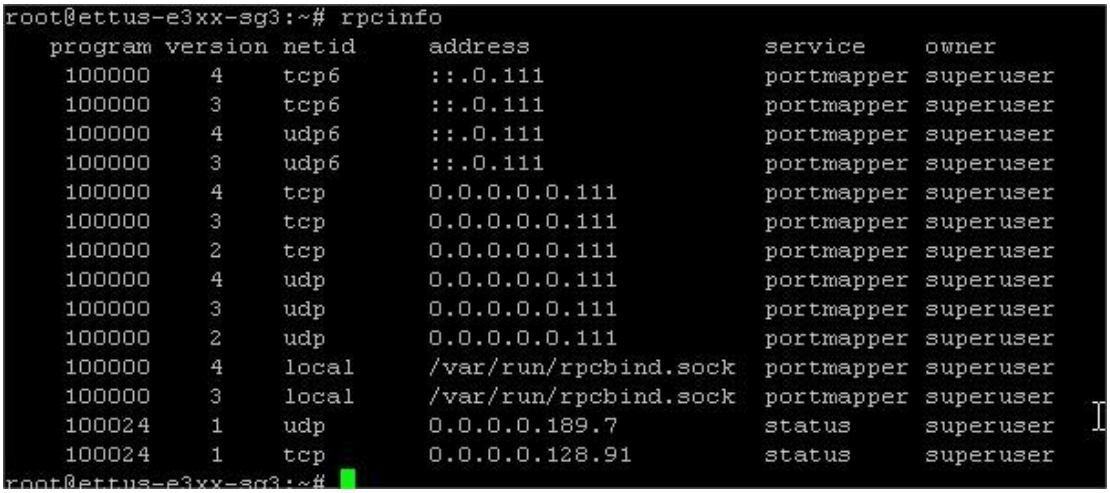

Fig. 22 Información RPC

Este servicio aporta información valiosa para un atacante si estuviera en uso el nfs network file system, ya que es usual encontrar este servicio corriendo junto con el servicio RPC, pero el sistema no muestra información que pueda ser explotada como vemos en la figura 23.

```
root@ettus-e3xx-sg3:~# showmount 192.168.1.1 -a
clnt_create: RPC: Program not registered
```

Fig. 23 Información NFS

El tercer puerto identificado corre un servicio llamado Xtell en el puerto 4224, este es un servicio encargado de llevar mensajería entre programas, se ha revisado quién está haciendo uso de este servicio, encontrando que es parte integral de la mensajería que usa GNU Radio, en la figura 24 podemos ver el servicio corriendo junto con sus variables de entrono y configuración.

```
root@ettus-e3xx-sg3:/etc# ps -ex|grep xtell
 1706 ttyPS0    S+     0:00 grep xtell HZ=100 SHELL=/bin/sh TERM=linux HUSHLOGIN=
FALSE USER=root LD_LIBRARY_PATH=/opt/gnuradio3_7_10git/lib: PATH=/opt/gnuradio3_
7_10git/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/sbin:/usr/sbin:/sbin PWD=/et
c EDITOR=vi TZ=UTC PS1=\u@\h:\w\$  SHLVL=1 HOME=/home/root PYTHONPATH=/opt/gnura
dio3_7_10git/lib/python2.7/site-packages: LOGNAME=root PKG_CONFIG_PATH=/opt/gnur
```

Fig. 24 Proceso xtell

Para este servicio de Xtell, se evidencia la necesidad de filtrar los equipos que pueden conectarse, ya que este servicio es vulnerable a Buffer Overflow, permitiendo ejecutar codigo arbitrario como lo podemos ver en la vulnerabilidad publicada en la lista Common Vulnerabilities and Expousures CVE-2002-0332, por lo que se revisa la configuración del firewall de linux IPTables como podemos ver en la figura 25 y aunque se puede compilar e instalar el programa, *no es factible hacer uso del software*, ya que este sistema de radio tiene una capacidad de procesamiento baja frente a la carga que significaría instalar un firewall en el dispositivo y es necesario reservar esa capacidad de computo para hacer los calculos de la señal de radio, por lo tanto, se ha desidido fijar este control externo al dispositivo, estableciendo el control en dispositivos de telecomunicaciones.

```
root@ettus-e3xx-sg3:~# iptables
-sh: iptables: command not found
root@ettus-e3xx-sg3:~#
```

Fig. 25 Verificación de firewall

Con este panorama encontrado escenario inicial, nos proponemos desarrollar unas reglas de configuracion y de arquitectura que permitan mitigar los riesgos inherentes al sistema hallados en el análisis de riesgos y apoyados con el análisis de vulnerabilidades.

CAPITULO 3

Plan de seguridad propuesto para el proyecto “Desarrollo de Capacidades Tecnológicas en Comprobación técnica del espectro”

Este capítulo recoge las propuestas para mitigar las vulnerabilidades del prototipo del sistema de sensado de espectro. Se seleccionó los dispositivos Ettus N210 y Ettus E310 para el aseguramiento. El principal reto de asegurar este prototipo es la eficiencia en computación, por el corto margen de maniobra para introducir defensas en el mismo dispositivo, siendo necesario apoyarse en componentes adyacentes para la defensa.

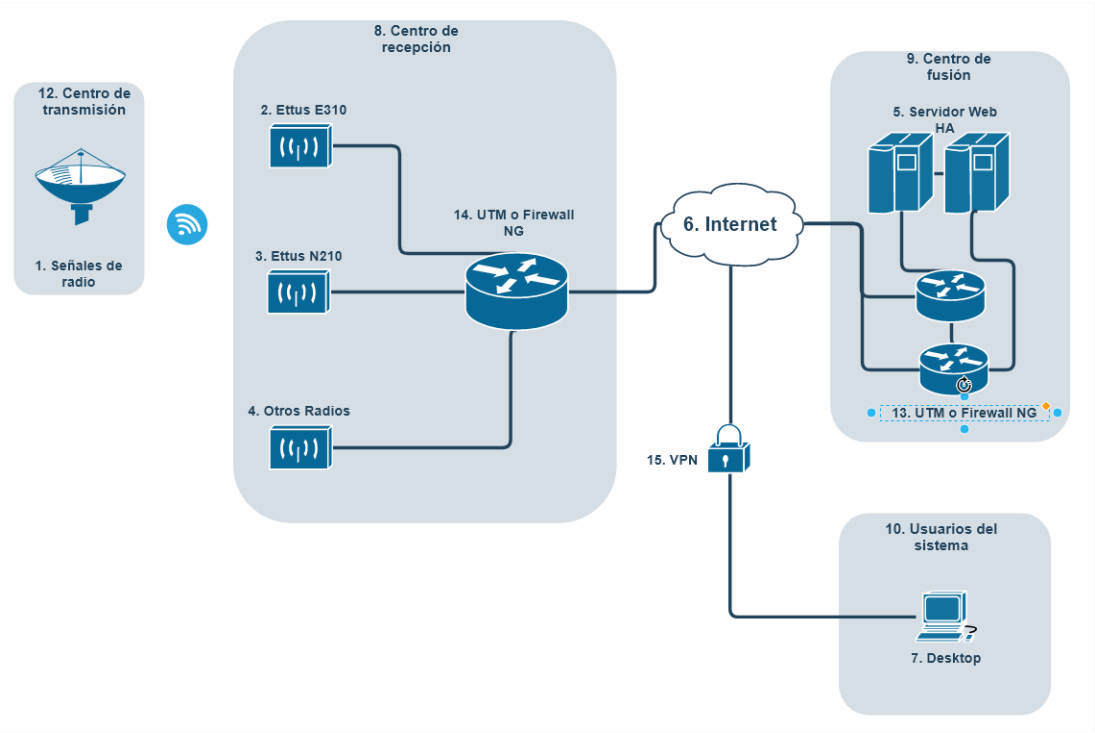

Fig. 26 Arquitectura propuesta

De la arquitectura inicial se propone implementar un Firewall de aplicación web (WAF), Sistema de prevención de intrusos (IPS), Sistema de detección de intrusos (IDS), Balanceo de carga, Antivirus de red y Firewall, dentro de un esquema de Alta disponibilidad HA para el Centro de fusión con todas sus conexiones cifradas por VPN hacia el exterior expuestas en la figura 26.

Para los centros de recepción se tendría un Sistema de prevención de intrusos (IPS), Sistema de detección de intrusos (IDS), Antivirus de red y Firewall, con sus conexiones cifradas por VPN. Los componentes físicos y lógicos los podemos ver en la tabla 17.

No.	Nombre	Componente lógico
1	Señales de radio	Componente único
2	Ettus E310	Componente único
3	Ettus N210	Componente único
4	Otros radios	Componente único
5	Servidor Web HA	Alta disponibilidad
6	Internet	Componente único
7	Desktop	Componente único
8	Centro de recepción	Componente único
9	Centro de fusión	Componente único
10	Usuarios del sistema	Componente único
12	Centro de transmisión	Componente único
13	UTM o Firewall NG Servidor 1	Firewall de aplicación web, Sistema de detección de intrusos, Firewall, Sistema de prevención de intrusos, Antivirus de red, Balanceador de carga, Alta disponibilidad, Virtual private network
14	UTM o Firewall NG Recepción	Firewall de aplicación web, Sistema de detección de intrusos, Firewall, Sistema de prevención de intrusos, Antivirus de red, Balanceador de carga, Alta disponibilidad
15	VPN	Software VPN del firewall NG

Tabla 17 Elementos de arquitectura

Los componentes únicos no tienen segmentación lógica, por lo tanto solo cuentan con la descripción establecida en el capítulo 2. La descripción de los demás componentes lógicos, los podemos ver a continuación en la arquitectura de seguridad.

1.7 Arquitectura de seguridad

1.7.1 Firewall NG o UTM

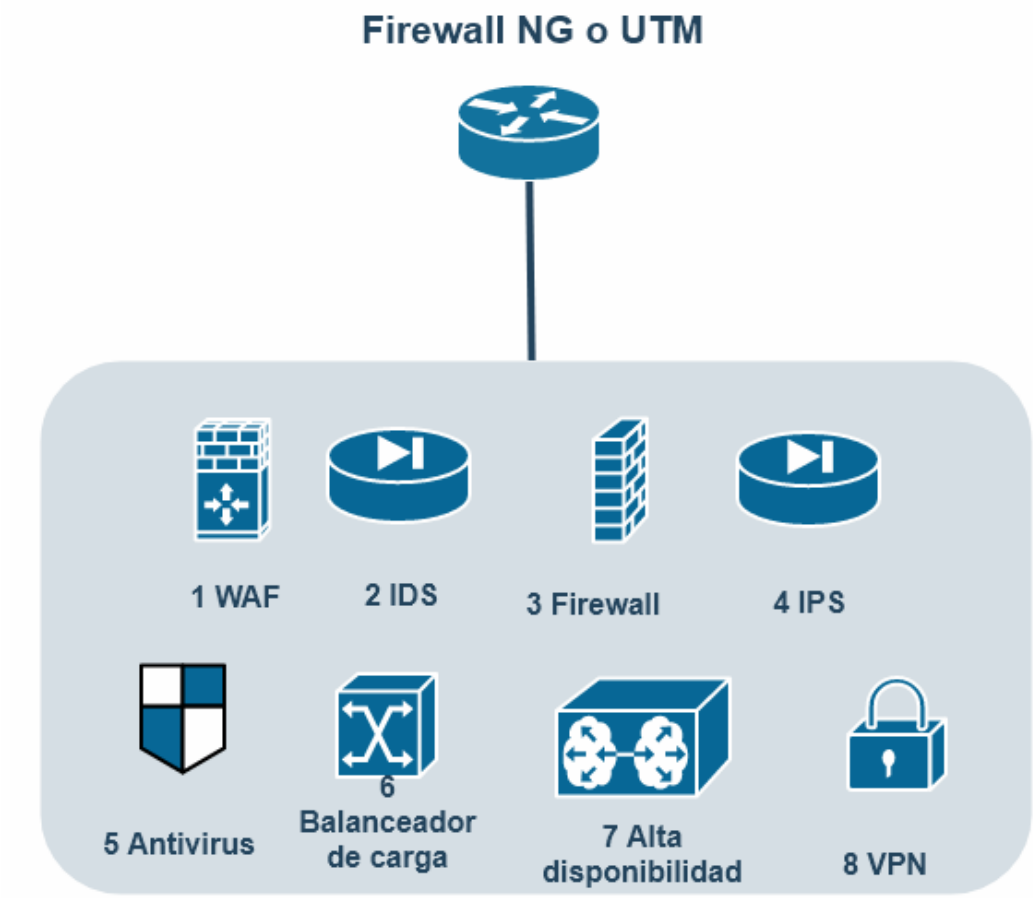

Fig. 27 Segmentación lógica

Los sistemas de seguridad anteriormente expuestos, vienen a ser suplidos por el dispositivo de manejo de amenazas unificado UTM por sus siglas en inglés o un firewall de próxima generación Firewall NG, figura 27. Estos incluyen de manera integral el Firewall, Sistema de detección de intrusos, Sistema de prevención de intrusos, Firewall de aplicación, Balanceador de carga y Antivirus de red, presentando estos dispositivos en un modelo de alta disponibilidad, duplicando su presencia física en los puntos críticos, como podemos ver en la figura 26

Arquitectura propuesta. También podemos ver la duplicación del servidor del centro de fusión, aplicando el concepto de alta disponibilidad. Esto nos da una arquitectura compacta y fácil de manejar.

La integración de los servicios en el Gateway de la red es llamado Comprehensive Gateway Security Service (CGSS)[15], la cual provee una protección en tiempo real de la capa de aplicación frente a ataques como virus, troyanos, gusanos, vulnerabilidades conocidas y de denegación de servicio. Para la implementación y selección de estos dispositivos, es necesario tener un estimado del tráfico para su dimensionamiento, afectando así los costos de la implementación, pero no está dentro del alcance de la investigación establecerlos, a continuación expondremos cada uno de los elementos incorporados en este dispositivo.

1.7.1.1 Firewall de aplicación web

Incorporamos un Firewall de aplicación web, ya que es un control que se implementa para revisar la comunicación http, buscando prevenir los ataques más comunes como Inyección por sentencia SQL (SQLi), o Cross Site Scripting XSS dentro de las amenazas más comunes de las aplicaciones web[10], que están presentes dentro de nuestros hallazgos como el número 89 del anexo informe de riesgos “Perdida de integridad de la información por SQLi, XMLi, JSONi”. Para cumplir con este control, también se analizó herramientas opensource modsercurity, una de las herramientas más populares, la cual podemos encontrar en https://modsecurity.org/. Esta representa una herramienta de control factible, gracias al bajo costo de entrada, también encontraremos algunas herramientas comerciales como Fortiweb, F5 ASM, entre otros, los cuales cumplen con el control requerido. Estas herramientas de pago cuentan con soporte especializado, mientras que el soporte de las herramientas opensource, están soportadas por comunidades virtuales que se unen en torno a las herramientas.

El impedimento para usar herramientas open source como modsecurity son las siguientes:

- Plugin corriendo en cada servidor de aplicaciones. Esto significa que se añade una carga adicional de cómputo para validar las reglas del firewall de aplicación, lo que podría afectar su desempeño conforme se aumente la cantidad de transacciones.

- Experticia para escribir las reglas. Para poder escribir una regla, se necesita conocer exactamente cómo funciona un ataque para poder prevenirlo. Generar

este conocimiento toma tiempo y no se podría delegar fácilmente la administración.

- Experticia para entender los protocolos. Para que las reglas escritas sean efectivas, se necesita conocer bien los protocolos de comunicación, para no interrumpir su comunicación en el proceso de sanitización de la comunicación.

- La mayoría de las configuraciones deben ser manuales.

- Las ventajas de usar una herramienta plugin como modsecurity son las siguientes:

- Bajo costo de implementación

- Conocimiento apoyado en una comunidad virtual con apoyo del desarrollador de obtener soporte comercial

- Código abierto, al ser una herramienta de código abierto presenta transparencia en su desarrollo

- Versatilidad para el desarrollo de nuevas reglas

- Ventajas de usar una herramienta de pago:

- Mejor desempeño en la detección de ataques

- Aprendizaje automático

- Posibilidad de integrar el balanceador de carga con el WAF

- Flujo de trabajo para configuración por plantillas

- Amplio soporte comercial

- Rápido desarrollo frente a ataques de día cero por parte del soporte del fabricante

- Diseño de arquitectura de software/hardware en alta disponibilidad

- Academia de enseñanza de la herramienta

- Fácil integración con herramientas de monitoreo SIEM

- Desventajas de una herramienta de pago:

- Alto costo de implementación
- Mayor espacio físico para su despliegue
- Costos operativos adicionales

Por lo expuesto anteriormente, se resalta que modsecurity necesita un plugin corriendo en el servidor, por lo que requeriría procesamiento adicional con el que no se cuenta en los ETUS por su limitado desempeño, por lo que se descarta en el diseño. Para las marcar comerciales se encuentra que en cuanto a efectividad, unas características muy parecidas en desempeño y efectividad[11].

1.7.1.2 Sistema de detección de intrusos

Para nuestro diseño es necesario contar con un sistema de prevención de intrusos IDS por sus siglas en inglés, ya que este, es un sistema que se encarga de la detectar accesos no autorizados a nivel de red o a nivel de host. Encontramos estos sistemas en dos categorías, Sistema de detección de intrusos de red NetworkIDS NIDS por sus siglas en inglés y Sistema de detección de intrusos de equipo HostIDS o HIDS por sus siglas en inglés.

El sistema de detección de intrusos incorporado debe contar con las siguientes características de detección[12]:

- Detección por base de firmas: Nuestro sistema debe detectar los ataques mediante la firma o huella del tipo de ataque, este es el método más rápido y efectivo, ya que cosiste en la comparación del ataque conocido contra la base de datos de firmas. Esta es solo una de las características que debe tener ya que este solo es efectivo frente a ataques conocidos.

- Detección por comportamiento: Para complementar la detección de intrusos el IDS incorpora la revisión de patrones en las comunicaciones, siendo muy efectivo para detectar vulnerabilidades desconocidas o abuso de privilegios.

- Detección por políticas: Con esta característica podríamos definir claramente las reglas o políticas para los protocolos que están participando de la comunicación, siendo capaz de distinguir comandos dentro de los protocolos para los cuales no se haya autorizado su ejecución. Su debilidad es el alto consumo de recursos para evaluar las políticas.

La baja capacidad de cómputo de los Ettus implica el descarte del uso de los HIDS, siendo más adecuado el uso de un NIDS. Por lo tanto, la recomendación sería usar un NIDS para detectar las amenazas de intrusos en el sistema, para controlar amenazas como “Acceso indebido por abuso de derechos”, “Acceso indebido por falsificación de derechos” o “Acceso indebido por ataque de fuerza bruta”, presentes en las amenazas del sistema.

1.7.1.3 Firewall

Incorporamos un Firewall en el diseño, porque este dispositivo nos ayudará a revisar los paquetes, descartando aquellos que no cumplan con las listas de control se accesos ACL por sus siglas en ingles. El dispositivo se encargará de llevar un registro de todos los accesos que se estén llevando a cabo, en caso de no encontrar el registro de acceso, lo detectará como un acceso no permitido, descartando los paquetes de comunicación.

Este dispositivo debe trabajar en conjunto con el Sistema de Detección de Intrusos IDS y el Sistema de Prevención de Intrusos IPS para proteger efectivamente los sistemas; sus reglas deben ser definidas sobre cada uno de los puertos red de entrada y salida, y debe tener la capacidad de recibir actualizaciones de las reglas de los otros sistemas de detección[13].

La recomendación de este control, es brindar la capacidad de zonificar las redes, separando las zonas de acceso externo DMZ o zonas desmilitarizadas, de las zonas internas, actuando sobre la capa 2, 3 y 4 del modelo OSI, extendiendo su control sobre las MAC, las IP y los puertos, ayudando a controlar amenazas como “Acceso indebido a la información por uso no autorizado”, “Divulgación de información por espionaje remoto”.

1.7.1.4 Sistema de prevención de intrusos

El Sistema de prevención de Intrusos IPS por sus siglas en inglés, nos ayuda a articular las funcionalidades de un Firewall y un Sistema de Detección de Intrusos, descartando inmediatamente los paquetes sospechosos, actuando inmediatamente sobre la comunicación[12], apoyando así la protección de las zonas de red a las que se tienen acceso. Su ubicación debe ir de cara a la WAN en la parte externa de la red y la LAN en la parte interna de la red.

Este control brinda seguridad a los ETTUS, descargando en el IPS el análisis de grandes flujos de tráfico sin afectar los cómputos de geolocalización que se deben realizar, ya que el apoyo viene adyacente al tráfico de los paquetes de red para el cual el IPS está optimizado, dando la capacidad de subir hasta la capa 7 del

modelo OSI, esto nos da el control de amenazas como “Denegación de servicio por DoS ó DDoS”, “Acceso indebido por explotación de vulnerabilidad conocida” y “Acceso indebido por ataque de fuerza bruta”.

1.7.1.5 Antivirus de red

Esta funcionalidad nos permite identificar y eliminar programas malignos del tráfico de la red que puedan estar amenazando las computadoras, como gusanos, troyanos, etc. La particularidad del antivirus de red es que funcionan en la capa de comunicaciones, impidiendo que la transmisión del software malicioso se complete, siendo muy efectivo para la eliminación de este tipo de amenazas.

La recomendación de este control, apoya el funcionamiento de los ETTUS, ya que el control está optimizado para analizar grandes flujos de tráfico, impidiendo que se completen las transmisiones del software malicioso, eliminando la necesidad de instalar antivirus en los ETTUS, solucionando la limitante de procesamiento de los mismos, con esto controlamos amenazas como "Fuga de información por instalación de spyware”, “Mal funcionamiento del equipo por pertenecer a una botnet", "Mal funcionamiento del equipo por troyano”, “Mal funcionamiento del equipo por adware","Mal funcionamiento del equipo por driver-by-downloads", "Mal funcionamiento del equipo por instalación de rootkit", "Mal funcionamiento del equipo por virus", "Perdida de confidencialidad por instalación de backdoors" y "Secuestro de información por instalación de ransomware"

1.7.1.6 Balanceador de carga

El balanceador de carga es un dispositivo de hardware que nos ayudará a balancear el tráfico de las peticiones entrantes hacia los servidores usando algún algoritmo dentro de los siguientes especificados.

- Round Robin: Este método es parecido al de tomar turnos, el cual va distribuyendo desde el primero hasta el último y comenzando nuevamente cuando llega al final.

- Round Robin con peso: Este método usa el sistema de turnos, pero entrega la carga dependiendo del peso que se tenga asignado, es decir si tengo dos servidores en la cola y uno tiene peso de 2 y el otro peso de 1, se entregaran el doble de paquetes al servidor con peso de 2.

- Least Connection: Este método entregará la conexión al servidor que cuente con menos conexiones en el instante.

- Least Connection con peso: Este método entregará la conexión al servidor que cuente con menos conexiones en el instante, pero sobrecargando al servidor que tenga más peso.

Con esta distribución de peticiones estaremos garantizando la disponibilidad del servicio en el centro de fusión, gracias a que si un servidor queda fuera de servicio, sería detectado automáticamente por el balanceador y distribuida su carga hacia los servidores adyacentes para procesar las peticiones[14].

1.7.1.7 Alta disponibilidad

Este concepto es incorporado en el diseño propuesto con el objetivo de asegurar la disponibilidad del servicio, principalmente en el centro de fusión, teniendo en cuenta los puntos de fallos potenciales, añadiendo redundancia física y lógica en los componentes críticos, su incorporación mitiga amenazas como "Desconexión de los equipos por fallas en el suministro de energía", "Error de comunicación por fallas en las redes de comunicaciones" y "Indisponibilidad de los equipos críticos de enrutamiento en el datacenter". Este concepto lo aplicamos a las UTM o Firewall NG y a los servidores Web.

1.7.1.8 Virtual Private Network VPN

La red privada virtual nos da la capacidad de aislar nuestra mensajería del tráfico de internet, ya que nos brinda una capa de cifrado, autenticación y autorización, necesaria para mantener alejados a los interesados malintencionados de su contenido.

1.7.2 Seguridad en los switch

El modelo propuesto no incluye los switch, ya que, para la cantidad de dispositivos en el sistema, sería suficiente con los 4 puertos que traen la mayoría de los dispositivos de seguridad. Es trascendente remarcar el uso de las VLAN en caso de hacer uso de estos dispositivos, ya que nos proveen segmentación de la red, eliminando el broadcast y aumentando la seguridad y el acceso a los recursos.

1.8 Línea base de los radios

Para los dispositivos ETTUS hemos definido el conjunto de parámetros y configuraciones necesarias con el fin de elevar la seguridad. La línea base expuesta a continuación debe ser aplicada a cada uno de los dispositivos a ser desplegados en el sistema de monitoreo.

1.8.1 Cambiar Contraseñas por Defecto

Buena práctica

Se deben cambiar las contraseñas que traen por defecto las cuentas del dispositivo. Esto se debe hacer siempre que no sea posible remover o deshabilitar la cuenta.

Solución

Creación de cuentas de usuarios
Para que los usuarios ingresen con contraseñas únicas, se debe usar el siguiente comando:

#useradd (nombre de usuario)
#passwd (nombre del usuario)

Cuando el usuario realice su primera autenticación, se le pedirá el cambio de contraseña.

#change –d 0 (nombre del usuario)

Este comando sirve para que un usuario se autentique con usuario y contraseña que le asignaron los administradores y paso seguido, lo fuerce a cambiar la contraseña.

Referencias

- El sistema debe forzar el cambio de contraseñas temporales generadas automáticamente después de su primer uso.

- Garantizar que las contraseñas proporcionadas, al crear o modificar una cuenta de usuario, sean seguras.

1.8.2 Configurar Autenticación Segura

Buena práctica

Se debe endurecer la autenticación para los usuarios sobre los sistemas operativos críticos, mitigando la posibilidad de dejar la consola desatendida.

Solución

Establecer el tiempo permitido para tener una consola establecida sin actividad.

Verificar que los siguientes parámetros de configuración se encuentran en el archivo /etc/profile.d

Crear el archivo sshautologout.sh con el siguiente comando.

touch /etc/profile.d autologout.sh

Establecer los valores de las variables para presentar sshautologout.sh con los siguientes comandos.

echo "TMOUT = 300" >> / etc / profile.d / autologout.sh
echo "readonly TMOUT" >> / etc / profile.d / autologout.sh
echo " export TMOUT " >> / etc / profile.d / autologout.sh

Configurar los permisos del archivo.

chmod + x / etc / profile.d / sshautologout.sh

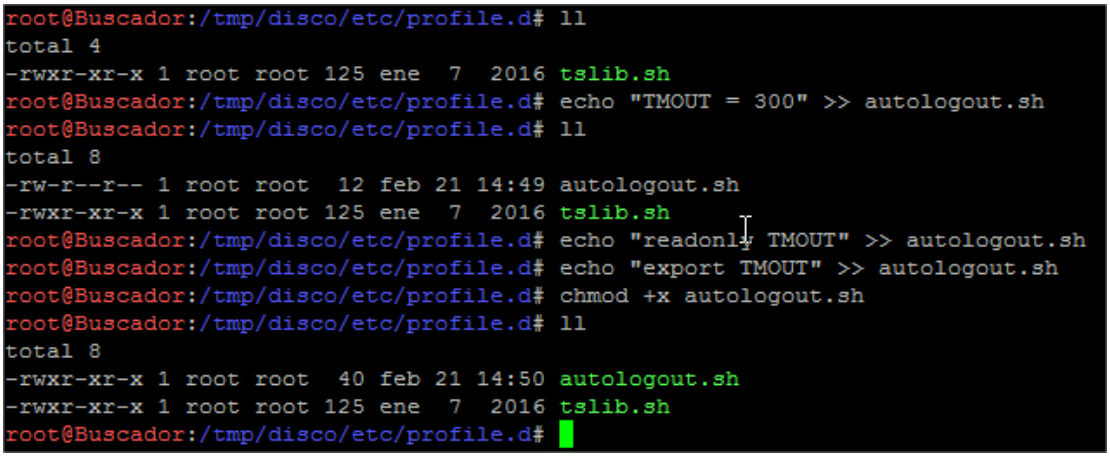

Fig. 28 Ssh auto logout

Configurar el intervalo de tiempo de espera de los clientes SSH, figura 28.

SSH permite a los administradores establecer un intervalo de tiempo de inactividad. Después de este intervalo ha pasado, el usuario con inactividad se desconectará automáticamente.

Abrir el archivo /etc/ssh/sshd_config para establecer los valores para los siguientes parámetros, figura 29.

ClientAliveInterval = 300
ClientAliveCountMax = 0

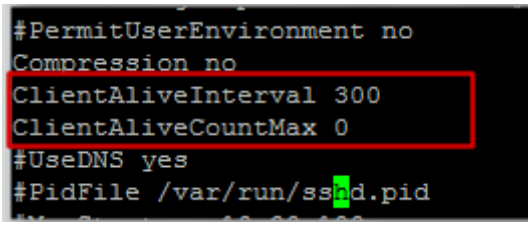

Fig. 29 Ssh Tiempo de sesión

Reiniciar el servicio con el siguiente comando.

service sshd restart
Stopping sshd: [OK]
Starting sshd: [OK]

Ocultar la información del sistema para prevenir ataques.

Editar el archivo /etc/issue
Eliminar la información de la versión del sistema operativo, figura 30

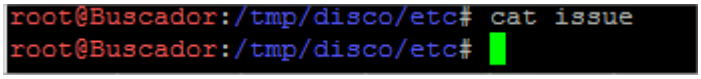

Fig. 30 Información de sistema operativo

Asignar un banner de ingreso al sistema

Asignar el banner para el ingresar por ssh.

Editar el archivo sshd_config

vi /etc/ssh/sshd_config

Agregar la línea Banner /etc/banners, figura 31

Fig. 31 Banner MOTD

```
#  echo "
   *     ************************************          *
   *     *   ! ! ! ! !  ATENCION ! ! ! ! !  *       *
   *     ************************************          *
   *                                        *
   *  Su ingreso a este sistema fue reportado a                    *
   *  nuestro servidor de monitoreo y gestión.                     *
   *  Cualquier modificación debe ser aprobado por                 *
   *  el Ministerio de Comunicaciones.                *
   *  LOS USUARIOS QUE INGRESEN SIN AUTORIZACION      *
   *  SERAN SUJETOS  A INVESTIGACION Y PODRAN              *
   *  RECIBIR ACUSACIONES PENALES BAJO LA LEY 1273     *
   *  DE 2010 Y/O  SANCIONES DISCIPLINARIAS POR           *
   *  PARTE DE LA ORGANIZACION.                                    *
 " >> / etc / bannerSsh
```

1.8.3 Definir Autenticación Root

Buena práctica

El SO debe estar configurado de tal forma que no permita que el usuario *root* o Administrador pueda autenticarse directamente; para esto debe ingresar mediante cambio de identidad

Solución

Requerir ingresar como usuario y luego escalar los permisos a super usuario.

```
> sudo su
```

root's password:

Editar el siguiente archivo

edit /etc/ssh/sshd_conf

En la línea PermitRootLogin debe estar el valor no, figura 32

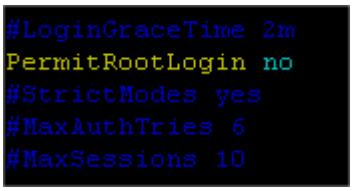

Fig. 32 Prohibir login de root

Referencias

- La gestión administrativa del sistema debe realizarse a través de usuarios con privilegios de administración que permitan el registro de tareas a cada individuo.

1.8.4 Deshabilitar Parámetros en Archivo Seguro

Buena práctica

Se debe utilizar el sistema de archivo más seguro que posea el sistema operativo.

Solución

Se deben deshabilitar los siguientes parámetros en el archivo /etc/modprobe.d/blacklist, figura 33, su descripción la podemos encontrar en la tabla 18.

blacklist cramfs
blacklist freevxfs
blacklist jffs2
blacklist hfs
blacklist hfsplus
blacklist squashfs
blacklist udf

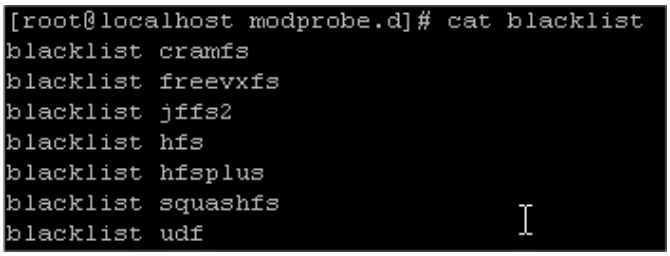

Fig. 33 Prohibir sistema de ficheros inseguros

Parámetro	*Descripción*
Cramfs (compressed RAM file system)	Es un sistema de archivos diseñado para simplicidad y eficiencia en espacio. * Es un sistema de solo lectura. No soporta control de acceso sobre los archivos
Freevxfs	Sistema de archivos VERITAS VxFS (TM)
jffs2	Es un sistema de ficheros con soporte para transacciones especializado en memorias Flash.
Hfs	Es el sistema de archivos utilizado por las máquinas con sistema operativo MacOS . No soporta cifrado ni registro de cambios en archivos
Hfsplus	Es el sistema de archivos utilizado por las máquinas con sistema operativo MacOS . No es posible implementar listas de control de acceso en este sistema de archivos
Squashfs	Es un sistema de archivos diseñado para compresión de archivos.

Tabla 18 Sistemas de ficheros inseguros

Referencias

- La organización debe deshabilitar las funciones innecesarias de un servicio. (Hardening de servicios)

1.8.5 Gestionar Usuarios

Buena práctica

Las diferentes funciones que se realizan en el sistema operativo, tales como administrar, operar, monitorear, respaldar información, entre otras, deben ser asignadas a usuarios diferentes para garantizar el principio de segregación de funciones.

Solución

Creación de grupo y Usuario seguro.

Existe control de usuarios y grupos en el núcleo de la administración del sistema. Los usuarios pueden ser gente real (cuentas ligadas a un usuario físico en particular) o usuarios lógicos (cuentas existentes para aplicaciones particulares).

Ambos tipos de usuarios, tienen un ID de usuario y un ID de grupo. Los IDs de usuario son únicos y los ID de grupos son expresiones lógicas de organización.

Los usuarios forman grupos y los grupos forman fundaciones de usuarios ligados a los que les dan permisos de lectura, escritura o de ejecución de un archivo determinado

Ejecutar los siguientes comandos para crear una cuenta de usuario desde el indicador de comandos de la shell:

1. En el indicador de comandos de la shell, regístrese como root.
2. Teclee useradd, deje un espacio, a continuación escriba el nombre de la nueva cuenta de usuario en la línea de comandos y pulse enter.
3. A continuación escriba passwd seguido de un espacio y del nombre de usuario de nuevo.
4. Debería ver New UNIX password en el indicador de comandos de la shell, pidiéndole que escriba la contraseña de la nueva cuenta.
5. Vuelva a ingresar la contraseña para confirmarla. (Verá el siguiente mensaje, indicándole que la nueva cuenta ha sido creada y passwd: all authentication tokens updated successfully)
6. El nombre de login que quiere que tenga este usuario y el nombre completo en los campos respectivos. Cada cuenta pertenece al menos a un grupo. Los grupos se usan para determinar los permisos a los accesos del fichero. El grupo por defecto para una cuenta de usuario será el mismo que un nombre de login.

Ingresar con la cuenta creada

Referencias

- El sistema no debe permitir a un actor del sistema, aumentar los privilegios para él mismo.

1.8.6 Implementar Políticas de Contraseñas

Buena práctica

Implementar y configurar políticas para la generación de cuentas en el sistema.

Solución

A continuación, se presentan los aspectos más importantes para implementar políticas de contraseñas y su implementación para un sistema basado en Linux, tiempo de vida de contraseñas y nuevas cuentas.

En los archivos /etc/login.defs y /etc/default/useradd se encuentran los parámetros a configurar relacionados con el tiempo de vida de las contraseñas las contraseñas.

Archivo /etc/login.defs, figura 34.

Password aging controls:
#
PASS_MAX_DAYS Maximum number of days a password may be used.
PASS_MIN_DAYS Minimum number of days allowed between password changes.
PASS_MIN_LEN Minimum acceptable password length.
PASS_WARN_AGE Number of days warning given before a password expires.

```
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   60
PASS_MIN_DAYS   1
PASS_MIN_LEN    10
PASS_WARN_AGE   7
```

Fig. 34 Políticas de contraseñas

Archivo /etc/default/useradd

INACTIVE=-1
EXPIRE=

Nota: El parámetro PASS_MIN_LEN en /etc/login.defs no ejerce ningún efecto. La longitud mínima de las contraseñas es controlada por el módulo pam_cracklib, que se explicará más adelante.

Cuentas existentes

El comando chage es usado para modificar los parámetros de tiempo de las contraseñas en cuentas que ya existen en el sistema. chage no actualiza el campo del último cambio de contraseña en /etc/shadow, por tanto, las contraseñas pueden expirar inmediatamente luego de correr el comando. Se debe correr con la opción -d para modificar el campo de último cambio de contraseña en /etc/shadow

Ejemplo:

El usuario pepe ya fue creado sin expiración de contraseña (parámetro PASS_MAX_DAYS=99999).

Se pretende configurar los siguiente:

Un mínimo de 7 días necesarios para poder cambiar la contraseña.
Que la contraseña expire luego de 90 días.
Generar advertencias de expiración de contraseña 14 días antes de que sea efectivo.

Comando: # chage -m 7 -M 90 -W 14 pepe

Cuando la cuenta expira, se genera un proceso de "gracia" en el que la contraseña es aceptada por el sistema, pero inmediatamente se debe cambiar la contraseña. En el momento en que se cambia la contraseña, la conexión se cierra y se debe iniciar sesión nuevamente:
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user pepe.
Changing password for pepe
(current) UNIX password:
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
Connection to host closed.
Longitud y Complejidad de contraseñas

Ambos, pam_cracklib y pam_passwdqc son módulos utilizados para fortalecer la longitud y complejidad de las contraseñas. Aunque pam_passwdqc es más poderoso, basta con pam_cracklib para tener las capacidades adecuadas en un ambiente de producción.

Ejemplo: Se requiere una longitud mínima de 9 caracteres, con al menos 1 caracter en minúscula, 1 caracter en mayúscula y un caracter numérico (dígito):

En el archivo /etc/pam.d/system-auth se configura la siguiente línea de la siguiente manera:

La línea:
password requisite /lib/security/$ISA/pam_cracklib.so retry=3

Se reemplaza por:
password requisite /lib/security/$ISA/pam_cracklib.so retry=3 minlen=12 lcredit=1 ucredit=1 dcredit=1 ocredit=0
Historial de contraseñas

El historial de contraseñas se utiliza para evitar el "re-uso" de antiguas contraseñas. Esto puede ser habilitado usando las librerías pam_unix (para almacenar las contraseñas antiguas) y pam_cracklib (para prevenir el "re-uso"). Por defecto, esta funcionalidad esta deshabilitada.

Para habilitar esta funcionalidad se debe:

Crear el archivo para almacenar las contraseñas antiguas:

```
# touch /etc/security/opasswd
# chown root:root /etc/security/opasswd
# chmod 600 /etc/security/opasswd
```

Configurar PAM. Se debe modificar en el archivo /etc/pam.d/system-auth:

A la línea:

password sufficient pam_unix.so nullok use_authtok md5 shadow

Se le agrega el parametro remember y su respectivo parámetro (para este ejemplo, el sistema recuerda las últimas 24 contraseñas):

password sufficient pam_unix.so nullok use_authtok md5 shadow remember=24
Bloqueo de cuentas

Para habilitar el bloqueo de cuentas luego de un número fallido de intentos, se debe utilizar la librería pam_tally, en la configuración de autenticación (auth) y en la configuración de cuenta (account).

Para habilitar esto con una gestión adecuada, se realiza lo siguiente:

Crear el archivo para almacenar los intentos fallidos

```
# touch /var/log/faillog
# chown root:root /var/log/faillog
# chmod 600 /var/log/faillog
```

Configurar PAM. Se debe modificar en el archivo /etc/pam.d/system-auth:

```
auth        required      pam_tally.so onerr=fail no_magic_root

account     required      pam_tally.so deny=5 no_magic_root reset
```

El módulo pam_tally en RHEL 3/4 no soporta el parámetro unlock_time. Se necesita correr un script periódicamente desde un cron para reiniciar el número de intentos fallidos. el root crontab debe quedar de la siguiente manera:

```
# Reset pam_tally counter twice hourly
0,30 * * * * /usr/local/bin/reset_failed_logins
```

1.8.7 Proteger Autenticación de Ataques de Fuerza Bruta

Buena práctica

Se necesita proteger la autenticación en consola frente ataques de fuerza bruta

Solución

Con el siguiente procedimiento aseguraremos la autenticación de Linux a ataques de fuerza bruta, este procedimiento contempla ataques al usuario root.

1. Editamos el archivo /etc/pam.d/password-auth y añadimos lo siguiente para que deshabilite la cuenta por 30 segundos.

```
auth required pam_tally2.so deny=3 even_deny_root unlock_time=30 audit
account  required  pam_tally2.so
```

El orden en que se insertan debe ser el descrito en la imagen siguiente, esto tendrá efectos en su funcionamiento:

2. Reiniciamos el servicio ssh

service sshd restart

3. Verificamos el tallylog

cat /var/log/tallylog

4. Revisamos el registro de claves erróneas
pam_tally2 -u Usuario1

5. Reseteamos el registro de claves erróneas de ser requerido
pam_tally2 -u Usuario1 –reset

Nota: El procedimiento bloquea la cuenta por 30 segundos, si se sufre de un ataque de fuerza bruta sostenido, el mismo ataque mantendrá la cuenta inhabilitada hasta que este cese y pasen 30 segundos. Las otras cuentas que se hayan creado se mantendrán activas.

1.8.8 Registrar Eventos

Buena práctica

El sistema operativo Linux debe realizar automáticamente el registro de los eventos del sistema, en especial la recolección de aquellos que representen un alto y mediano impacto en la disponibilidad del servicio.

Solución

Configurar en la ruta /etc/syslog.conf

Comando logger

Permite enviar mensajes al sistema de log del sistema
- Sintaxis: logger [opciones] [-p prioridad] [mensaje]
- La prioridad se especifica de la forma *facilidad.nivel* (por defecto, usa user.notice)

Establecer un almacenamiento de Logs centralizado

auth,user.* @LOGHOST
Kern.* @LOGHOST
Daemon.* @LOGHOST
Syslog.* @LOGHOST
lpr,news,uucp,local0,local1,local2,local3,local4,local5,local6.* @LOGHOST

Establecer un almacenamiento de Logs Local

auth,user.* /var/log/messages
kern.* /var/log/kern.log
daemon.* /var/log/daemon.log
Syslog.* /var/log/syslog
lpr,news,uucp,local0,local1,local2,local3,local4,local5,local6.*
/var/log/unused.log

Ejecutar el comando ls -la /var/log/ para verificar que se encuentren los siguientes archivos

-rw------- 1 root root daemon.log
-rw------- 1 root root kern.log
-rw------- 1 root root messages
-rw------- 1 root root syslog
-rw------- 1 root root unused.log

Cada archivo debe tener permisos de Lectura (r) y Escritura (w) -rw------

El permiso que debe asignar es 600 más el nombre del archivo para que queden de la siguiente manera.

Referencias

- Los eventos de seguridad del sistema que deben ser monitoreados deben estar identificados.
- La organización debe controlar que la configuración del BIOS en las máquinas sólo pueda ser accesible por personal autorizado.

- El sistema debe registrar el nivel de severidad para cada evento excepcional y de seguridad.
- El sistema debe restringir el acceso a objetos del sistema que tengan contenido sensible. Solo permitirá acceso a usuarios autorizados.

1.8.9 Verificar Registros

Buena práctica

Verificar registros en sistemas tipo Linux

Solución

Para verificar los registros en sistemas tipo Linux contamos con algunos comandos tales como:

tail: Muestra el contenido de un archivo en pantalla. También muestra registros en tiempo real.
grep: Es usado para buscar archivos de registro.
less: También puede mostrar en pantalla los registros.

En Linux los registros son comúnmente almacenados dentro del directorio /var/log.

Para poder visualizar los diferentes tipos de registros, vamos a mostrar un ejemplo de cómo visualizar los registros de tipo mensajes:

```
tail -f /var/log/messagess
less /var/log/messagess
more /var/log/messagess
```

Nota: Cómo podemos ver, podemos usar diferentes opciones para visualizar nuestros registros, la más usada suele ser tail –f.

También podemos hacer búsquedas de algún suceso determinado del cual estemos interesados en encontrar:

```
grep 'search-string' /var/log/messages
egrep 'word1|word2' /var/log/messages
```

Referencias

- El sistema debe registrar todos los eventos excepcionales y de seguridad en una o varias bitácoras.

1.9 Análisis de resultados

1.9.1 Amenazas presentes en el sistema

El sistema presenta 158 riesgos agrupados por tipo de amenaza en la tabla 19.

Amenazas	Número Amenazas	Porcentaje	Porcentaje acumulado	Acumulado
Malware	30	19%	19%	30
Ataque técnico	24	15%	35%	54
Falla técnica	16	10%	45%	70
Compromiso de funciones	15	10%	54%	85
Daño Físico	14	9%	63%	99
Fallas de infraestructura	14	9%	72%	113
Exposición de información	11	7%	79%	124
Violación de reglas	11	7%	87%	135
Perturbación por radiaciones	10	6%	93%	145
Contenido peligroso	6	4%	97%	151
Desastre Natural	3	2%	99%	154
Disturbios sociales	2	1%	100%	156
Total	156			

Tabla 19 Acumulado de amenazas por tipo de amenaza

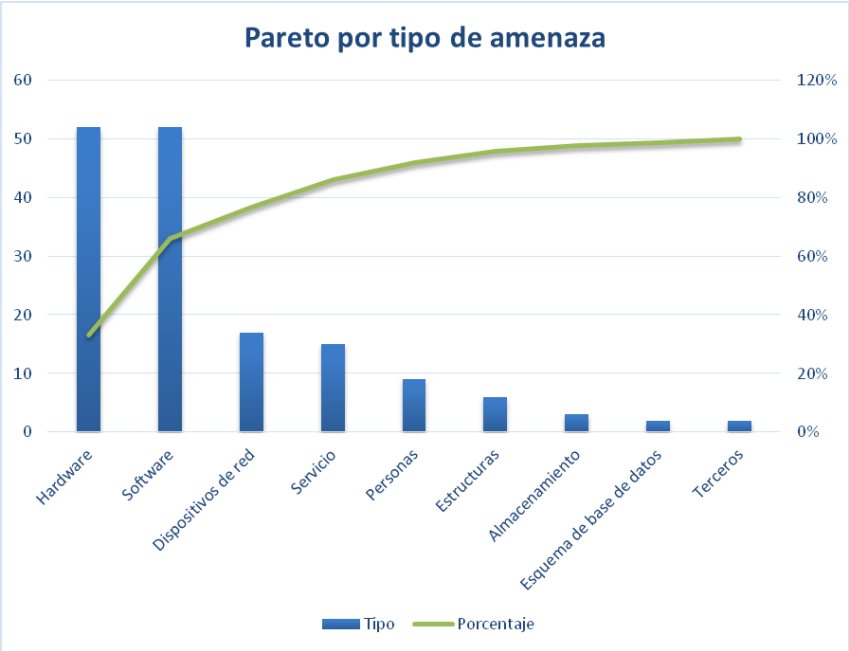

Fig. 35 Pareto de amenazas

La agrupación de los activos de información que intervienen en la valoración de activos y la evaluación de riesgos, demuestran que el impacto mas grande frente a las amenazas estarían relacionados con la arquitectura de seguridad, siendo necesario aplicar los conceptos en el punto 3.1 Arquitectura de seguridad. Enfocandonos inicialmente en los controles frente a Malware, Ataque Técnico y Falla Técnica, Compromiso de Funciones, Daño Físico, Fallas de infraestructura, Exposición de información lo que nos daría un cubrimiento del 80% frente a los riesgos evaluados, como podemos observar en la Figura 35.

1.9.2 Revisión de activos de información

En la tabla 20 podemos observar la distribución de las amenazas por el tipo de activo de información.

Tipo	Número	Porcentaje	Porcentaje acumulado	Acumulado
Hardware	52	33%	33%	52
Software	52	33%	66%	103
Dispositivos de red	17	11%	77%	120
Servicio	15	9%	87%	135
Personas	9	6%	92%	144

Estructuras	6	4%	96%	149
Almacenamiento	3	2%	97%	152
Esquema de base de datos	2	1%	99%	154
Terceros	2	1%	100%	156
Total	156	1		

Tabla 20 Tipo de activo de información

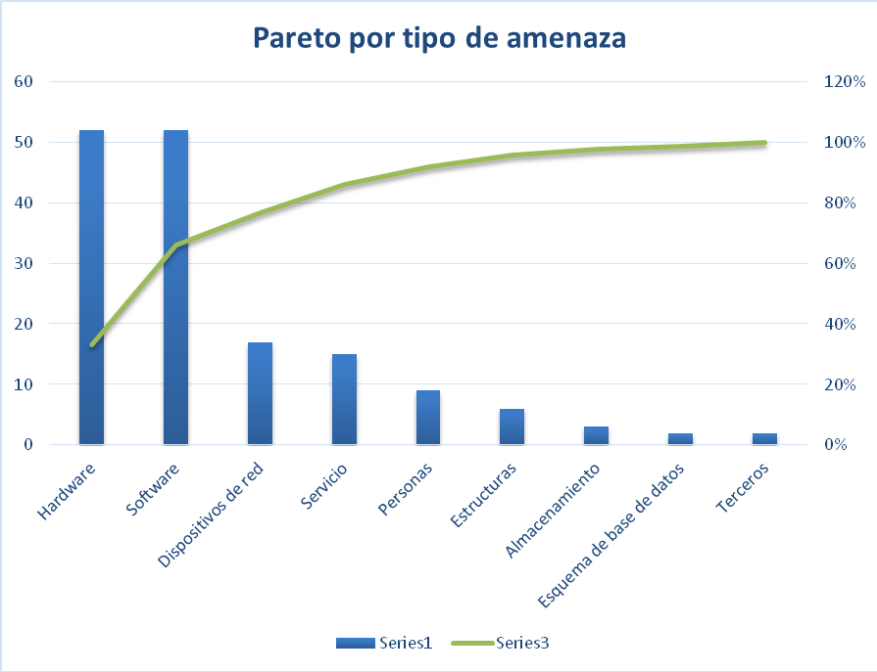

Fig. 36 Pareto por tipo de amenaza

Identificamos de la valoración de activos y la evaluación de riesgos, los componentes más importantes en el sistema, los cuales son el Hardware, Software, los Dispositivos de red y el Servicio como podemos ver en la Figura 36. Reflejando con datos la primera impresión que se tiene al principio de la evaluación, pero permitiendo a través de esta investigación, la priorización para el desarrollo de los controles, teniendo en cuenta el impacto que las amenazas puedan tener sobre el tipo de activo de información.

1.9.3 Covertura del plan de riesgos

Se hace un análisis independientemente del riesgo inherente, evaluando la implementación del control, y evaluando si la mitigación generada por el control es aceptable. Esto lo podemos ver en las tablas del análisis de riesgo, donde encontramos un tratamiento residual aceptable pero también evidenciamos un estado de no implementado, como podemos ver en el anexo de análisis de riesgos, donde teníamos un panorama inicial de riesgos inherente no aceptable del 75%, figura 37.

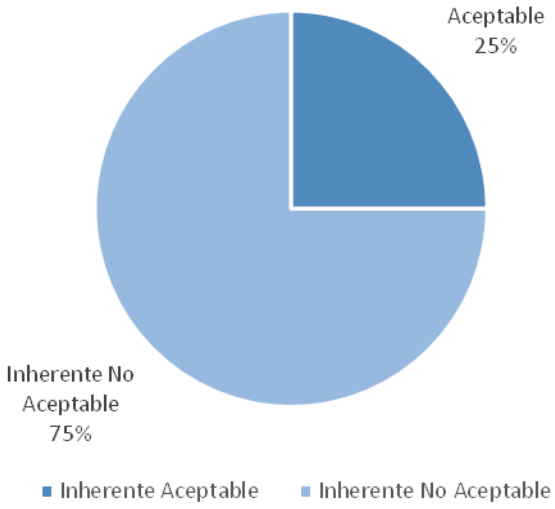

Fig. 37 Mapa inicial de riesgo inherente

Aplicando los controles realizados en el análisis, se mitiga el panorama de riesgos en un 98%, figura 38

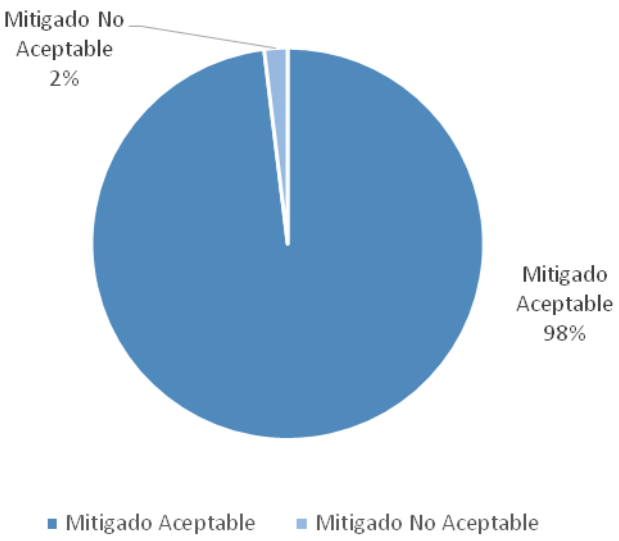

Fig. 38 Mapa de riesgo con controles

El 2% de los riesgos que no se pudieron controlar, obedecen a escenarios en los cuales quedan fuera del alcance de esta investigación, para lo cual se dejan abiertas iniciativas posteriores que profundicen el estudio, debido a su complejidad.

El Plan de tratamiento de riesgos es aceptable para los riesgos evaluados, esto refleja la efectividad del plan al 98%, siendo necesario evaluar el estado de la implementación nuevamente para identificar el avance en la mitigación de riesgos frente al sistema.

1.9.4 Efectividad del tratamiento del riesgo

De la revisión encontramos que para el monitoreo del espectro electromagnético, se parte de un sistema con alto nivel de riesgo, mostrando que es posible tomar el control del mismo, como se pudo evidenciar la entrada sin autorización como superusuario. Dando lugar a la necesidad de definir unas líneas bases para el sistema que eliminen las vulnerabilidades que traen los sistemas desde fábrica. Teniendo en cuenta está carencia de líneas base del sistema y la arquitectura de seguridad, además de los riesgos de otros componentes ajenos a los ETTUS, obtenemos el mapa de riesgos mostrado en la tabla 21.

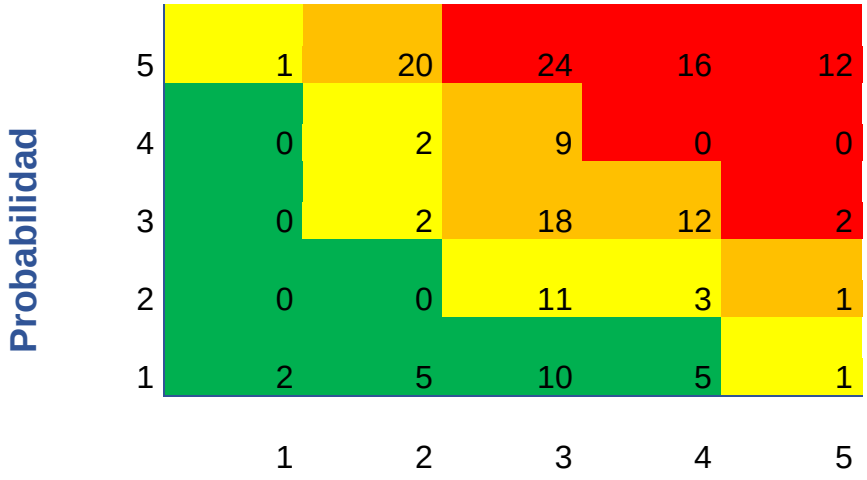

Tabla 21 Mapa de calor de riesgo inherente

Con la presente investigación se ha logrado cambiar este mapa al mostrado en la tabla 21, aplicando los controles descritos en el plan de acción hacia el mapa de la figura 22.

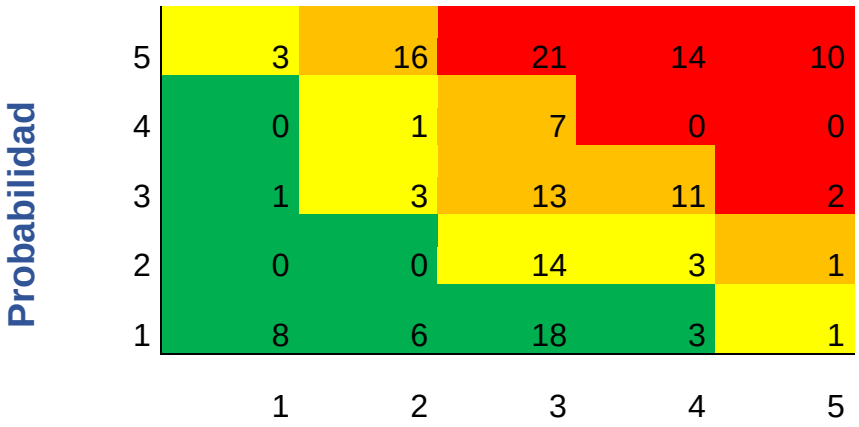

Tabla 22 Mapa de calor del riesgo residual avance actual

Teniendo en cuenta que el estado ideal del plan de trabajo plantea llevar los riesgos al mapa de calor de la tabla 23.

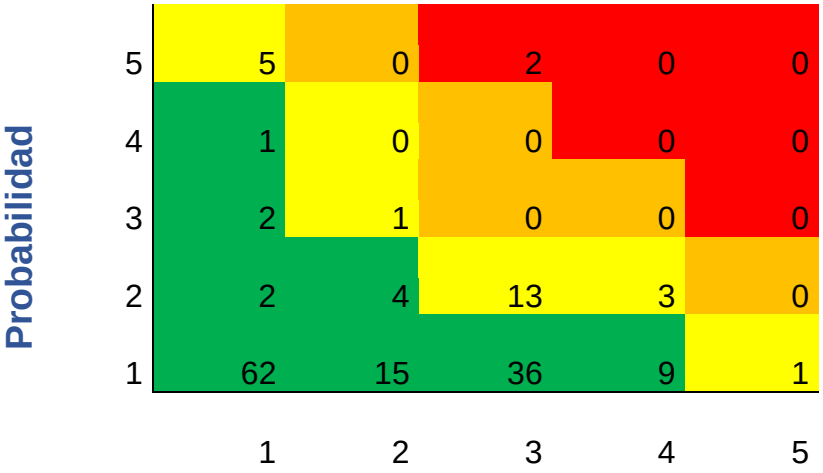

Tabla 23 Mapa de calor del riesgo residual planeado

En el mapa de calor del riesgo inherente tabla 21, se identifica que existen 114 vulnerabilidades críticas, que es la suma de los cajones naranjados y rojos. En el mapa de calor de riesgo residual avance actual, tabla 22, se identifica que quedan 96 vulnerabilidades por cerrar, es decir, un avance del 26%, aunque la meta es del 98% como se puede ver en el mapa de calor de riesgo residual planeado tabla 23. Se identifica también, que de las 156 vulnerabilidades, a 42 de ellas, no se les va a dar tratamiento, ya que se acepta el riesgo por estar por debajo de la línea

amarilla, la cual demarca el apetito de riesgo. El 84% faltante en los riesgos inherentes, indica que todavía queda campo de investigación en los otros componentes del sistema para llegar a un estado ideal mostrado en la tabla 23, además y que nuestra contribución a la seguridad, ha sido acorde con el alcance de la investigación.

1.9.5 Avance del plan de riesgos

Se ha logrado cerrar el 26% de los riesgos, pero es necesario cerrar el 84% de los riesgos inherentes restantes de esta investigación que aún están fuera de nuestro apetito de riesgo, ya que desde la revisión de la arquitectura de seguridad y la línea base definida relacionada con los ETTUS (Alcance de este trabajo), no es posible generar su implementación. Esto se abordará en los trabajos futuros relacionados con esta investigación. Generando un nuevo ciclo del planear, hacer, verificar y un actuar dentro del proceso de seguridad, para lograr le mejoramiento continuo de la seguridad.

CONCLUSIONES

- Se deja planteada una metodología de evaluación del riesgo basado en los estándares más usados en la evaluación de riesgo tecnológico, su aplicación ayudó a identificar las amenazas del sistema, dejándolas documentadas en términos técnicos estándar.

- Para los Ettus encontramos vulnerabilidades no evidentes en su configuración por defecto, en la arquitectura del sistema y en el proceso que se debe realizar para su operación, como lo demostramos en el desarrollo de la evaluación de vulnerabilidades, esto a pesar que la búsqueda de vulnerabilidades llevada a cabo en páginas especializadas en el registro de vulnerabilidades no arrojaran resultados, la última búsqueda fue llevada a cabo el 5 de febrero de 2019.

- Con los controles aplicados dentro del plan de riesgo, hemos logrado cerrar el 26% del total de riesgos identificados dentro del alcance de esta investigación, dejando trazado un plan a seguir para lograr el estado ideal.

- Se deja documentada la recomendación de arquitectura de seguridad con su descripción y diseño gráfico, con los elementos necesarios para trabajar de manera funcional y segura. En principio, se aseguró la información para preservar su confidencialidad, se incorporó el concepto de alta disponibilidad y redundancia para asegurar la disponibilidad del servicio y se establecieron líneas base para definir una integridad en los dispositivos, abordando así los tres pilares de la seguridad informática.

RECOMENDACIONES

- Implementación de técnicas de seguridad informática para garantizar los principios de integridad, confidencialidad y disponibilidad de la Información a un sistema de radiolocalización híbrido. – Dirigido por GIDATI

- Implementación de los procesos de gestión de seguridad para un sistema de interceptación de señales ilegales.

- Diseño e implementación de centro de datos seguro para el almacenamiento y operación de información registrada por redes de sensores.

BIBLIOGRAFÍA

[1] C. J. E. Valentín Barral, Javier Rodas, José A. García-Naya, “A NOVEL , SCALABLE AND DISTRIBUTED SOFTWARE ARCHITECTURE FOR SOFTWARE-DEFINED RADIO WITH REMOTE INTERACTION Valent ´ ın Barral , Javier Rodas , Jos ´ ıa-Naya , Carlos J . Escudero University of A Coru ˜ na , Spain,” no. April, pp. 80–83, 2012.

[2] A. M. Wyglinski, D. P. Orofino, M. N. Ettus, and T. W. Rondeau, “Revolutionizing software defined radio: Case studies in hardware, software, and education,” *IEEE Commun. Mag.*, vol. 54, no. January, pp. 68–75, 2016.

[3] G. Berardinelli, J. L. Buthler, F. M. L. Tavares, O. Tonelli, D. A. Wassie, F. Hakhamaneshi, T. B. Sørensen, and P. Mogensen, “Distributed Synchronization of a testbed network with USRP N200 radio boards,” *Conf. Rec. - Asilomar Conf. Signals, Syst. Comput.*, vol. 2015-April, pp. 563–567, 2015.

[4] J. Mitola and G. Q. Maguire, “Cognitive radio: making software radios more personal,” *IEEE Pers. Commun.*, vol. 6, pp. 13–18, 1999.

[5] S. Bhattacharjee, S. Sengupta, and M. Chatterjee, “Vulnerabilities in cognitive radio networks: A survey,” *Comput. Commun.*, vol. 36, no. 13, pp. 1387–1398, 2013.

[6] Pmg-ssi, “No Title,” 2013. .

[7] Nist, “Guide for conducting risk assessments,” no. September, p. 95, 2012.

[8] Icontec, “NTC-ISO/IEC 27005,” no. 571, 2015.

[9] ICONTEC, “Information Technology Sevcurity Techniques Information Security Incident Management,” 2011.

[10] M. Heiderich, E. A. V. Nava, G. Heyes, D. Lindsay, M. Heiderich, E. A. V. Nava, G. Heyes, and D. Lindsay, “Chapter 8 – Web application firewalls and client-side filters,” *Web Appl. Obfuscation*, pp. 199–216, 2011.

[11] E. M. P. VILLARRAGA, “ANÁLISIS COMPARATIVO DE UN FIREWALL DE APLICACIONES WEB COMERCIAL Y UN OPEN SOURCE FRENTE AL TOP 10 DE OWASP,” 2016.

[12] H.-J. L. a, C.-H. R. L. a N, and Y.-C. L. a B, “Intrusion detection system: A comprehensive review,” *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, 2012.

[13] R. Wald, F. Villanustre, T. M. Khoshgoftaar, R. Zuech, J. Robinson, and E. Muharemagic, “Using Feature Selection and Classification to Build Effective and Efficient Firewalls,” pp. 850–854.

[14] V. R. Chandakanna and V. K. Vatsavayi, “A QoS-aware self-correcting observation based load balancer,” *J. Syst. Softw.*, vol. 115, pp. 111–129, 2016.

[15] S. Ali, M. H. Al Lawati, and S. J. Naqvi, “Unified threat management system approach for securing sme’s network infrastructure,” *Proc. - 9th IEEE Int. Conf. E-bus. Eng. ICEBE 2012*, pp. 170–176, 2012.
[16] V. F. Pérez, “Anteproyecto MaestríaV4.” .
[17] N. S. Report, “Nessus Report,” 2013.
[18] V. F. Pérez, “Informe de riesgo tecnológico,” pp. 1–90.

ANEXOS

Anteproyecto MaestríaV4.2[16]

Reporte de vulnerabilidades[17]

Informe de riesgos[18]