ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

Análisis y evaluación de protocolos de comunicación en sistemas de video vigilancia en zonas remotas para garantizar disponibilidad del servicio

ERICA PAULINA PADILLA UVIDIA

Trabajo de Titulación modalidad: Proyectos de Investigación y Desarrollo presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMATICA

Riobamba – Ecuador

ENERO – 2023

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado Análisis y evaluación de protocolos de comunicación en sistemas de video vigilancia en zonas remotas para garantizar disponibilidad del servicio, de responsabilidad de la señorita Erica Paulina Padilla Uvidia ha sido prolijamente revisado y se autoriza su presentación.

Dr. Juan Mario Vargas Guambo; Mag. _____

PRESIDENTE

Ing. Diego Fernando Veloz Cherrez; Mag. _____

DIRECTOR

Ing. Alberto Leopoldo Arellano Aucancela; Mag. _____

MIEMBRO

Ing. Danilo Mauricio Pastor Ramírez; Ph. D. _____

MIEMBRO

Riobamba, enero de 2023

DERECHOS INTELECTUALES

Yo, Erica Paulina Padilla Uvidia, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

_____

ERICA PAULINA PADILLA UVIDIA

060410718-5

DECLARACIÓN DE AUTENTICIDAD

Yo, Erica Paulina Padilla Uvidia, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autora, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

_____

ERICA PAULINA PADILLA UVIDIA

060410718-5

DEDICATORIA

Este trabajo lo dedico con mucho amor y cariño a mis padres y hermanos ya que me han brindado un apoyo incondicional para cumplir este sueño y me han impulsado con amor.

A mi esposo y mis hijas por ser esa fuente de inspiración y fuerza para seguir adelante, alcanzando éxitos y ser ejemplo para ellas.

A mis sobrinos por ser aquella muestra de inocencia y amor constante en mi existencia.

Erica

AGRADECIMIENTO

Agradezco primeramente a Dios por permitirme realizar este trabajo con el cual cumplo con una meta trazada en mi vida y cumplimos nuestro sueño más anhelado.

A mi familia por apoyarme constantemente y a los docentes que han brindado toda su ayuda en este camino.

Erica

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En el presente trabajo de titulación se realizó un análisis de protocolos de comunicación en sistemas de video vigilancia para zonas remotas que garanticen la disponibilidad del servicio de manera constante. Para realizar un análisis completo se utilizó la herramienta Nessus, en el cual se reflejan vulnerabilidades de red que comprometan a la disponibilidad del servicio, siendo comprobadas mediante OWASP como estándar de verificación con la aplicación de un ataque DDoS y Cobit5 como testeador de diseño de implementación. De igual forma, a más de analizar la cámara laser como componente principal, también se analizó los equipos de radiofrecuencia (RF), ya que por ser un ambiente remoto se utilizan enlaces RF de largo alcance; encontrando como hallazgos principales: claves por defecto, puertos habilitados, servicio de autodetección habilitada, disponibilidad de energía, evidenciando la necesidad de incrementar la seguridad perimetral. Por lo cual, se realizó un hardening al sistema de video vigilancia mediante un firewall opensource (OPNsense) para el filtrado de IP, mitigando principalmente la denegación de servicio. Adicionalmente con el trabajo conjunto del firewall y el monitoreo de video vigilancia al sistema eléctrico, se identificó fallos de disponibilidad de energía, que al mejorar el sistema de banco de baterías se logró incrementar la disponibilidad de funcionamiento al 95%. Concluyendo así que el uso de un firewall como seguridad perimetral más el trabajo conjunto con la video vigilancia, reducen las vulnerabilidades de funcionamiento ofreciendo así un incremento de 7,71% de disponibilidad. Se recomienda un aumento de respaldo al banco de batería, ya que este brinda más tiempo de funcionamiento para que el firewall detecte fallos y poder tener una respuesta inmediata sin dejar inactiva a la cámara laser.

Palabras clave: <PROTOCOLOS DE COMUNICACIÓN>, <SISTEMAS DE VIDEOVIGILANCIA>, <NESSUS (SOFTWARE)>, <EQUIPOS DE RADIOFRECUENCIA>, <HARDENING>.

SUMMARY

In this degree work, an analysis of communication protocols in video surveillance systems for remote areas that guarantee the availability of the service constantly was carried out. To perform a complete analysis, the Nessus tool was used, which reflects network vulnerabilities that compromise the availability of the service, being tested using OWASP as a verification standard with the application of a DDoS attack and Cobit5 as an implementation design tester. Similarly, in addition to analyzing the laser camera as the main component, the radio frequency (RF) equipment was also examined, since it is a remote environment and long-range RF links are used; the main findings were: default keys, enabled ports, enabled auto-detection service, power availability, evidencing the need to increase perimeter security. Therefore, the video surveillance system was hardened using an open-source firewall (OPNsense) for IP filtering, mainly mitigating denial of service. In addition, the joint work of the firewall and the video surveillance monitoring of the electrical system identified power availability failures, which increased operating availability by improving the battery bank system to 95%. This concludes that the use of a firewall as perimeter security plus the joint work with the video surveillance reduces the operating vulnerabilities, thus offering a 7.71% increase in availability. An increase of backup to the battery bank is recommended since it provides more operating time for the firewall to detect failures and have an immediate response without leaving the laser camera inactive.

Keywords: <COMMUNICATION PROTOCOLS>, < VIDEO SURVEILLANCE SYSTEMS>, <NESSUS (SOFTWARE)>, < RADIO FREQUENCY EQUIPMENT>, <HARDENING>.

CAPÍTULO I

1. INTRODUCCIÓN

1.1. Situación Problemática

Con la aparición de nuevas tecnologías el mundo de la seguridad electrónica ha tenido un progreso excesivo conforme a estos avances, donde encontramos que la mayoría de la seguridad electrónica está conectada a la red de internet, ahora llamado el internet de las cosas.

En enero de 2009, un equipo de investigadores de China estudió el incremento de estos dispositivos, donde determinan que estos duplicarán su número cada 5 años. (Evans, D. 2011)

Hoy en día en cada hogar tenemos por lo menos un dispositivo conectado a la red, y como calcular la cantidad de dispositivos en el mundo, si cada día este aumenta, gracias a los estudios y mediante cálculo podemos decir que en 2020 serian 50 mil millones de dispositivos conectados como son computadores, móviles, sistemas de video vigilancia, alarmas, sensores, dispositivos de red o cámaras IP. (Cisco IBSG, abril 2011)

Todo esto ha revolucionado el significado de la seguridad, ya que la tendencia actual en los negocios, apuesta la seguridad al uso de sistemas de video vigilancia apoyado de un monitoreo permanente. En la provincia del Guayas existe el mayor número de sistemas de vigilancia con cámaras de larga distancia, estas han ido desde infrarrojas hasta térmicas. Por ello el monitoreo funciona las 24 horas los 365 días del año, donde muchas empresas ponen todo el valor de sus producciones en manos de estos sistemas. Y es así como hoy en la actualidad la mayor parte del sector camaronero en la provincia de El Oro usa estas tecnologías como seguridad. (Villamar Chamba, G. P. 2018)

El sector camaronero se ha convertido en un punto principal para la economía del país, ya que somos el mayor exportador de camarón en el mundo, colocando así un alto valor a su producción, la cual se desarrolla directamente en el ámbito acuícola. El mismo que ha sido constantemente atacado principalmente por delincuentes marítimos o también llamados piratas, los cuales siempre se encuentran armados. Por esta razón ha disminuido radicalmente la seguridad personal, ya que se

perdían muchas vidas. Dando lugar a que la tecnología se encargue ahora de la seguridad en estos sectores alejados, pero de vital importancia. (Rodríguez Macías, W. H. 2017)

Cabe recalcar que el sector camaronero se encuentra en grandes extensiones de territorios, en ocasiones en islas, por lo que es imposible la presencia de la policía nacional.

Convirtiéndose así la video vigilancia como el sistema central de seguridad en camaroneras, donde este sistema debe tener una disponibilidad del 100% ya que todo el giro del negocio dependería de este, el uso de este sistema ha incrementado nuestra seguridad física pero no se ha analizado nuestra seguridad de software. En 2018 tuvo lugar el segundo ataque cibernético de denegación de servicios, el mismo que fue realizado mediante el malware Mirai del 2016 pero con un arsenal de herramientas actualizadas. (Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. 2017)

Mirai utilizó muchos dispositivos de la red mediante bootnets, de los cuales tomo el control mediante la aplicación de usuarios y contraseñas por defecto, ya que la mayoría eran cámaras ip, routers, equipos de red. El ataque fue dirigido hacia un servidor de DDNS, en donde reposaban dominios muy frecuentes como Amazon, Twitter, Spotyfy, Paypal, los cuales tuvieron muchas pérdidas. (Kambourakis, G., Kolias, C., & Stavrou, A. 2017).

De acuerdo al mercado actual existe una gran variedad de marcas de cámaras IP, donde Dahua, Hikvisión, Paradox, DSC, son empresas que se encargan de la seguridad electrónica, y han sido las más comercializadas en los últimos años, según el cuadrante de Garner del 2017 Hikvision es uno de los mejores sistemas de video vigilancia, pero la revista A&S la cual maneja los mejores rankings a nivel mundial coloco a Dahua dentro de los mejores 50 security 2019.

Estas empresas han ido innovando sus productos donde podemos encontrar desde dispositivos pequeños, hasta cámaras de largo alcance como por ejemplo las cámaras láser de 1.2 km, pues estas son dirigidas para grandes extensiones y ambientes externos.

1.2. Formulación del problema

¿La aplicación de diferentes protocolos de comunicación permitirá asegurar la disponibilidad del servicio de video vigilancia en áreas críticas que necesitan una cobertura amplia y de manera autónoma?

1.3. Justificación de la investigación

Como ya analizamos la seguridad en las cámaras como dispositivos IoT se han visto vulneradas constantemente, dejando un hueco de seguridad en toda la infraestructura de red, pues la cámara al encontrarse conectada a la red y no tener seguridad permite una conectividad con dispositivos adyacentes pues posterior al ataque de Mirai las empresas dedicadas a la seguridad electrónica empezaron a preocuparse por la seguridad de sus equipos al momento que se conectan a la red, por ello sus sistemas de interfaz tuvieron actualizaciones de firmware, ya que una de las mayores vulnerabilidades era permitir el funcionamiento de todo el sistema con las credenciales de fábrica. (Arcos, 2016)

Aun con este tipo de seguridad sus equipos siguen siendo vulnerables al momento que se encuentra en la red de internet, ya que por la acogida que han tenido las apps las empresas desarrollaron interfaces de fácil manejo que se conectan con servidores remotos, activando protocolos para que los usuarios puedan monitorear todo este sistema de seguridad electrónica por medio de dichas apps, como P2P, sin saber que se abre una puerta inmensa de acceso para los ciber atacantes. (Cybereason, 2018)

En marzo del 2019 Unit 42 un equipo de análisis de amenazas detecto que Mirai tiene nuevas variantes que incluyen 27 nuevos exploits para realizar ataques, en los cuales incluye ataques de fuerza bruta y que el payload malicioso se encuentra alojado en una empresa de seguridad electrónica en Colombia. Con esto podemos comprobar que, así como mejoran las empresas en su seguridad los ciber atacantes también evolucionan. (Harán, 2019)

Estos ataques no solo pueden tener como objetivo ingresar al sistema de video vigilancia y tener el control de dichos equipos, si no también tener como objetivo el ingreso al servidor o a información sensible de la empresa, como también realizar otro tipo de ataque como es el DDoS (ataque distribuido denegación de servicio) que significa que nos colisionará algún servicio en la red de la empresa, como lo menciona Harán estos ataques se están dirigiendo al sector empresarial.

Este ataque simplificaría totalmente la disponibilidad del servicio de video vigilancia, cuanto afectaría perder este servicio, Rodríguez demuestra que las pérdidas por delincuencia en el sector camaronero son muy representativas, las mismas que disminuyen con la implementación de sistemas de video vigilancia, pero que se podría mejorar en configuración e instalación para mantener la disponibilidad

del servicio. Por ello, la presente investigación se enfoca en el análisis de las herramientas, protocolos, estrategias que utilizan los cibernautas para realizar sus accesos a los sistemas de video vigilancia. (Rodriguez, 2017)

Dentro de los protocolos se analizará la comunicación de las cámaras. Como mencionamos por el giro del negocio hemos determinado las cámaras de largo alcance, un estudio revela los beneficios de usar cámaras térmicas para el sector camaronero, pero esta a su vez tiene un costo muy elevado, existiendo una alternativa presupuestaria como lo es las cámaras láser, las cuales tienen el mismo alcance, con un menor valor comercial. (Rodriguez, 2017)

En el ámbito laboral estas cámaras laser han brindado mejor respuesta gracias a su agilidad de movimiento y aceleración de zoom en el lente. Obteniendo mayor provecho en la continuidad del servicio de video vigilancia.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Analizar los diferentes protocolos de comunicación en sistemas de video vigilancia para zonas remotas que garanticen la disponibilidad del servicio.

1.4.2. Objetivos específicos

- Estudiar los principales protocolos de comunicación a nivel de la capa de aplicación en video vigilancia y su implicación en los diferentes tipos de ataques de cámaras laser para evitar vulnerabilidades en el sistema.
- Implementar un ambiente de video vigilancia para pruebas de similares características con protocolos estudiados para determinar cuál brinda mejor prestación.
- Diseñar la red de video vigilancia con cámaras laser en el sector camaronero e implementando las necesidades del sistema de video vigilancia acorde al análisis de vulnerabilidades realizado.

- Evaluar la disponibilidad del servicio del sistema de video vigilancia a través de la reducción de vulnerabilidades en el sistema reforzado.

1.5. Hipótesis

1.5.1. Hipótesis general

Ho: Al analizar los protocolos de comunicación en la transmisión de video vigilancia el uso de protocolos específicos garantiza la disponibilidad del servicio.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Introducción

El siguiente marco teórico nos ayudará a fundamentar nuestro proyecto, para las personas que no poseen ningún conocimiento sobre el mismo, teniendo así una idea clara para comprender el propósito, las necesidades y el impacto que nuestro estudio provocará.

2.2. Redes de Video vigilancia

A partir del 2013 apareció la necesidad de implementar los sistemas de video vigilancia como apoyo para maximizar la seguridad física en los diferentes establecimientos, sean empresas, condominios, fábricas, entre otros. Se creía que con este sistema se complementaría con seguridad de sensores y demás. Inicialmente estos sistemas eran en circuitos cerrados. Existe la elaboración de una metodología para añadir los sistemas de video vigilancia con otras tecnologías en la Universidad de San Carlos de Guatemala, basado únicamente en conexiones físicas. (Tomás & Ajanel, 2013)

Un Sistema de video vigilancia IP, no es más que el conjunto de dispositivos IP conectados a la red que interactúan entre sí. García mencionaba que un sistema de video vigilancia consistía en instalar cámaras sobre una red, las mismas que graban y esto es almacenado en un grabador digital, lo cual se puede mirar en tiempo real mediante un monitor. (Merchan Carreño & García Marcillo, 2021)

Una red de video vigilancia está compuesta de 3 elementos fundamentales: grabador, cámaras y elementos de conexión.

Figura 1-2: Video vigilancia IP

Fuente: Qloudea data solutions

2.2.1. Grabador IP

Equipo de grabación en red, para cámaras, estos difieren en el número de cámaras que soportan y la capacidad de memoria desde 1TB hasta 8TB, al igual que la velocidad de procesamiento. Como un ordenador posee dirección IP propias y está directamente conectado a la red. (Merchan Carreño & García Marcillo, 2021)

Figura 2-2: Grabador IP- NVR

Fuente: www.tecnoseguro.com

Las cámaras y grabadores de video incluyen varias funcionalidades extras como correo, conexión remota, conexión de alarmas, todo esto para centralizar una pequeña red de seguridad, así como también su propia interfaz gráfica.

2.2.2. Cámara IP

Una cámara de red, también llamada cámara IP, puede describirse como una cámara y un ordenador combinados para formar una única unidad. Los componentes principales que integran este tipo de cámaras de red incluyen una lente, un sensor de imagen, uno o más procesadores y memoria. (Todoelectronica, 2019)

Como un ordenador, la cámara de red dispone de su propia dirección IP, está directamente conectada a la red. Existe una variedad de cámaras, las clasificaremos por su alcance y funcionamiento.

Figura 3-2: Cámara IP

Fuente: Dahua Technology Co., Ltd, 2020

Por su funcionamiento las clasificaremos en fija y automatizadas.

2.2.2.1. Cámara Fija

Es aquella que una vez instalada se mantiene en esa posición, es decir no varía su ángulo de visualización. (© 2010-2022 Dahua Technology Co., Ltd, 2020)

2.2.2.2. Cámara Automatizada

Son aquellas que poseen un motor el cual puede ser programado por el usuario para que la cámara se mueve en el ángulo deseado durante el tiempo deseado. Dentro de esta clasificación varían según su manera de retroiluminación: cámaras térmicas y cámaras laser.

2.2.2.3. Cámara Térmica

Las cámaras térmicas crean imágenes a partir del calor que irradian siempre todos los objetos, vehículos o personas.

Las cámaras térmicas son menos susceptibles a las condiciones de luz complicadas, como sombras, retro iluminaciones e incluso objetos camuflados.

Figura 4-2: Cámaras Térmicas

Fuente: Dahua Technology Co., Ltd, 2020

2.2.2.4. Cámara Láser

Es una cámara de posicionamiento IP que cuenta con tecnología starlight y puede realizar zoom óptico de 45x. Incluye láser IR con distancia de desde 550m hasta 1.2km para visualización nocturna, auto tracking, funciones inteligentes.

Figura 5-2: Cámara Laser IP

Fuente: Dahua Technology Co., Ltd, 2020

Adicional posee la tecnología PFA (Algoritmo de Enfoque Predictivo), la cual ha introducido métodos para garantizar la precisión y la previsibilidad de la dirección del ajuste de la distancia sujeto. PFA garantiza la claridad de la imagen durante todo el proceso de acercamiento y acorta el tiempo de enfoque.

Las cámaras láser traen varios protocolos de los cuales podemos mencionar: IPv4/IPv6, HTTP, HTTPS, SSL, TCP/IP, UDP, UPnP, ICMP, IGMP, SNMP, RTSP, RTP, SMTP, NTP, DHCP, DNS, PPPOE, DDNS, FTP, IP Filter, QoS, Bonjour, 802.1x. Para su interoperabilidad traen los protocolos ONVIF, PSIA, CGI. (© 2010-2022 Dahua Technology Co., Ltd, 2020)

El protocolo ONVIF (Open Network Video Interface Forum) es un estándar de comunicación basado en los modelos IETF y Web Services, para la conexión entre productos de seguridad física basados en IP, como cámaras de video vigilancia y plataformas de gestión de vídeo. (revistaseguridad360, 2022)

El objetivo principal es facilitar la integración de diferentes marcas de equipos de video, estandarizando la comunicación entre ellos, pudiendo conectar de forma sencilla y casi automática los dispositivos. ONVIF en cámaras significa que el usuario tiene la posibilidad de seleccionar productos de vídeo en red, de diferentes fabricantes, con la seguridad de poder conectarlas entre ellas y así cubrir por completo sus necesidades.

De la misma forma, el estándar ONVIF significa que el usuario se asegura no estar sujeto a soluciones propietarias basadas en una tecnología de un fabricante individual ya que está abierto a todas las empresas y organizaciones. (Álvarez R, 2017)

2.3. Servicios e importancia

Hoy en día no solo se asegura el medio físico sino también la información, pero cabe recalcar que se comete muchos errores al momento de instalar un sistema de video vigilancia, ya que se considera solo el acceso físico, y no se asegura a nivel lógico a nuestro sistema, puesto que también es un blanco contra ataques cibernéticos.

Los sistemas de video vigilancia se han convertidos en los ojos de seguridad de las empresas, y más aún de las que se encuentran en zonas remotas como lo son las empresas acuícolas, ya que su ubicación dificultad la asistencia inmediata del servicio policial, se cuenta con el resguardo marítimo, pero este es escaso comparado con la presencia e incremento de la delincuencia.

Por ellos todos estos sistemas son transmitidos directamente hacia empresas especializadas en monitoreo 24/7, las mismas que deben mantener una comunicación constante y fluida, de allí nace la importancia de la disponibilidad de los sistemas de video vigilancia, ya que una desconexión del servicio podría significar pérdidas en el negocio.

2.4. Infraestructura de Red

Cuando hablamos de empresas acuícolas debemos entender que estamos refiriendo a grandes extensiones, por ello la utilización de cámaras de largo alcance facilita el manejo y optimiza el recubrimiento de toda la zona, en la actualidad la utilización de cámaras láser es la principal en el sector camaronero. (Andrango Marcillo, M. E. 2018).

Figura 6-2: Cámara en ubicación real

Elaborado por: Erica Padilla,2022

Ya que la ubicación es remota se utiliza enlaces inalámbricos para la comunicación entre la camaronera y el centro de monitoreo mediante la utilización de torres.

La utilización de su acceso remoto es primordial, donde para la visualización de nuestra cámara se lo realiza mediante su aplicativo web. Lamentablemente la industrialización de equipos de vigilancia en este caso cámaras se dirige específicamente a la visualización de imagen, a la compatibilidad de equipos y a su funcionalidad, pero dejan un amplio campo descubierto, la seguridad, la misma que se ha visto comprometida los últimos años.

Figura 7-2: Enlace Troncal

Elaborado por: Erica Padilla,2022

Cabe recalcar que las organizaciones o empresas no tienen mucho conocimiento de estos sucesos, donde existen varias maneras que un atacante logre acceder a la red, bajo diferentes modalidades como denegación de servicio o ataques a sesiones de usuarios para obtener un acceso no autorizado. Por ello es muy importante que todo el personal tenga conocimiento sobre la importancia de la seguridad informática, para mantener la disponibilidad del servicio.

Al mencionar monitoreo mediante video vigilancia nos dirigimos a transmisión video sobre la red, del cual dependerá toda la seguridad de nuestra empresa. Al transmitir video sobre la red este debe tener una fluidez potencial, por lo cual la calidad de servicio debe ser alta y sobre todo el servicio continuo.

La continuidad de un servicio es una de las características de la seguridad de la información para la protección de datos, la disponibilidad. Al depender la seguridad física de nuestro negocio de la transmisión de video vigilancia, la disponibilidad se convierte en el punto primordial de nuestra continuidad del negocio.

Los aplicativos webs hoy en día son los sitios con más problemas de seguridad, ya que no poseen controles que verifiquen la continuidad del servicio en la red. Naudi en su artículo nos revela que el 55% de sitios web y el 84% de aplicativos de internet presentan problemas de vulnerabilidades graves, y estas seguirán en aumento. Al ejecutarse estos ataques se está vulneran la disponibilidad de nuestro servicio.

2.5. Hacking Ético

2.5.1. Ataques

Los ataques cibernéticos tienen motivaciones económicas, sociales o políticas y se llevan a cabo principalmente a través de Internet. Los ataques son dirigidos al público en general, a organizaciones privadas o países. Se llevan a cabo mediante la difusión de programas maliciosos (virus), accesos web no autorizados, sitios web falsos y otros medios diseñados para robar información personal o institucional desde los blancos de ataques, lo que causa perjuicios muy graves. (Trend Micro Incorporate,2019)

Estos se basan en los protocolos TCP/IP, la comunicación entre sistemas que conforman una red permite el tráfico de datos en la misma, por lo cual se convierte en un punto de interés para los atacantes informáticos por el volumen de datos que se maneja y la parcialmente simplicidad que conlleva el acceso a la misma. (Juan P, 2017)

En el estudio de vulnerabilidades realizada para dispositivos IoT, se revela que el 54 % de conexiones atacantes o maliciosas son recibidas por los puertos de Telnet y Http, el 46% restante se encontraba en los demás puertos, lo que nos indica un mayor interés en cámaras IP para conexiones maliciosas, es decir son el blanco preferido de los atacantes, por ello se comprueba porque estos son los dispositivos usados para ataques de gran escala. (Tambe et al., 2019)

Entre los ataques más comunes que se dan al internet de las cosas es por la utilización de aplicativos web en los cuales tenemos acceso no autorizado y el DDOS, denegación de servicios. Un estudio dirigido a este tipo de ataque nos indica el aumento de este ataque a dispositivos IOT ya que su ingreso en el mercado está más enfocado a su funcionalidad, descuidando su seguridad, por ello han sido blanco de ataques a gran escala como Hakai y Reaper, este último no es más que el actualizado Mirai del 2016. (Tambe et al., 2019)

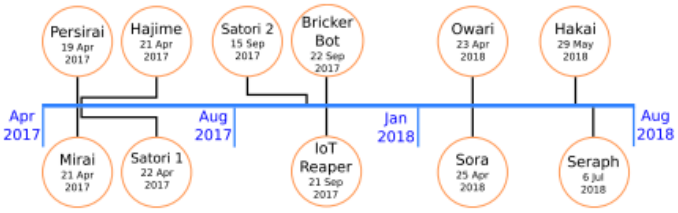

Figura 8-2: Ataques a través del tiempo

Fuente: Tambe, 2019

2.5.2. Prueba de penetración

Las pruebas de penetración o pruebas de "pen testing", cuenta con varias actividades de infraestructura de la cual se desea realizar dicho trest, por tal motivo que este proceso necesita identificar las vulnerabilidades que podrían materializarse más adelante, además de los daños que podría causar en la infraestructura tecnológica, ya sea por el atacante o por la penetración. El objetivo del proceso que se va a realizar es el identificar que incidentes de seguridad pueden darse antes de

que estos se materialicen y, posteriormente, corregir o mejorar el sistema, para garantizar la confidencialidad, integridad y disponibilidad de la información. (Miguel, 2017)

- Fase de reconocimiento: Se establece el objetivo y toda la información para lograr un ataque exitoso.
- Fase de escaneo: Aplicación de la información obtenida en la fase anterior para el primer escaneo de puertos y servicios.
- Fase de enumeración: Obtener información primordial como usuarios, contraseñas.
- Fase de acceso: Obtiene con claridad cada una de las vulnerabilidades.
- Fase de mantenimiento de acceso: Inserción de programas maliciosos para mantener el acceso para el atacante activo.

Herramientas para desarrollo de un test de penetración

- Kali Linux: Software libre
- Aplicaciones de Kali Linux
    - NESSUS: Herramienta de escaneo de vulnerabilidades.
    - Metasploit: Herramienta para ataques no autorizados.

2.5.3. Ethical Hacking

2.5.3.1. Fuerza Bruta

A los ataques de fuerza bruta también se le denomina ataque criptoanalítico, ya que los ataques de fuerza bruta se basan en funciones criptológicas para "descifrar" el cifrado e infiltrarse en la máquina. (ESGEEKS, s.f.)

2.5.3.2. Secuestro de Sesión

El secuestro de sesión, también conocido como *session hijacking*, es un problema importante que puede afectar a la seguridad de los usuarios a la hora de navegar por la red. Su función es lograr

acceso no autorizado a información o servicios en un sistema. Normalmente esto ocurre cuando un atacante roba o secuestra las cookies de sesión cuando un usuario navega por internet. (Jiménez, 2020)

2.5.3.3. Desbordamiento de Buffer

Ocurre cuando un programa intenta almacenar más datos en un área de almacenamiento temporal de los que puede contener. Escribir fuera del área de memoria asignada puede dañar los datos, bloquear el programa o provocar la ejecución de código malicioso que puede permitir que un atacante modifique el espacio de direcciones del proceso de destino. (Fabian, 2022)

2.5.3.4. Inyección SQL

Es un ataque que tiene como fin introducirse en la base de datos de un sitio web. Tiene diferentes finalidades como eliminar datos para provocar el caos y, en otras ocasiones, lo que buscan es editar la base de datos, especialmente en el caso de sitios web financieros. (Belcic, 2021)

2.5.4. Denegación de Servicios

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado. (Europol, 2018)

2.6. Defensas

2.6.1. Seguridad Informática

Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. (López, P. A. 2010).

Un sistema siempre se mantendrá bajo un margen de riesgos, para lo cual se debe constantemente considerar los elementos de sistema, los peligros que los afectan y las medidas de prevención, estos deben permanecer en contante actualización.

Un sistema seguro debe cumplir con las propiedades de integridad, confidencialidad y disponibilidad de la información.

La seguridad se divide en activa y pasiva, dependiendo de los elementos utilizados, así como también de la actuación que van a tener los mismos. (Alegre Ramos, M. D. P., & García-Cervigón Hurtado, A. 2011), teniendo en cuenta que su principal objetivo es proteger el sistema informático, información, equipos y usuarios.

- Activa. - Es toda aquella que usa medidas para detectar las amenazas, y en la existencia generan mecanismos adecuados para evitar problemas. Ejemplos: contraseñas, antivirus, firewall.
- Pasiva. - Es el conjunto de medidas usadas luego de un fallo o ataque para que el impacto producido sea menor y se reactiven las medias de recuperación del sistema. Ejemplo: copias de seguridad, uso de redundancia, uso de SAI.

Dentro de la norma ISO 27002 nos habla sobre los objetivos de la seguridad informática que es la preservación de la confidencialidad, integridad, disponibilidad y el No Repudio. (iso2700.es, 2019)

2.6.1.1. Integridad

Refiere a salvaguardar la información con precisión, es decir, la información enviada debe ser completa y sin errores.

2.6.1.2. Confidencialidad

Especifica que la información tendrá acceso únicamente la persona adecuada.

2.6.1.3. Disponibilidad

Indica que la información debe encontrarse disponible cuando el usuario lo requiera.

2.6.2. NIST – CSF

La NIST público en febrero del 2014 la CSF, "infraestructura de Seguridad Cibernética", convirtiéndose según Gartner en el marco más utilizado con un 30% de las empresas privadas y proyectado al 50% en el 2020.

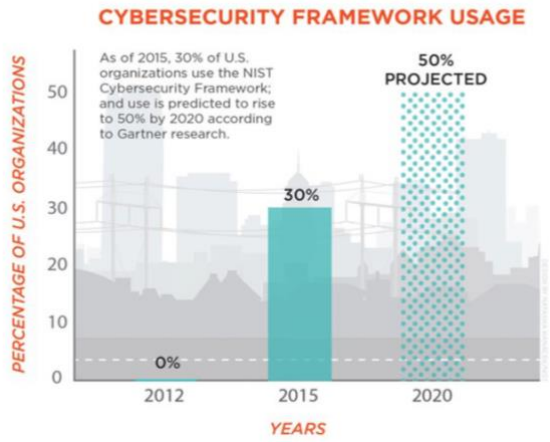

Figura 9-2: Crecimiento de dispositivos conectados a la red

Fuente: Hanacek, 2013

El CSF ofrece una estructura sencilla y efectiva en 3 elementos: núcleo, niveles y perfiles.

El núcleo hace referencia a los controles de seguridad de las normas adoptadas, entre ellas ISO 27001, NIST 800-53, COBIT (Objetivos de Control para la información y tecnología). (Hanacek, 2013)

En la práctica el núcleo apoya las 5 funciones de gestión de riesgos: Identificar, Proteger, Detectar, Responder y Recuperar.

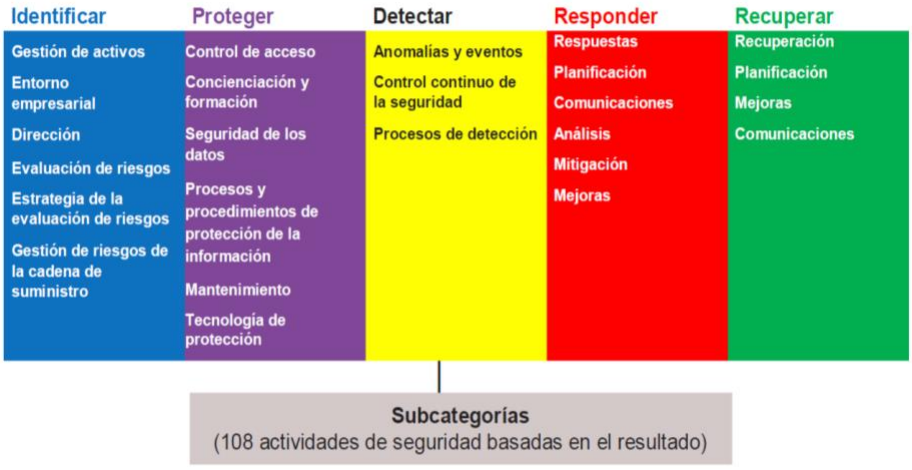

Figura 10-2: Funciones de Gestión de Riesgos

Fuente: AWS, 2021

2.6.2.1. COBIT 5

COBIT 5 provee un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. (ISACA, 2012)

Figura 11-2: Principios COBIT5

Fuente: ISACA, 2012

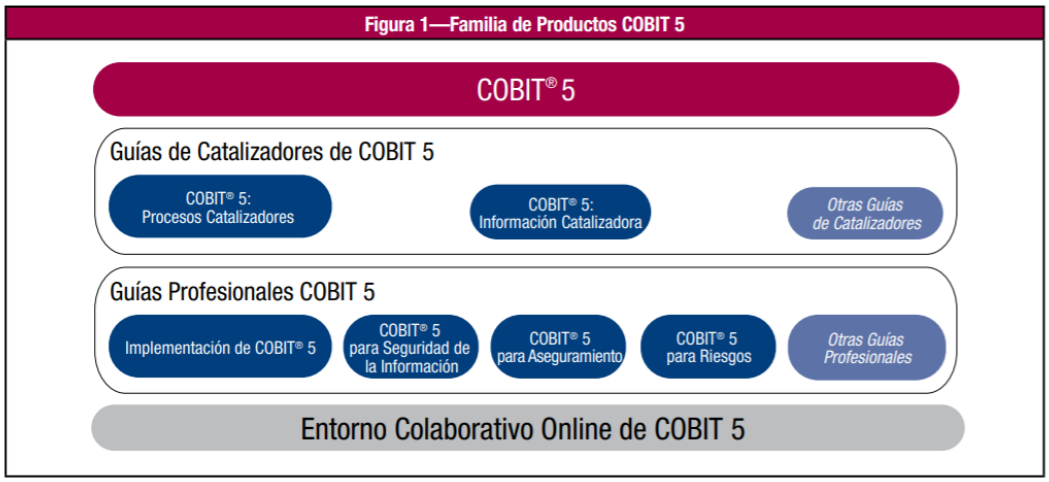

Figura 12-2: Productos COBIT5

Fuente: ISACA, 2012

El *Programa de Evaluación COBIT 5* incorpora el Modelo de Referencia de Proceso COBIT5 e ISO/IEC 15504 como base para el marco de medición y el proceso de evaluación.

- **Marco de Medición**

El proceso de evaluación en el uso de Cobit5 como vemos en la Figura 13-2 supone determinar una calificación de capacidades para un proceso, lo que comprende:

Nivel del proceso	Capacitación
0 (Incompleto)	El proceso no se encuentra implementado o falla en conseguir el objetivo del proceso. A este nivel, hay poca o ninguna evidencia de un proceso sistematizado para la consecución de los objetivos del proceso.
1 (Ejecutado)	Un proceso implementado consigue el propósito del proceso.
2 (Gestionado)	El proceso ejecutado ahora es implementado de forma gestionada (planificada, monitorizada y ajustada) y los resultados son adecuadamente establecidos, controlados y mantenidos.
3 (Establecido)	El proceso gestionado ahora es implementado utilizando un proceso definido que permite conseguir los resultados del proceso.
4 (Predecible)	Un proceso establecido, opera en los límites definidos, para a conseguir los resultados del proceso.
5 (Optimizado)	Un proceso predecible, es continuamente mejorado para alcanzar los objetivos del negocio actuales y futuras.

Figura 13-2: Niveles de capacitación de procesos

Fuente: ISACA, 2013

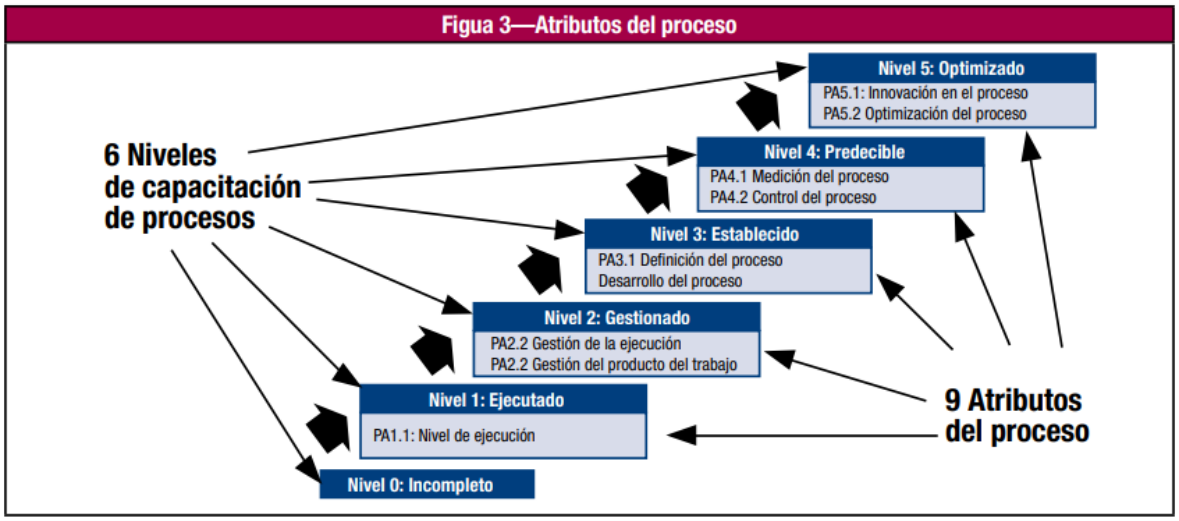

Figura 14-2: Atributos del proceso

Fuente: ISACA, 2013

- **Marco de implementación**

Dentro de Cobit5 tenemos el marco de referencia de implementación, a continuación, observamos en la figura 15-2 las fases de implementación.

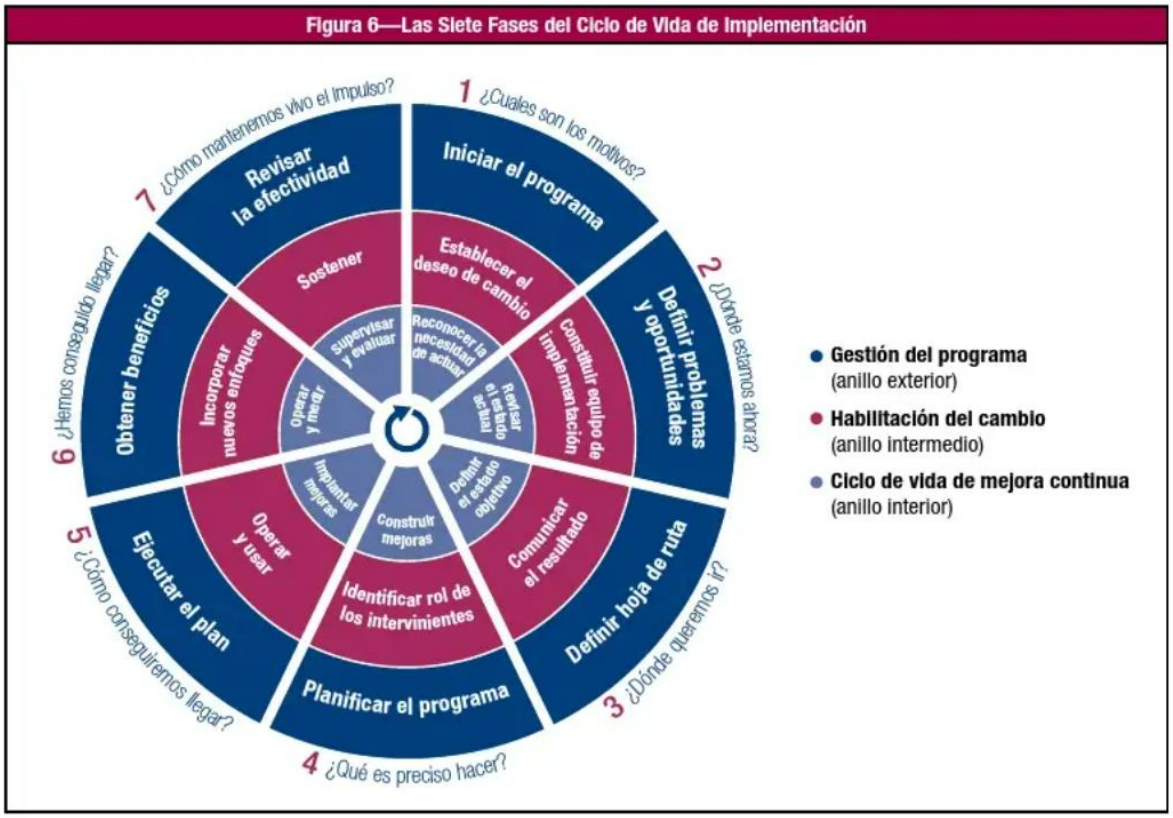

Figura 15-2: Fases de implementación Cobit5

Fuente: ISACA, 2012

2.6.2.2. OWASP para aplicaciones

OWASP está dirigido para 3 áreas de trabajo como: desarrollador de software, testador de software y especialista en seguridad cada una con características esenciales para su funcionamiento.

OWASP como estándar de verificación de seguridad en aplicaciones (ASVS) tiene dos objetivos principales

- Ayudar a las organizaciones en el desarrollo y mantenimiento de aplicaciones seguras.

- Permitir la alineación entre las necesidades y ofertas de los servicios de seguridad, proveedores de herramientas de seguridad y consumidores. (owasp.org, 2018)

El ASVS define 3 niveles de verificación de seguridad donde ASVS1 se dirige a todo tipo de software, ASVS2 es para apps que contienen datos sensibles, que requieren protección, y ASVS 3 es para apps más críticas que requieren el más alto nivel de confianza. (owasp.org, 2018)

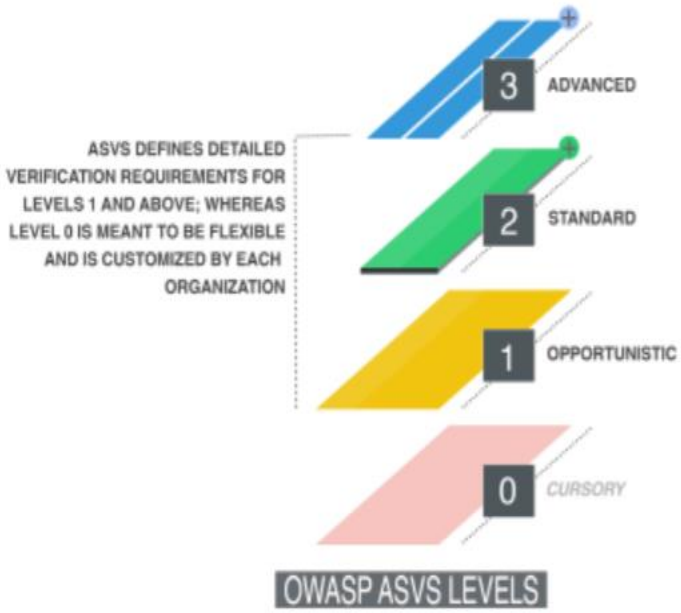

Figura 16-2: Niveles de Seguridad ASVS (OWASP, 2017)

Fuente: OWASP, 2017

ASVS se especifica para algunas industrias, ya que cada una tiene activos diferentes, únicos y valiosos bajo regulaciones y normativas específicas como lo mostraremos a continuación en la tabla.

Tabla 1-2: Estándar de verificación de seguridad en la practica

Industria	Perfil de amenaza	L1 Recomendación	L2 Recomendación	L3 Recomendación
Manufacturera, profesional, transporte, tecnología, utilidades, infraestructura y defensa	Estas industrias no parecen tener mucho en común, pero los agentes de amenaza que suelen atacar a las organizaciones en este segmento son más propensos a realizar ataques enfocados con más tiempo, habilidad y recursos. A menudo la información sensible o los sistemas no son fáciles de localizar y requieren utilizar o manipular individuos que trabajen dentro de la organización, utilizando técnicas de ingeniería social. Los ataques pueden involucrar individuos que trabajan dentro de la organización, extraños a la organización, o una combinación de ambos. Sus objetivos pueden incluir acceso a la propiedad intelectual para obtener ventajas estratégicas o tecnológicas. Tampoco queremos pasar por alto a los atacantes que buscan abusar la funcionalidad de la aplicación para influenciar el comportamiento de la aplicación o alterar sistemas sensibles. La mayoría de los atacantes buscan información sensible que puede ser utilizada directa o indirectamente para beneficiarse al incluir datos personales a la información de pago. A menudo los datos pueden utilizarse para una variedad de esquemas de fraude, robo de identidad o pagos fraudulentos.	Todas las aplicaciones accesibles desde la red.	Aplicaciones que contienen información interna o información sobre empleados que pueden aprovecharse utilizando la ingeniería social. Aplicaciones que contiene información poco esencial, pero de importante propiedad intelectual o secretos comerciales.	Aplicaciones que contiene valiosa propiedad intelectual, secretos comerciales o secretos del gobierno (p. ej. en los Estados Unidos esto puede ser cualquier cosa clasificados en secreto o superior) que es fundamental para la supervivencia o el éxito de la organización. Aplicaciones que controlan funcionalidad sensible (p. ej. transporte, fabricación de equipos, sistemas de control) o que tienen la posibilidad de amenazar la seguridad

Fuente: OWASP, 2017

Elaborado por: Erica Padilla, 2022

- **Requisitos para la verificación**

V1. Arquitectura, diseño y modelado

Tabla 2-2: Verificación de arquitectura, diseño y modelado

1.1	Verificar que todos los componentes de la aplicación se encuentran identificados y asegurar que son necesarios	
1.2	Verificar todos los componentes, tales como bibliotecas, módulos y sistemas externos, que no son parte de la aplicación pero que la misma los necesita para funcionar se han identificado.	
1.3	Verificar que se ha definido una arquitectura de alto nivel para la aplicación.	
1.4	Verificar que todos los componentes de la aplicación se definen de acuerdo con las funciones de negocio o de seguridad que proporcionan.	
1.5	Verificar que todos los componentes que no son parte de la aplicación pero que son necesarios para su funcionamiento, sean definidos de acuerdo con las funciones de negocio o de seguridad que proporcionan.	
1.6	Verificar que se ha realizado un modelo de amenazas para la aplicación en cuestión y que éste cubre riesgos asociados con la suplantación de identidad, manipulación, repudio, revelación de información y elevación de privilegios (STRIDE).	
1.7	Verificar que todos los controles de seguridad (incluyendo las bibliotecas que llaman a servicios de seguridad externos) tienen una implementación centralizada	
1.8	Verificar que los componentes están separados unos de otros mediante controles de seguridad, tales como segmentación de la red, reglas de firewall, o grupos de seguridad basados en la nube.	
1.9	Verificar que la aplicación tiene una clara separación entre la capa de datos, la capa de control y la capa de presentación, tal que las decisiones de seguridad pueden aplicarse en sistemas confiables.	
1.10	Verificar que no hay ninguna lógica de negocio sensible, claves secretas u otra información propietaria en el código del lado del cliente.	
1.11	Verificar que todos los componentes de la aplicación, bibliotecas, módulos, frameworks, plataformas y sistemas operativos se encuentran libres de vulnerabilidades conocidas	

Fuente: OWASP, 2017

V2. Autenticación

Tabla 3-2: Verificación de autenticación

2.1	Verificar que todas las páginas y recursos requieran autenticación excepto aquellos que sean específicamente destinados a ser públicos (Principio de mediación completa).	
2.2	Verificar que todos los campos de credenciales no reflejen las contraseñas del usuario. Cargar la credencial por parte de la aplicación implica que la misma fue almacenada de forma reversible o en texto plano, lo que se encuentra explícitamente prohibido.	
2.3	Verificar que todos los controles de autenticación se realicen del lado del servidor.	
2.4	Verificar que los controles de autenticación fallan de forma segura para evitar que los atacantes no puedan iniciar sesión.	
2.5	Verificar que los campos de contraseñas permiten o fomentan el uso de frases como contraseñas (passphrases) y no impiden el uso de gestores de contraseñas, contraseñas largas o altamente complejas.	
2.6	Verificar que toda función relacionada con la autenticación (como registro, actualización del perfil, olvido de nombre de usuario, recuperación de la contraseña, token perdido / deshabilitado, funciones de	

	help desk o IVR) que pueda ser utilizada de forma indirecta como mecanismo de autenticación, sea al menos tan resistente a ataques como el mecanismo primario.	
2.7	Verificar que la funcionalidad de cambio de contraseña solicite la contraseña anterior, la nueva contraseña y una confirmación de la contraseña.	
2.8	Verificar que todas las decisiones de autenticación son registradas en la bitácora sin almacenar información sobre la contraseña o el identificador de la sesión. Esto debería incluir los metadatos necesarios para investigaciones de seguridad.	
2.9	Verificar que las contraseñas de las cuentas se encuentren almacenadas utilizando una rutina de hashing con una sal, y que requiera un factor de trabajo lo suficientemente alto para evitar un ataque de fuerza bruta.	
2.10	Verificar que las credenciales son transportadas mediante un enlace cifrado adecuadamente y que todas las páginas/funciones que requieren que el usuario introduzca credenciales se realicen utilizando enlaces cifrados.	
2.11	Verificar que las funciones de recuperar contraseña y acceso no revelen la contraseña actual y que la nueva contraseña no se envíe en texto plano al usuario	
2.12	Verificar que no es posible enumerar información mediante las funcionalidades de: inicio de sesión, reinicio o recuperación contraseñas.	
2.13	Verificar que no se utilizan contraseñas por defecto en la aplicación o cualquiera de los componentes utilizados por la misma (como "admin/password").	
2.14	Verificar que existen mecanismos de anti-automatización que previenen la verificación de credenciales obtenidas de forma masiva, ataques de fuerza bruta y ataques de bloqueos de cuentas.	
2.15	Verificar que todas las credenciales de autenticación para acceder a servicios externos a la aplicación se encuentran cifradas y almacenadas en un lugar protegido	
2.16	Verificar que las funcionalidades de recuperar contraseña y otras formas de recuperar la cuenta utilizan mecanismos de TOTP (Time-Based One-Time Password) u otro tipo de soft token, push a dispositivo móvil u otro tipo de mecanismo de recuperación offline. El uso de un valor aleatorio en un correo electrónico o SMS debe ser la última opción ya que son conocidas sus debilidades.	
2.17	Verificar que el bloqueo de la cuenta se divida en estado de bloqueo suave y duro, y éstas no son mutuamente excluyentes. Si una cuenta está temporalmente bloqueada de forma suave debido a un ataque de fuerza bruta, esto no debe restablecer el bloqueo de estado duro.	
2.18	Verificar que si la aplicación hace uso de conocimiento basado en preguntas (también conocido como "secreto"), las preguntas no violan leyes de privacidad y son lo suficientemente fuertes para proteger la cuenta de recuperaciones maliciosas.	
2.19	Verificar que el sistema puede configurarse para no permitir el uso de un número de contraseñas utilizadas anteriormente.	
2.20	Verificar que la re-autenticación basada en riesgo, autenticación de dos factores o firma de transacciones se encuentra implementada en los lugares adecuados.	
2.21	Verificar que existen medidas para bloquear el uso de contraseñas comúnmente utilizadas y contraseñas débiles.	
2.22	Verificar que todos los desafíos de autenticación, ya sea exitosa o fallida, responden en el mismo tiempo promedio	
2.23	Verificar que secretos, llaves de API y contraseñas no se incluyen en el código fuente o en los repositorios en línea de código fuente.	
2.24	Verificar que, si una aplicación permite a los usuarios autenticarse, puedan hacerlo mediante autenticación de dos factores u otra autenticación fuerte, o cualquier esquema similar que proporcione protección contra la divulgación de nombres de usuario y contraseñas	
2.25	Verificar que las interfaces administrativas de la aplicación no sean accesibles a intrusos.	
2.26	Autocompletar de navegadores e integración con gestores de contraseñas deben estar permitidos a no ser que se encuentren prohibidos por políticas de riesgos.	

Fuente: OWASP, 2017

V3. Gestión de Sesiones

Tabla 4-2: Verificación de gestión de sesiones

3.1	Verificar que no se utiliza un gestor de sesiones personalizado, o que, si el gestor de sesiones es personalizado, éste sea resistente contra los ataques más comunes.	
3.2	Verificar que las sesiones se invalidan cuando el usuario cierra la sesión.	
3.3	Verificar que las sesiones se invalidan luego de un período determinado de inactividad.	
3.4	Verificar que las sesiones se invalidan luego de un período determinado de tiempo, independientemente de que se esté registrando actividad (timeout absoluto).	
3.5	Verificar que todas las páginas que requieren autenticación poseen acceso fácil y visible a la funcionalidad de cierre de sesión.	
3.6	Verificar que el identificador de sesión nunca se revele en URLs, mensajes de error o registros de bitácora. Esto incluye verificar que la aplicación no es compatible con la re-escritura de URL incluyendo el identificador de sesión.	
3.7	Verificar que toda autenticación exitosa y re-autenticaciones generen un nuevo identificador de sesión.	
3.10	Verificar que sólo los identificadores de sesión generados por la aplicación son reconocidos como activos por ésta.	
3.11	Verificar que los identificadores de sesión son suficientemente largos, aleatorios y únicos para las sesiones activas.	
3.12	Verificar que los identificadores de sesión almacenados en cookies poseen su atributo “path” establecido en un valor adecuadamente restrictivo y que además contenga los atributos "Secure" y "HttpOnly"	
3.16	Verificar que la aplicación limita el número de sesiones concurrentes activas.	
3.17	Verificar que una lista de sesiones activas esté disponible en el perfil de cuenta o similar para cada usuario. El usuario debe ser capaz de terminar cualquier sesión activa.	
3.18	Verificar que al usuario se le sugiera la opción de terminar todas las otras sesiones activas después de un proceso de cambio de contraseña exitoso.	

Fuente: OWASP, 2017

V4. Control de acceso

Tabla 5-2: Verificación de control de acceso

4.1	Verificar que existe el principio de privilegio mínimo - los usuarios sólo deben ser capaces de acceder a las funciones, archivos de datos, URL, controladores, servicios y otros recursos, para los cuales poseen una autorización específica. Esto implica protección contra suplantación de identidad y elevación de privilegios	
4.4	Verificar que el acceso a registros sensibles esté protegido, tal que sólo objetos autorizados o datos sean accesibles por cada usuario (por ejemplo, proteger contra la posible manipulación hecha por usuarios sobre un parámetro para ver o modificar la cuenta de otro usuario).	

Fuente: OWASP, 2017

V5. Manejo de entrada de datos maliciosos

Tabla 6-2: Verificación de manejo de entrada de datos maliciosos

5.1	Verificar que el entorno de ejecución no es susceptible a desbordamientos de búfer, o que los controles de seguridad previenen desbordamientos de búfer.	
5.3	Verificar que las fallas de validación de entradas de datos del lado del servidor sean rechazadas y registradas.	
5.5	Verificar que se aplican las rutinas de validación de entradas de datos del lado del servidor.	
5.6	Verificar que un único control de validación de entrada es utilizado por la aplicación para cada tipo de datos que es aceptado.	
5.10	Verificar que todas las consultas de SQL, HQL, OSQL, NOSQL y procedimientos almacenados, llamadas de procedimientos almacenados están protegidos por la utilización de declaraciones preparadas o parametrización de consultas, y por lo tanto no sean susceptibles a la inyección de SQL	
5.11	Verificar que la aplicación no es susceptible a la inyección LDAP, o que los controles de seguridad previenen inyección LDAP.	
5.12	Verificar que la aplicación no es susceptible a la inyección de comandos del sistema operativo, o que los controles de seguridad previenen la inyección de comandos del sistema operativo	
5.13	Verificar que la aplicación no es susceptible a la inclusión de archivo remoto (RFI) o inclusión de archivo Local (LFI) cuando el contenido es utilizado como una ruta a un archivo.	
5.14	Verificar que la aplicación no es susceptible a ataques comunes de XML, como manipulación de consultas XPath, ataques de entidad externa XML, y ataques de inyección XML.	
5.15	Asegurar que todas las variables string utilizadas dentro de HTML u otro lenguaje web interpretado en cliente se encuentra apropiadamente codificada manualmente o se utiliza plantillas que automáticamente codifican contextualmente para asegurar que la aplicación no sea susceptible a ataques DOM Cross-Site Scripting (XSS).	
5.16	Si el framework de la aplicación permite asignación automática de parámetros en masa (también llamada enlace automático de variables o variable biding) desde la petición entrante a un modelo, verificar que campos sensibles de seguridad como "*accountBalance*", "*role*" o "password" sean protegidos de enlaces automáticos maliciosos.	
5.17	Verificar que la aplicación contenga defensas contra los ataques de contaminación de parámetros HTTP (agregar parámetros a la URL), particularmente si el framework de la aplicación no hace distinción sobre el origen de los parámetros de la petición (GET, POST, cookies, cabeceras, ambiente, etc.)	
5.18	Verificar que las validaciones del lado del cliente se utilizan como una segunda línea de defensa, en adición a la validación del lado del servidor.	
5.19	Verificar que todos los datos de entrada sean validados, no solamente los campos de formularios HTML sino también todos los orígenes de entrada como las llamadas REST, parámetros de consulta, encabezados HTTP, cookies, archivos por lotes, fuentes RSS, etc.; mediante validación positiva (lista blanca), o utilizando otras formas de validación menos eficaces tales como listas de rechazo transitorio (eliminando símbolos defectuosos), o rechazando malas entradas (listas negras).	
5.20	Verificar que datos estructurados fuertemente tipados son validados un esquema definido incluyendo; caracteres permitidos, longitud y patrones (p. ej. tarjeta de crédito o teléfono o validando que dos campos relacionados son razonables, tales como validación de coincidencia entre localidad y código postal)	
5.21	Verificar que los datos no estructurados sean sanitizados cumpliendo medidas genéricas de seguridad tales como caracteres permitidos, longitud y que caracteres potencialmente dañinos en cierto contexto sean anulados (p. ej. nombres naturales con Unicode o apóstrofos, como ねこ o O'Hara)	

5.22	Verificar que HTML no confiable proveniente de editores WYSIWYG o similares sean debidamente sanitizados con un sanitizador de HTML y se manejen apropiadamente según la validación de entrada y codificación	
5.23	Para tecnologías de plantilla de codificación automática, si ésta se ha deshabilitado, asegurar que la sanitización de HTML esté habilitada en su lugar.	
5.24	Verificar que los datos transferidos desde un contexto DOM a otro, utilice métodos de JavaScript seguro, como pueden ser .innerText y .val	
5.25	Verificar que cuando se interprete JSON en navegadores, que JSON.parse sea el utilizado para interpretarlo y no eval().	
5.26	Verificar que los datos de autenticación se eliminen del almacenamiento del cliente, tales como el DOM del navegador, después de terminada la sesión.	
5.21	Verificar que los datos no estructurados sean sanitizados cumpliendo medidas genéricas de seguridad tales como caracteres permitidos, longitud y que caracteres potencialmente dañinos en cierto contexto sean anulados (p. ej. nombres naturales con Unicode o apóstrofos, como ねこ o O'Hara)	
5.22	Verificar que HTML no confiable proveniente de editores WYSIWYG o similares sean debidamente sanitizados con un sanitizador de HTML y se manejen apropiadamente según la validación de entrada y codificación	
5.23	Para tecnologías de plantilla de codificación automática, si ésta se ha deshabilitado, asegurar que la sanitización de HTML esté habilitada en su lugar.	
5.24	Verificar que los datos transferidos desde un contexto DOM a otro, utilice métodos de JavaScript seguro, como pueden ser .innerText y .val	
5.25	Verificar que cuando se interprete JSON en navegadores, que JSON.parse sea el utilizado para interpretarlo y no eval().	
5.26	Verificar que los datos de autenticación se eliminen del almacenamiento del cliente, tales como el DOM del navegador, después de terminada la sesión.	

Fuente: OWASP, 2017

V11. Requisitos de verificación de configuración de seguridad HTTP

Tabla 7-2: Requisitos de verificación de configuración de seguridad HTTP

11.1	Verificar que la aplicación acepte solo un conjunto definido de métodos de solicitud HTTP y que son necesarios, como GET y POST, y métodos no utilizados (por ejemplo: TRACE, PUT y DELETE) se encuentran explícitamente bloqueados.	
11.2	Verificar que cada respuesta HTTP contenga una cabecera content-type en la que se especifique un conjunto utilizando un conjunto de caracteres seguros (Ejemplo: UTF-8, ISO 8859-1).	
11.3	Verificar que los encabezados HTTP agregados por un proxy confiable o dispositivos SSO, tales como un token de portador (bearer), son autenticados por la aplicación.	
11.4	Verificar que el cabezal X-FRAME-OPTIONS se encuentra 11.1especificado para los sitios que no deben ser embebidos en X-Frame en sitios de terceros	
11.5	Verificar que los encabezados HTTP o cualquier parte de la respuesta HTTP no expongan información detallada de la versión de los componentes del sistema.	
11.6	Verificar que todas las respuestas del API contienen opciones X-Content-Type: nosniff y Content-Disposition: attachment; filename="api.json" (u otro nombre de archivo apropiado para el tipo de contenido).	
11.7	Verificar que la política de seguridad de contenido (CSPv2) está en uso de tal manera que ayude a mitigar vulnerabilidades de inyección comunes de DOM, XSS, JSON y Javascript	
11.8	Verificar que el encabezado "X-XSS-Protection: 1; mode=block" esté presente para habilitar a los navegadores a filtrar XSS reflejados	

Fuente: OWASP, 2017

V15. Lógica del negocio

Tabla 8-2: Lógica del negocio

15.1	Verificar que la aplicación sólo procese flujos lógicos de negocios en orden secuencial, con todos los pasos procesados en tiempo humano realista, y no procesados fuera de orden, con pasos salteados, con pasos del proceso de otro usuario, o de transacciones muy rápidamente enviadas.	
15.2	Verificar que la aplicación tiene límites de negocio y los aplique correctamente por cada usuario, con alertas configurables y reacciones automatizadas ante ataques inusuales o automáticos.	

Fuente: OWASP, 2017

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. Introducción

Para el desarrollo del proyecto nos enfocaremos al área de actividad camaronera, la cual requiere de un servicio continuo de seguridad bajo vigilancia remota con cámaras láser. Se realizará de forma descriptivo explicativo para conocer los procesos y estructuras frente a la seguridad de nuestro sistema de video vigilancia. Se establecerá el uso de procedimientos mediante el uso de metodologías, por lo cual he decidido usar varias metodologías una de aplicación como OWASP y una de gestión como COBIT 5 para la implementación.

3.2. Tipo y diseño de la investigación

Este proyecto se basa en la investigación y la experimentación de procesos, por lo cual comprenderá diferentes métodos y técnicas para fundamentar las bases teóricas y analizar los resultados.

3.3. Método de investigación

Tabla 1-3: Metodología de investigación

OBJETIVOS	MÉTODO	DESCRIPCIÓN	TÉCNICA
Estudiar los principales protocolos de comunicación a nivel de la capa de aplicación en video vigilancia y su implicación en los diferentes tipos de ataques	Inductivo, deductivo	Mediante este método inductivo se observa, estudia y conoce como actúan los protocolos de transmisión dentro de nuestra cámara IP. Allí aplicaremos el método deductivo para determinar las características generales de los	Será fundamental para analizar la bibliografía adquirida y de ella inducir y concluir.

de cámaras laser para evitar vulnerabilidades en el sistema.		protocolos hacia lo particular que serían las cámaras IP.	
Implementar un ambiente de video vigilancia para pruebas de similares características con protocolos estudiados para determinar cuál brinda mejor prestación.	Científico descriptivo	Los estudios exploratorios en el ambiente de video vigilancia para zonas remotas nos ayudan a familiarizarnos con los eventos desconocidos, para así poder obtener información sobre las características de red de nuestra cámara laser.	recolección de información.
	Experimental	Este consiste en la realización de pruebas controladas hacia el sistema referencial para entender los procesos causales de ataques a la red de video vigilancia.	En este proceso se realiza las pruebas en nuestro sistema.
Diseñar la red de video vigilancia con cámaras laser en el sector camaronero e implementando las necesidades del sistema de video vigilancia acorde al análisis de vulnerabilidades realizado.	Analítico	Luego de realizar todo el análisis de vulnerabilidades que comprometan la disponibilidad de la cámara laser aplicaremos este método para distinguir todas las necesidades de nuestro sistema de video vigilancia.	Con ello descomponemos nuestra seguridad en física y lógica que involucran todas las partes del sistema analizado.
Evaluar la disponibilidad del servicio del sistema de video vigilancia a través de la reducción de vulnerabilidades en el sistema reforzado.	Estadístico	Consiste en una secuencia de procedimientos para el manejo de los datos cualitativos y cuantitativos de la investigación	Representará los resultados hallados.

Elaborado por: Erica Padilla, 2022

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Fase 1. Iniciar el programa

El motivo principal de este proyecto será explorar, donde se aplicará la seguridad en sistemas de video vigilancia, un tema de poco conocimiento en un ambiente de gran relevancia por el giro del negocio, en nuestro caso la disponibilidad o continuidad del servicio.

Nuestro sistema de video vigilancia se basa en un sistema de monitoreo a equipos mediante un aplicativo web, en nuestro caso el principal monitoreo es el de la cámara laser. Por ello debemos estudiar como transmite este, que protocolos utiliza y como mejorar su seguridad.

4.1.1. Actividad 1. Estudio de Protocolos de transmisión

Estudiaremos los protocolos que nuestra cámara laser tiene disponibles dentro de su configuración, los cuales detallaremos a continuación.

- *FTP*

  Es un protocolo de comunicación de la capa de aplicación, que permite transferir archivos como imágenes o videos de una cámara IP a una aplicación. Este funciona con control de acceso, es decir, bajo usuario y contraseña.

- *SMTP*

  Este protocolo se utiliza para el envío de emails. Este protocolo trabaja con las cámaras IP para añadir imágenes adjuntas en los correos o notificaciones de alerta.

- *HTTP*

  Hyper Transfer Protocol es un protocolo de transferencia de información entre diferentes servicios mediante páginas web. En las cámaras IP este trabaja enviando el video desde el dispositivo.

- *HTTPS*

  Este protocolo de transferencia segura en Internet usa encriptación para su transmisión. Las cámaras IP utilizan este protocolo para la transmisión de video desde el dispositivo usando certificados digitales.

  Por supuesto la primera ventaja de este nuevo protocolo es la seguridad para el usuario, especialmente en una sociedad donde las compras online, transferencias de dinero y operaciones bancaria son cada vez más comunes. Ofrecer HTTPS garantiza 100% autenticación del usuario, se evitan futuras suplantaciones, spammers y fuga de archivos confidenciales. Asegurando la confidencialidad, pero no la disponibilidad.

- *RTSP*

  Es un protocolo de transmisión de video o audio a través de UDP o TCP con el cual tenemos el control remoto de cualquier dispositivo que tenga esta disponibilidad.

- *UPnP*

  UPnP intentará reenviar puertos en su enrutador o módem de manera automática. Esto podría ser muy bueno si hablamos de velocidad de conexión. Sin embargo, si el deja credenciales predeterminadas y reenvía automáticamente los puertos dejamos un hueco de seguridad, facilitando el ingreso de visitantes no deseados. Si reenvió manualmente los puertos HTTP y TCP en su enrutador / módem, esta función debe desactivarse independientemente. Se recomienda deshabilitar UPnP cuando la función no se usa en aplicaciones reales.

- *IP FILTER*

  El componente de filtrado IP de las reglas de paquetes le permite controlar qué tráfico IP desea permitir que entre y salga de la red de su empresa. Se utiliza este protocolo como ayuda a nivel de protección para el filtrado de paquetes.

El filtrado de paquetes se realiza bajo la aplicación de una regla específica, que en realidad lleva a cabo una acción determinada.

- PERMIT — permite que el paquete procese como de costumbre
- DENY — descarta inmediatamente el paquete
- IPSEC — envía el paquete mediante una conexión de red privada virtual (VPN), que usted especifica en la regla de filtro

Después de aplicar una regla, el sistema reanuda la comparación secuencial de reglas y paquetes y asigna acciones a todas las reglas correspondientes. Si no encuentra una regla coincidente para un paquete concreto, el sistema lo descarta de forma automática. La regla de denegación por omisión del sistema garantiza que el sistema descartará de manera automática cualquier paquete que no coincida con una regla de filtro. Recuerde que, si se designa una regla de filtro para permitir el tráfico en solo una dirección, como la de entrada o salida, el sistema implementa la regla de denegación por omisión en ambas direcciones; es decir, se descartan tanto el paquete de entrada como el de salida. (IBM, 2021)

A nivel de cámaras este protocolo permite filtrar los paquetes autorizados de una dirección IP, es decir registramos que dirección será la única en acceder a nuestra cámara.

Luego del análisis de todos los protocolos que soporta la cámara podemos concluir que poseen seguridad de encriptación de datos para una conexión segura, pero estos ayudan a su disponibilidad mas no la prevalecen. Por ello debemos realizar un análisis a nuestro aplicativo web.

4.2. Fase 2. Definición de problemas y oportunidades

Consiste en el análisis de la situación actual de nuestro sistema de video vigilancia con cámaras laser, para entender la importancia de la seguridad para la detección y corrección de ataques a nuestras cámaras láser.

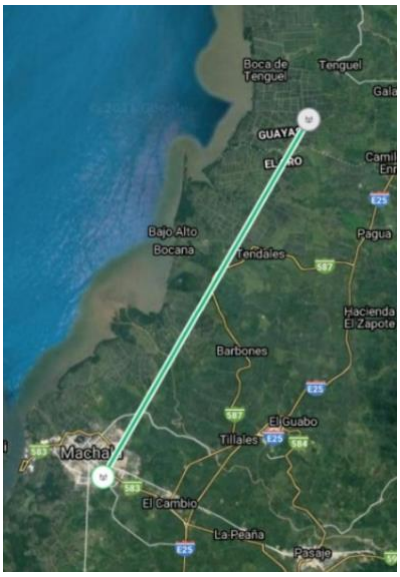

Figura 1-4: Enlace Troncal

Elaborado por: Erica Padilla, 2022

4.2.1. Actividad 1. Analizamos la ubicación de nuestro sistema, como acceso físico, abastecimiento de energía, movilidad, y estructura del sistema.

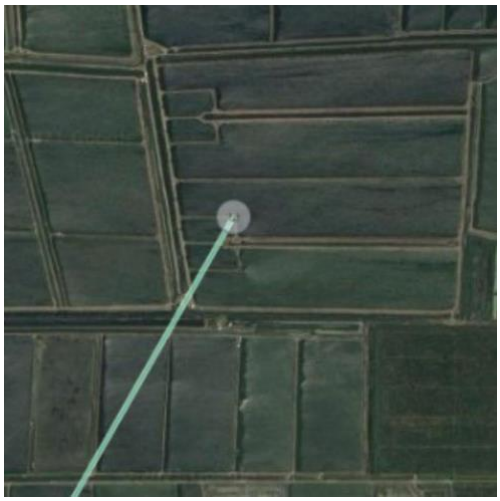

Figura 2-4: Ubicación Geográfica Cámara Laser

Elaborado por: Erica Padilla, 2022

- **Acceso Físico**. - El acceso es mediante vía terrestre, el mismo que tiene un nivel de dificultad elevado ya que existen varias camaroneras aledañas y hacen una visualización confusa de la ubicación.
- **Abastecimiento de Energía**. - Este sistema está basado en un sistema de retroalimentación gracias al uso de baterías y un inversor.

Figura 3-4: Sistema de conexión eléctrica

Elaborado por: Erica Padilla, 2022

Tabla 1-4:10 Equipos Eléctricos

Equipos del sistema		
Cantidad	**Equipo**	**Características**
2	Baterías de gel	170 amp/hora
1	Inversor	24 voltios /110vol
2	Paneles	Depende ubicación
2	controladores	
1	Regulador	

Elaborado por: Erica Padilla, 2022

- **Movilidad.-** La estructura geográfica del negocio nos da como resultado un camino estrecho para la movilización, por ello es que la misma se la realiza caminando, o mediante transporte de 2 ruedas. Esto nos conlleva a una demora en detección y movilización dentro de la camaronera.
- **Estructura de Sistema.-** El sistema de video vigilancia está conformado por su red interna, el mismo que se transmite mediante un enlace hacia la sala de monitoreo como lo podemos observar. Adicional detallaremos los equipos.

Tabla 2-4: Equipos de Enlace de Red

Equipos del sistema		
Cantidad	**Equipo**	**Características**
2	Airfiber HD	5 GHz, Ganancia: 23dbi
1	Cámara PTZ laser	Alcance 1200m
1	Torre	42 metros

Elaborado por: Erica Padilla, 2022

Como podemos observar por la ubicación de nuestra cámara laser, al tener un medio de comunicación de radiofrecuencia de largo alcance, y la rapidez de la movilidad interna es nula debemos centrarnos en el manejo sobre acceso remoto.

Figura 4-4: Estudio del Radio Enlace

Elaborado por: Erica Padilla, 2022

4.2.2. Actividad 2. Diseño de ambiente de pruebas

Se diseña un ambiente de prueba de similares características al sistema de video vigilancia real.

Para la elaboración de nuestro sistema de pruebas hemos decidido trabajar con una cámara de menor tamaño, ya sea para su manejo y accesibilidad. Puesto que por la ubicación y costo de nuestra cámara laser la accesibilidad se convierte en un punto de dificultad.

Tabla 3-4: Características de Red, cámaras.

CÁMARA LÁSER		CÁMARA DE PRUEBAS	
Ethernet Smart Phone IOS, Android	RJ-45 (10Base-T/100Base-TX)	Ethernet	RJ-45 (10XBase-T/100Base-TX)
Protocolo	IPv4/IPv6, HTTP, HTTPS, SSL, TCP/IP, UDP, UPnP, ICMP, IGMP, SNMP, RTSP, RTP, SMTP, NTP, DHCP, DNS, PPPOE, DDNS, FTP, IP Filter, QoS, Bonjour,802.1x	Protocolo	IPv4/IPv6, HTTP, HTTPS, SSL, TCP/IP, UDP, UPnP, ICMP, IGMP, SNMP, RTSP, RTP, SMTP, NTP, DHCP, DNS, PPPOE, DDNS, FTP, IP Filter, QoS, Bonjour, 802.1x
Streaming Method	Unicast / Multicast	Método de streaming	Unicast / Multicast
Interoperabilidad	ONVIF, PSIA, CGI	Interoperabilidad	ONVIF Profile S&G, API
Edge Storage	NAS (Network Attached Storage), Local PC for instant recording, Micro SD card 128GB	Edge Storage	NAS (Network Attached Storage), Local PC for instant recording, Micro SD card 128GB
Web Viewer	IE, Chrome, Firefox, Safari	Web Viewer	IE, Chrome, Firefox, Safari
Management Software	Smart PSS, DSS	Management Software	Smart PSS, DSS, DMSS
Smart Phone	IOS, Android	Smart Phone	IOS, Android
			

Elaborado por: Erica Padilla, 2022

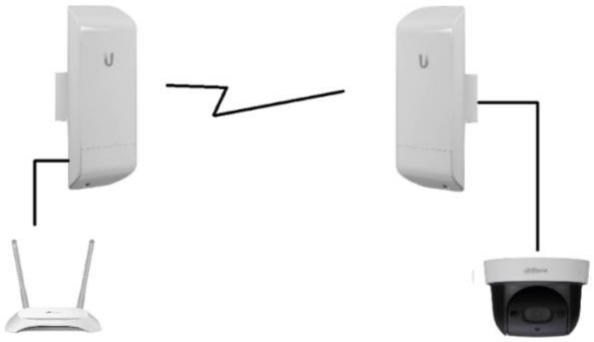

Figura 5-4: Ambiente de Pruebas

Elaborado por: Erica Padilla, 2022

4.2.3. Actividad 3. Medición de vulnerabilidades mediante la herramienta NESSUS.

Dentro de nuestro análisis mediante la herramienta NESSUS hemos obtenido 22 vulnerabilidades, las cuales las detallare y clasificare.

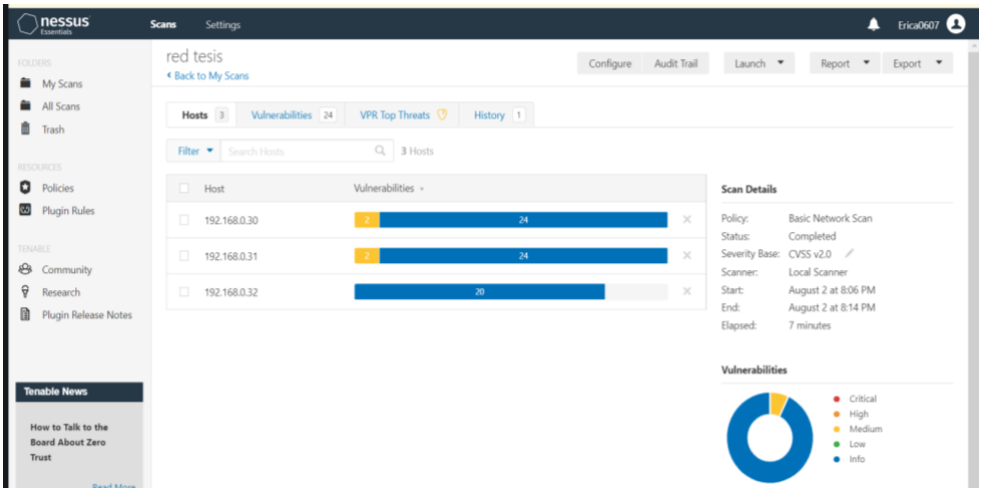

Figura 6-4: Vulnerabilidades Cámara

Elaborado por: Erica Padilla, 2022

Tabla 4-4: Vulnerabilidades

VULNERABILIDADES DE EQUIPOS	CONTROL DE ACCESO	INTEGRIDAD	CONFIDENCIALIDAD	DISPONIBILIDAD
Debilidad de contraseña			X	X
Sincronización Nessus				
JQuery 12				
HTTP				
Reenvió de IP activado				X
WEB Server				
Puertos abiertos			X	
Servicio detección				
Servicio de detección (SSH)	X			X
Common Platform			X	
Ethernet CARD	X			
Ethernet Mac	X			
ICMP Timestamp			X	
mDNS detección	X			
Nessus Escaneo			X	
ONVIF			X	
Fallos humanos		X	X	X
Energía Eléctrica				X

Elaborado por: Erica Padilla, 2022

Podemos observar las vulnerabilidades señaladas, hemos escogido estas, ya que nos vemos enfocados a la disponibilidad del servicio las cuales nos afectan de la siguiente manera.

- **Debilidad de contraseña:** Dentro del sistema de video vigilancia, los equipos de conexión inalámbrica, las antenas al iniciar su funcionamiento solicitan como seguridad el cambio de usuario y contraseña que viene de fábrica, pero no existe una comprobación de similitud, ya que si colocas el mismo usuario y contraseña permite el funcionamiento.
- **Puertos Abiertos y servicio de detección:** Existen variedad de puertos abiertos para la funcionalidad de protocolos como SSH, UPnP, que facilitan la detección de los dispositivos en la red.
- **Detección SSH:** Esta vulnerabilidad se encuentra ligada al control de acceso ya que puede sufrir ataques de fuerza bruta, esta utiliza el usuario y contraseña de nuestro ingreso a la interfaz gráfica para su funcionamiento.

- **Renvío de IP activado:** a nivel de nuestros dispositivos el riesgo de esto sería que puedan acceder a nuestros equipos, donde se reduciría el riesgo si hay una clave configurada, donde el peso de seguridad recae nuevamente en la debilidad de contraseñas.
- **Fallos Humanos:** Dentro de esta vulnerabilidad tenemos fallos físicos como olvidos de contraseñas, manipulación de software.
- **Energía Eléctrica:** Se refiere a la falta de continuidad en el sistema de energía eléctrica, ya que esta también forma parte primordial para la disponibilidad de nuestra cámara. Al encontrarse en lugares remotos, la energía tiene una inestabilidad considerable, ya sea pérdida total, parcial o fluctuaciones.

4.2.4. Actividad 4. Análisis Seguridad Lógica mediante la verificación de vulnerabilidades

Para la verificación si es necesario se realizará previamente la siguiente secuencia de procesos.

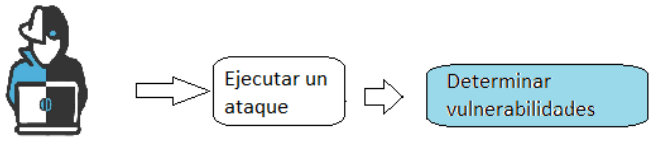

Figura 7-4: Diagrama para la verificación de vulnerabilidades

Elaborado por: Erica Padilla, 2022

Realizaremos la valoración de cada requerimiento de nuestras verificaciones mediante la calificación de capacidades de procesos de Cobit 5 Guía de Autoevaluación como observamos en la siguiente tabla.

Tabla 5-4: Calificación de procesos, Guía de autoevaluación

Nivel de proceso	Capacidad
0 (Incompleto)	El proceso no se ha implementado o no logra su propósito. En este nivel, hay evidencia escasa o nula de un logro sistemáticos del propósito del proceso.
1 (Realizado)	El proceso implementado logra su propósito.
2 (Gestionado)	El proceso ejecutado ahora es implementado de forma gestionada (planificada, monitorizada y ajustada) y los resultados son adecuadamente establecidos, controlados y mantenidos.
3 (Establecido)	El proceso gestionado ahora es implementado utilizando un proceso definido que permite conseguir los resultados del proceso.
4 (Predecible)	Un proceso establecido, opera en los límites definidos, para a conseguir los resultados del proceso.
5 (Optimizado)	Un proceso predecible, es continuamente mejorado para alcanzar los objetivos del negocio actuales y futuras

Fuente: ISACA, 2013

Elaborado por: Erica Padilla, 2022

De acuerdo con la ponderación del nivel de proceso se verifica la aplicación.

- V1: Arquitectura, diseñado y modelado de amenazas

Tabla 6-4: Verificación de arquitectura, diseñado y modelado de amenazas

1.4	Verificar que todos los componentes de la aplicación se definen de acuerdo con las funciones de negocio o de seguridad que proporcionan.	0
1.6	Verificar que se ha realizado un modelo de amenazas para la aplicación en cuestión y que éste cubre riesgos asociados con la suplantación de identidad, manipulación, repudio, revelación de información y elevación de privilegios (STRIDE).	0
1.8	Verificar que los componentes están separados unos de otros mediante controles de seguridad, tales como segmentación de la red, reglas de firewall, o grupos de seguridad basados en la nube.	0
1.9	Verificar que la aplicación tiene una clara separación entre la capa de datos, la capa de control y la capa de presentación, tal que las decisiones de seguridad pueden aplicarse en sistemas confiables.	0
1.10	Verificar que no hay ninguna lógica de negocio sensible, claves secretas u otra información propietaria en el código del lado del cliente.	0

Fuente: OWASP, 2017

Elaborado por: Erica Padilla, 2022

A nivel de diseño de la aplicación nos encontramos en un nivel 0, es decir tenemos muy poca evidencia que el aplicativo web este modelado bajo un régimen de protección de amenazas.

- V2: Requisitos de verificación de autenticación

Proceso 1. Para esta verificación se realizó un ataque de Inyección SQL al aplicativo web como se observa en la figura 8-4.

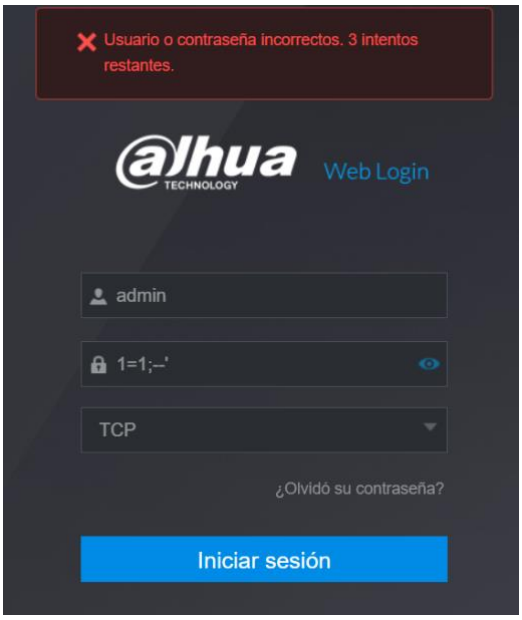

Figura 8-4: Inyección SQL al aplicativo web

Elaborado por: Erica Padilla, 2022

Tabla 7-4: Verificación de autenticación

2.1	Verificar que todas las páginas y recursos requieran autenticación excepto aquellos que sean específicamente destinados a ser públicos (Principio de mediación completa).	1
2.2	Verificar que todos los campos de credenciales no reflejen las contraseñas del usuario. Cargar la credencial por parte de la aplicación implica que la misma fue almacenada de forma reversible o en texto plano, lo que se encuentra explícitamente prohibido.	1
2.5	Verificar que los campos de contraseñas permiten o fomentan el uso de frases como contraseñas (passphrases) y no impiden el uso de gestores de contraseñas, contraseñas largas o altamente complejas.	0
2.7	Verificar que la funcionalidad de cambio de contraseña solicite la contraseña anterior, la nueva contraseña y una confirmación de la contraseña.	0
2.8	Verificar que todas las decisiones de autenticación son registradas en la bitácora sin almacenar información sobre la contraseña o el identificador de la sesión. Esto debería incluir los metadatos necesarios para investigaciones de seguridad.	0

2.9	Verificar que las contraseñas de las cuentas se encuentren almacenadas utilizando una rutina de hashing con una sal, y que requiera un factor de trabajo lo suficientemente alto para evitar un ataque de fuerza bruta.	0
2.11	Verificar que las funciones de recuperar contraseña y acceso no revelen la contraseña actual y que la nueva contraseña no se envíe en texto plano al usuario	1
2.13	Verificar que no se utilizan contraseñas por defecto en la aplicación o cualquiera de los componentes utilizados por la misma (como "admin/password").	1
2.14	Verificar que existen mecanismos de anti-automatización que previenen la verificación de credenciales obtenidas de forma masiva, ataques de fuerza bruta y ataques de bloqueos de cuentas.	0
2.16	Verificar que las funcionalidades de recuperar contraseña y otras formas de recuperar la cuenta utilizan mecanismos de TOTP (Time-Based One-Time Password) u otro tipo de soft token, push a dispositivo móvil u otro tipo de mecanismo de recuperación offline. El uso de un valor aleatorio en un correo electrónico o SMS debe ser la última opción ya que son conocidas sus debilidades.	0
2.17	Verificar que el bloqueo de la cuenta se divida en estado de bloqueo suave y duro, y éstas no son mutuamente excluyentes. Si una cuenta está temporalmente bloqueada de forma suave debido a un ataque de fuerza bruta, esto no debe restablecer el bloqueo de estado duro.	1
2.18	Verificar que si la aplicación hace uso de conocimiento basado en preguntas (también conocido como "secreto"), las preguntas no violan leyes de privacidad y son lo suficientemente fuertes para proteger la cuenta de recuperaciones maliciosas.	0
2.19	Verificar que el sistema puede configurarse para no permitir el uso de un número de contraseñas utilizadas anteriormente.	0
2.21	Verificar que existen medidas para bloquear el uso de contraseñas comúnmente utilizadas y contraseñas débiles	0
2.22	Verificar que todos los desafíos de autenticación, ya sea exitosa o fallida, responden en el mismo tiempo promedio	1
2.24	Verificar que, si una aplicación permite a los usuarios autenticarse, puedan hacerlo mediante autenticación de dos factores u otra autenticación fuerte, o cualquier esquema similar que proporcione protección contra la divulgación de nombres de usuario y contraseñas	0
2.25	Verificar que las interfaces administrativas de la aplicación no sean accesibles a intrusos.	0
2.26	Autocompletar de navegadores e integración con gestores de contraseñas deben estar permitidos a no ser que se encuentren prohibidos por políticas de riesgos.	0

Fuente: OWASP, 2017

Elaborado por: Erica Padilla, 2022

- V3. Requisitos de verificación de gestión de sesiones

Tabla 8-4: Verificación de gestión de sesiones

3.1	Verificar que no se utiliza un gestor de sesiones personalizado, o que, si el gestor de sesiones es personalizado, éste sea resistente contra los ataques más comunes.	0
3.2	Verificar que las sesiones se invalidan cuando el usuario cierra la sesión.	1
3.3	Verificar que las sesiones se invalidan luego de un período determinado de inactividad.	1
3.4	Verificar que las sesiones se invalidan luego de un período determinado de tiempo, independientemente de que se esté registrando actividad (timeout absoluto).	0
3.5	Verificar que todas las páginas que requieren autenticación poseen acceso fácil y visible a la funcionalidad de cierre de sesión.	1
3.6	Verificar que el identificador de sesión nunca se revele en URLs, mensajes de error o registros de bitácora. Esto incluye verificar que la aplicación no es compatible con la re-escritura de URL incluyendo el identificador de sesión.	1
3.7	Verificar que toda autenticación exitosa y re-autenticaciones generen un nuevo identificador de sesión.	0
3.10	Verificar que sólo los identificadores de sesión generados por la aplicación son reconocidos como activos por ésta.	0
3.11	Verificar que los identificadores de sesión son suficientemente largos, aleatorios y únicos para las sesiones activas.	0
3.12	Verificar que los identificadores de sesión almacenados en cookies poseen su atributo “path” establecido en un valor adecuadamente restrictivo y que además contenga los atributos "Secure" y "HttpOnly"	1
3.16	Verificar que la aplicación limita el número de sesiones concurrentes activas.	0
3.17	Verificar que una lista de sesiones activas esté disponible en el perfil de cuenta o similar para cada usuario. El usuario debe ser capaz de terminar cualquier sesión activa.	0
3.18	Verificar que al usuario se le sugiera la opción de terminar todas las otras sesiones activas después de un proceso de cambio de contraseña exitoso.	0

Fuente: OWASP, 2017

Elaborado por: Erica Padilla, 2022

- V4. Verificación de Control de acceso

Tabla 9-4: Verificación de Control de acceso

4.1	Verificar que existe el principio de privilegio mínimo - los usuarios sólo deben ser capaces de acceder a las funciones, archivos de datos, URL, controladores, servicios y otros recursos, para los cuales poseen una autorización específica. Esto implica protección contra suplantación de identidad y elevación de privilegios	1
4.4	Verificar que el acceso a registros sensibles esté protegido, tal que sólo objetos autorizados o datos sean accesibles por cada usuario (por ejemplo, proteger contra la posible manipulación hecha por usuarios sobre un parámetro para ver o modificar la cuenta de otro usuario).	1
4.9	Verificar que las mismas reglas de control de acceso implícitas en la capa de presentación son aplicadas en el servidor.	0

Fuente: OWASP, 2017

Elaborado por: Erica Padilla, 2022

- V5. Manejo de entrada de datos maliciosos

Ataque DDoS

Realizamos este ataque hacia el aplicativo web de nuestra cámara como se ve en la figura 9-3, mediante la herramienta Slowloris de kalylinux. Slowloris es una herramienta la cual envía una inundación de paquetes y la misma nos entrega un informe como en la figura 10-3.

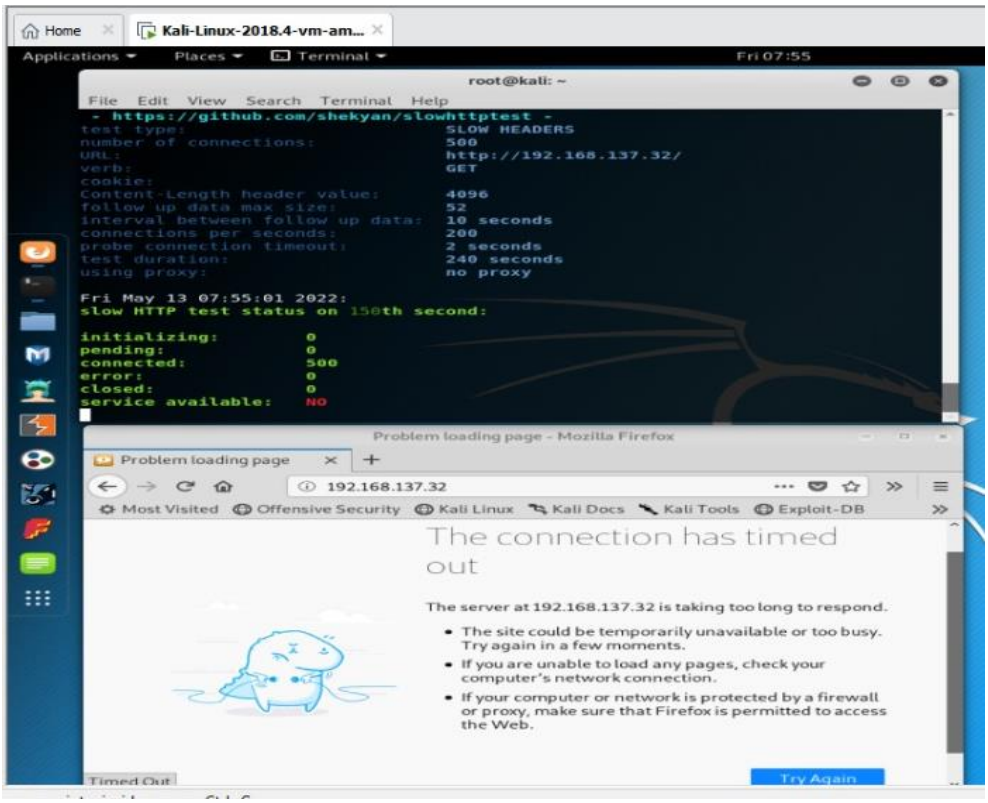

Figura 9-4: Denegación de Servicios cámara

Elaborado por: Erica Padilla, 2022

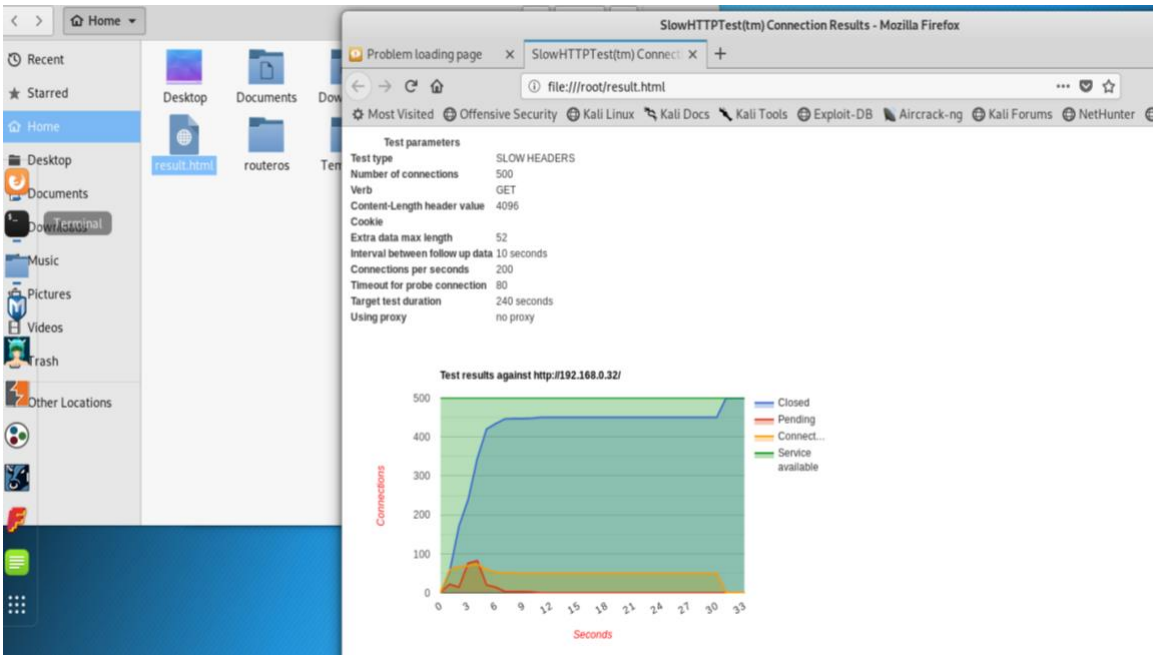

Figura 10-4: Reporte DDoS

Elaborado por: Erica Padilla, 2022

Tabla 10-4: Verificación entrada de datos maliciosos

5.1	Verificar que el entorno de ejecución no es susceptible a desbordamientos de búfer, o que los controles de seguridad previenen desbordamientos de búfer.	0
5.3	Verificar que las fallas de validación de entradas de datos del lado del servidor sean rechazadas y registradas.	0
5.5	Verificar que se aplican las rutinas de validación de entradas de datos del lado del servidor.	0
5.6	Verificar que un único control de validación de entrada es utilizado por la aplicación para cada tipo de datos que es aceptado.	0
5.10	Verificar que todas las consultas de SQL, HQL, OSQL, NOSQL y procedimientos almacenados, llamadas de procedimientos almacenados están protegidos por la utilización de declaraciones preparadas o parametrización de consultas, y por lo tanto no sean susceptibles a la inyección de SQL	1
5.17	Verificar que la aplicación contenga defensas contra los ataques de contaminación de parámetros HTTP (agregar parámetros a la URL), particularmente si el framework de la aplicación no hace distinción sobre el origen de los parámetros de la petición (GET, POST, cookies, cabeceras, ambiente, etc.)	0
5.18	Verificar que las validaciones del lado del cliente se utilizan como una segunda línea de defensa, en adición a la validación del lado del servidor.	0
5.19	Verificar que todos los datos de entrada sean validados, no solamente los campos de formularios HTML sino también todos los orígenes de entrada como las llamadas REST, parámetros de consulta, encabezados HTTP, cookies, archivos por lotes, fuentes RSS, etc.; mediante validación positiva (lista blanca), o utilizando otras formas de validación menos eficaces tales como listas de rechazo transitorio (eliminando símbolos defectuosos), o rechazando malas entradas (listas negras).	0
5.20	Verificar que datos estructurados fuertemente tipados son validados un esquema definido incluyendo; caracteres permitidos, longitud y patrones (p. ej. tarjeta de crédito o teléfono o validando que dos campos relacionados son razonables, tales como validación de coincidencia entre localidad y código postal)	0
5.21	Verificar que los datos no estructurados sean sanitizados cumpliendo medidas genéricas de seguridad tales como caracteres permitidos, longitud y que caracteres potencialmente dañinos en cierto contexto sean anulados (p. ej. nombres naturales con Unicode o apóstrofos, como ねこ o O'Hara)	0

Fuente: OWASP, 2017

Elaborado por: Erica Padilla, 2022

- V11. Requisitos de verificación de configuración de seguridad HTTP

Tabla 11-4: Verificación de configuración de seguridad HTTP

11.1	Verificar que la aplicación acepte solo un conjunto definido de métodos de solicitud HTTP y que son necesarios, como GET y POST, y métodos no utilizados (por ejemplo: TRACE, PUT y DELETE) se encuentran explícitamente bloqueados.	0
11.2	Verificar que cada respuesta HTTP contenga una cabecera content-type en la que se especifique un conjunto utilizando un conjunto de caracteres seguros (Ejemplo: UTF-8, ISO 8859-1).	0
11.3	Verificar que los encabezados HTTP agregados por un proxy confiable o dispositivos SSO, tales como un token de portador (bearer), son autenticados por la aplicación.	0
11.5	Verificar que los encabezados HTTP o cualquier parte de la respuesta HTTP no expongan información detallada de la versión de los componentes del sistema.	1

Fuente: OWASP, 2017

Elaborado por: Erica Padilla, 2022

- V15. Lógica del negocio

Tabla 12-4: Verificación de lógica del negocio

15.1	Verificar que la aplicación sólo procese flujos lógicos de negocios en orden secuencial, con todos los pasos procesados en tiempo humano realista, y no procesados fuera de orden, con pasos salteados, con pasos del proceso de otro usuario, o de transacciones muy rápidamente enviadas.	1
15.2	Verificar que la aplicación tiene límites de negocio y los aplique correctamente por cada usuario, con alertas configurables y reacciones automatizadas ante ataques inusuales o automáticos.	1

Fuente: OWASP, 2017

Elaborado por: Erica Padilla, 2022

4.2.5. Actividad 5. Análisis Seguridad Física

La variación de voltaje dentro de la ubicación de nuestro sistema se vuelve fundamental para garantizar el servicio y mantener la disponibilidad, por ello se evaluó el sistema de alimentación eléctrica.

Este sistema tiene 2 posibles fallos: Disponibilidad de energía eléctrica y desastres naturales. En la disponibilidad de la energía se pudo verificar que durante el año tiene un promedio de 30 cortes de energía con duración de 24 a 48 horas.

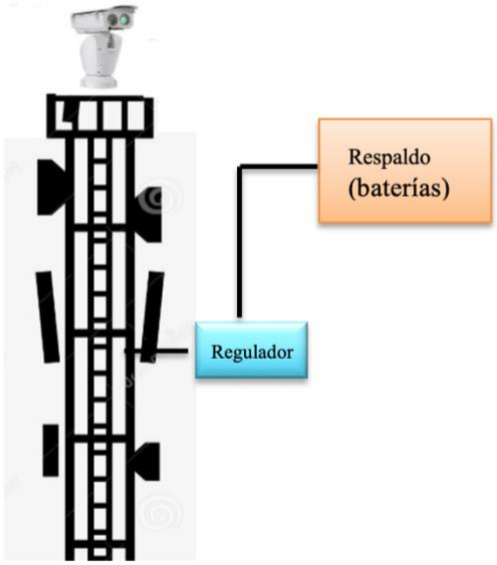

Figura 11-4: Sistema Eléctrico inicial

Elaborado por: Erica Padilla, 2022

4.3. Fase 3. Definir hoja de ruta

Para el desarrollo correcto de nuestro sistema nuestro objetivo principal es aumentar la disponibilidad de la transmisión de nuestra cámara laser. Por ello y por la información obtenida en todo el análisis anterior, determinamos la necesidad de implementar un hardening al sistema.

4.3.1. Actividad 1. Selección de hardening

La disponibilidad de nuestra cámara se ve afectada no solo a nivel lógico, sino también a nivel físico. Por ello necesitamos una seguridad que cubra todos nuestros dispositivos que incluyan su transmisión.

Seguridad Perimetral

La seguridad perimetral tiene como objetivo utilizar y manejar la información de una manera segura. Por ello es necesario incrementar credenciales de acceso para brindar un acceso seguro al aplicativo web, brindando controles de autenticación según el nivel de riesgo encontrado y para la negación de acceso a atacantes tentativos del sistema.

Para la sustentación de lo anterior se debe establecer reglas para nuestro sistema.

Ya que nuestro servicio se basa en aplicaciones en producción tenemos las siguientes herramientas de seguridad perimetral.

Firewall: Siendo el firewall una puerta de control de ingreso a la red, se convierte en nuestra mejor aliada para el manejo de seguridad a toda la infraestructura de nuestra red de video vigilancia.

4.4. Fase 4. Planificar el programa

Para la selección hemos encontrado la necesidad de monitorear el sistema eléctrico ya que uno de los factores más relevantes durante este trabajo ha sido la variación de voltaje y la perdida de energía.

4.4.1. Actividad 1. Construcción de mejoras

Monitoreo al sistema eléctrico. - Dentro de la realización de este proyecto pudimos observar que la disponibilidad de energía tiene una gran influencia en el funcionamiento de nuestra cámara, ya que, por la ubicación del sector camaronero, el difícil acceso, las empresas camaroneras instalan sus propios puntos de energía, ya que cuando hay algún fallo, ellos contratan personal privado que les solucione en la brevedad posible.

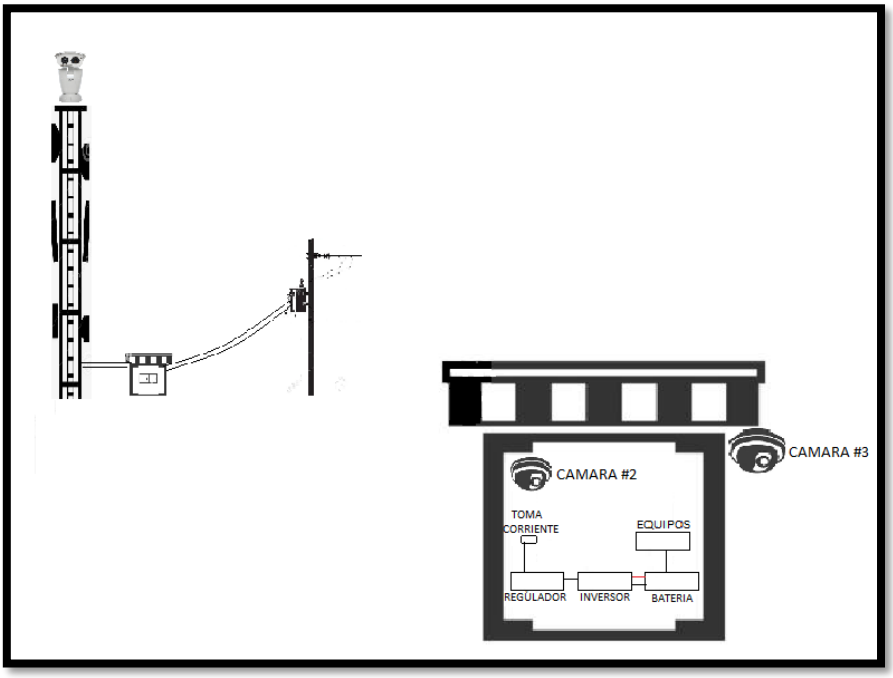

Figura 12-4: Sistema Eléctrico con cámaras de monitoreo

Elaborado por: Erica Padilla, 2022

4.4.2. Actividad 2. Recomendaciones de Seguridad

- Cambiar las contraseñas y utilizar contraseñas seguras: Se debe cambiar las contraseñas predeterminadas de inmediato y elegir una contraseña segura como se observa en la figura 3-13. Se considera una contraseña segura la que contenga mínimo 8 caracteres con una combinación de caracteres especiales, números y letras (mayúsculas y minúsculas).

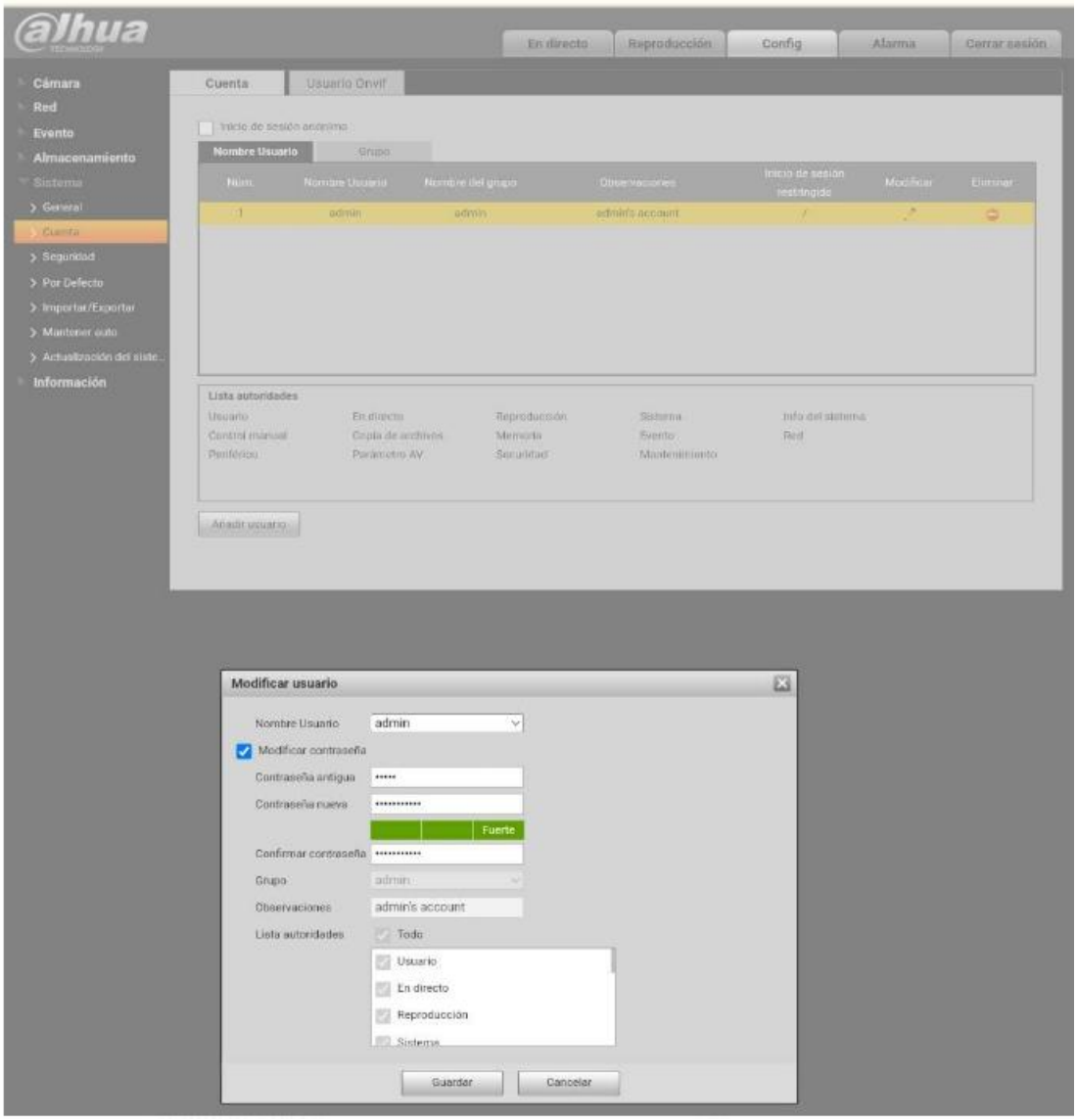

Figura 13-4: Cambio de contraseña

Elaborado por: Erica Padilla, 2022

- Actualizar el firmware: Cada marca de tecnología realiza el lanzamiento de firmware actualizado, con el cual se realiza correcciones de seguridad como se observa en la figura 3-14 verificar que se disponga de la última versión de firmware.

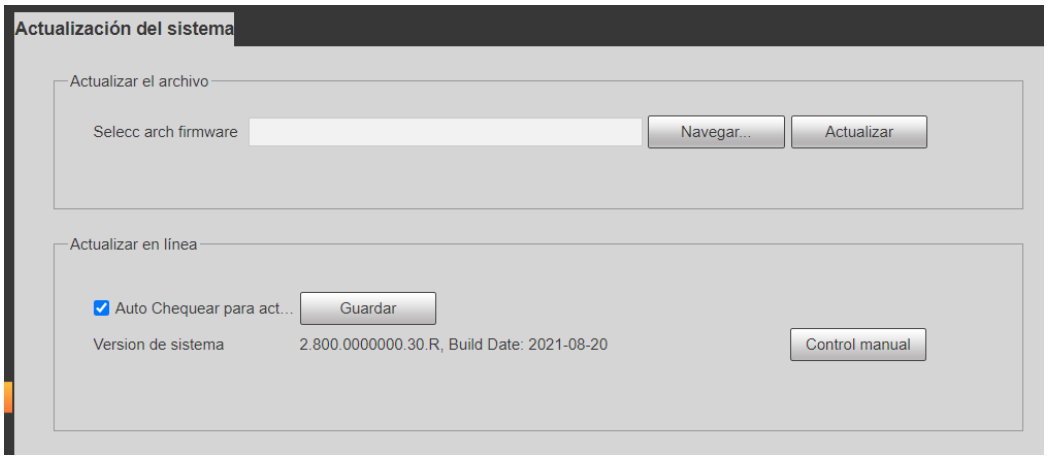

Figura 14-4: Actualización de firmware

Elaborado por: Erica Padilla, 2022

- Cambiar los puertos HTTP y TCP predeterminados: Estos puertos se pueden cambiar a cualquier conjunto de números entre 1025-65535 para evitar los puertos predeterminados y reducir el riesgo de intrusión. Como podemos observar en la figura 3-15 se cambió el puerto ya que el predeterminado es el 3777.

Figura 15-4: Puertos TCP y UDP

Elaborado por: Erica Padilla, 2022

- Cambiar la contraseña de ONVIF: Esta se debe cambiar de forma manual, ya que no es la misma que sus credenciales de acceso, como se observa en la figura 3-16, esta contraseña viene por defecto con admin-admin.

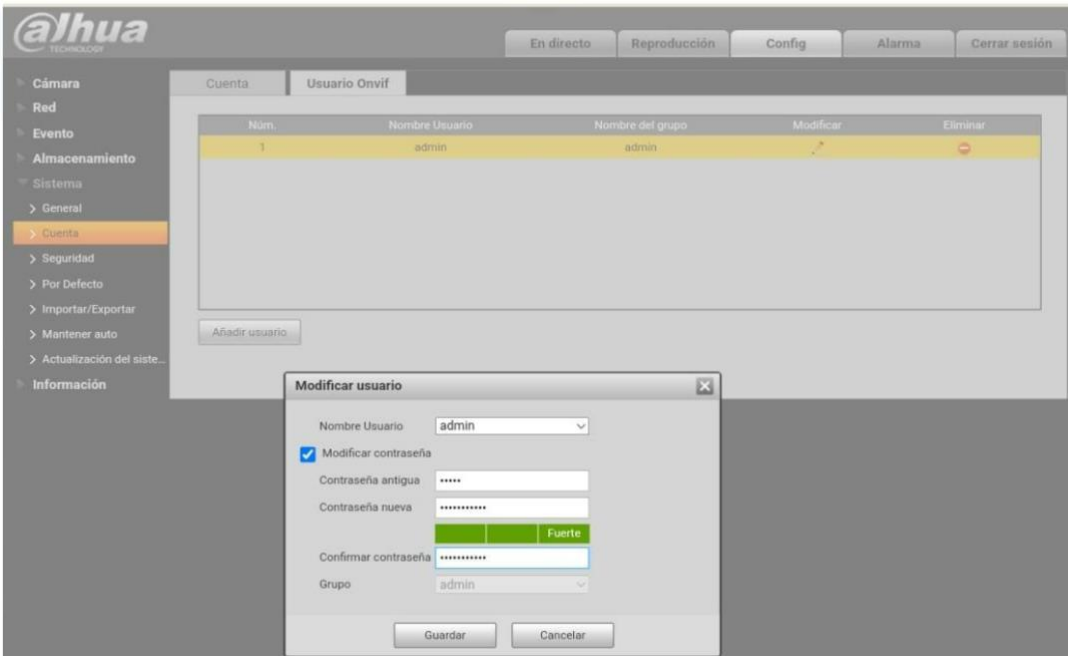

Figura 16-4: Contraseña onvif

Elaborado por: Erica Padilla, 2022

- Reenviar solo los puertos que necesita: Es importante reenviar solo los puertos HTTP y TCP.

- Desactivar el inicio de sesión automático: Evitar dejar credenciales visibles para usuarios sin autorización, como se observa en la figura 3-17 se puede restringir el inicio de sesión mediante un horario de acceso.

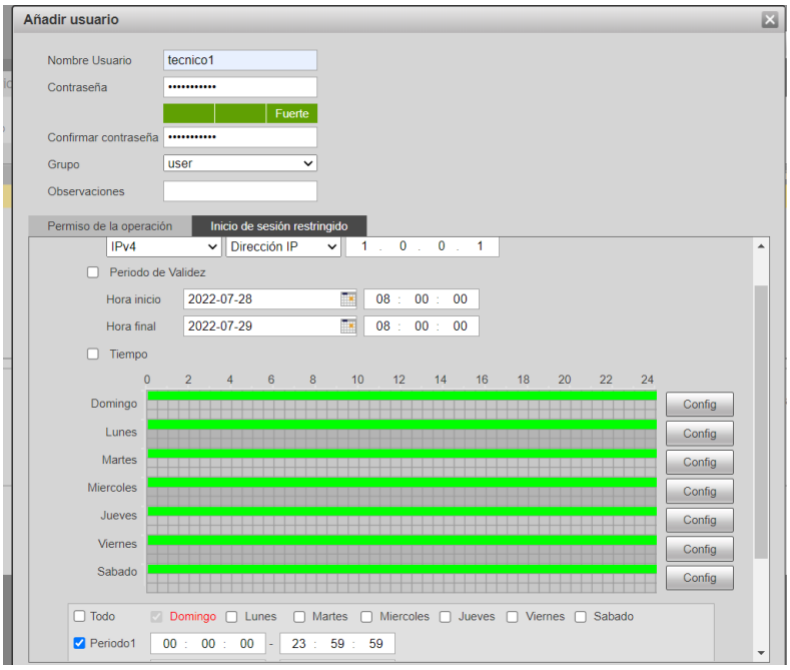

Figura 17-4: Restricción de inicio de sesión

Elaborado por: Erica Padilla, 2022

- Limitar las funciones de las cuentas: Si existen varios usuarios se debe delimitar los accesos de autorización a funciones específicas.

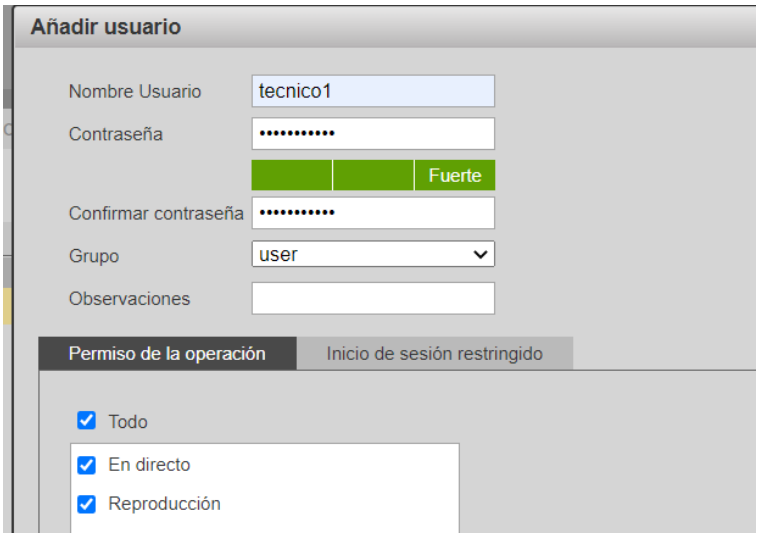

Figura 18-4: Delimitación de funciones

Elaborado por: Erica Padilla, 2022

- Desactivar SNMP: Si no se está utilizando se debe desactivar o si está utilizando SNMP, debe hacerlo solo temporalmente, solo para pruebas.

4.5. Fase 5. Ejecutar el Plan

4.5.1. Actividad 1. Implementación de hardening

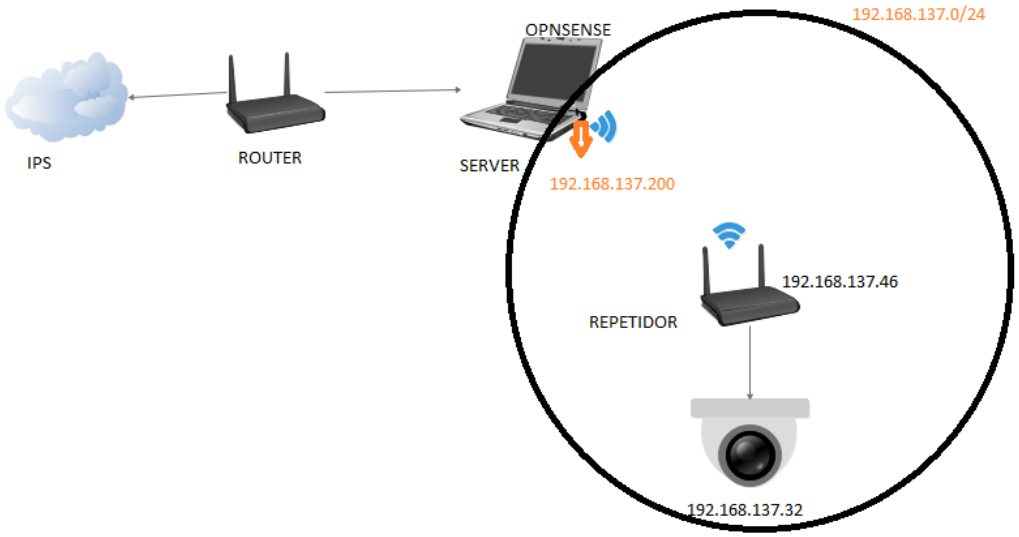

Figura 19-4: Diseño de Hardening

Elaborado por: Erica Padilla, 2022

La utilización de un servidor especialmente dirigido para el sistema de video vigilancia, se convierte en una necesidad primordial, ya que por evaluación se ha verificado que la falla de volteje dentro de la localización de nuestra cámara láser es sumamente alta, lo que nos exige un respaldo de almacenamiento, el mismo que va a estar ubicado en este servidor como observamos en la figura 3-13, pero en el mismo podemos implementar a su vez nuestro firewall, el cual nos ayuda a mantener

un seguimiento y control de seguridad en nuestro sistema, con la finalidad de mantener la disponibilidad del servicio.

FIREWALL OPNsense

Algunas de las principales características de este sistema operativo son que se administra vía web desde un completo panel de control, tenemos una gran cantidad de servicios como servidor Proxy, proxi caché, servidores VPN de tipo IPsec y OpenVPN, clientes IPsec y OpenVPN, servidor RADIUS, portal cautivo, sistema de detección y prevención de intrusiones Snort y también Suricata, servidor DNS, DNS Forwarder, DHCP server, DHCP relay, Dynamic DNS, compatibilidad con VLANs 802.1Q.

La activación del firewall que proteja el sistema de video vigilancia se observa en la imagen 3-14 con la asignación de direcciones IP.

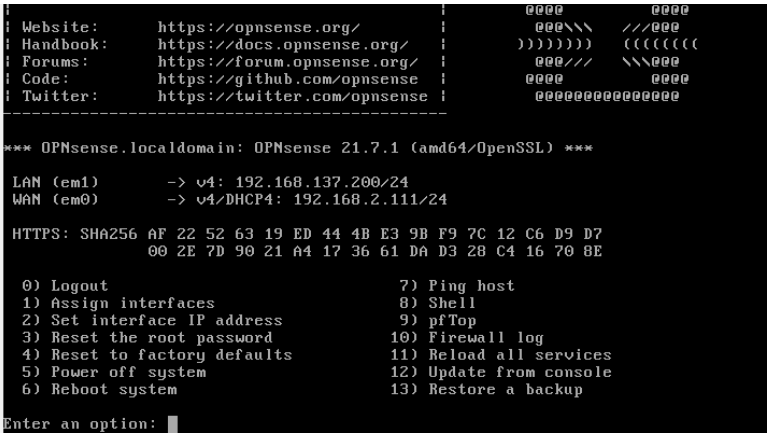

Figura 20-4: Direccionamiento OPNsense

Elaborado por: Erica Padilla, 2022

Este firewall trabaja juntamente con nuestro sistema de monitoreo al sistema eléctrico, ya que mediante las pruebas realizadas observamos que el monitoreo en el sistema eléctrico nos dará evidencia para evitar el sece de funcionamiento de nuestra cámara laser, la cual es nuestro objetivo principal.

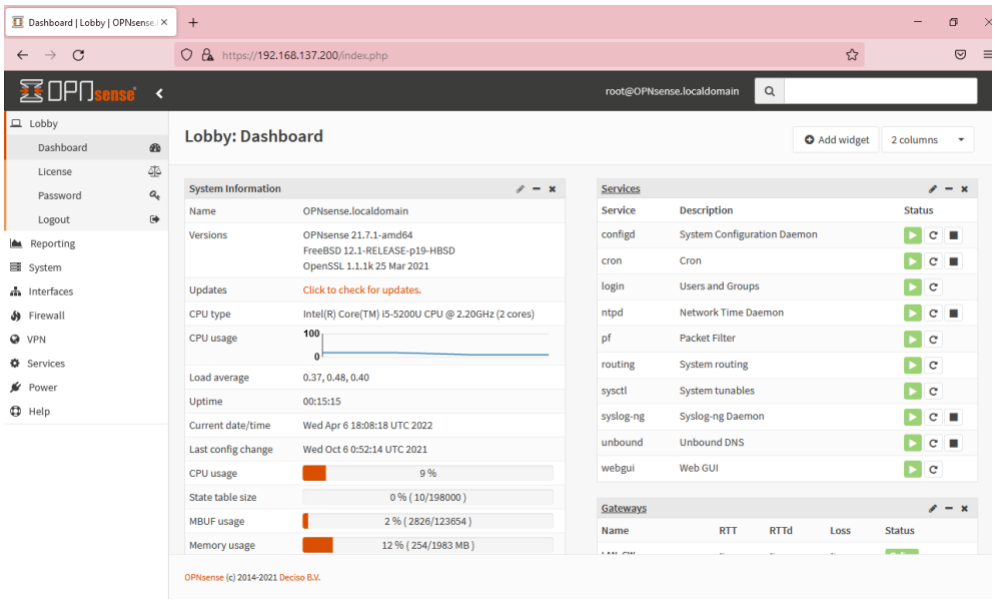

Figura 21-4: Funcionamiento interfaz gráfica

Elaborado por: Erica Padilla, 2022

4.5.2. Actividad 2. Implementación de cámaras a caseta

Se agregó las direcciones de las cámaras al firewall el cual nos avisa si estas tienen algún evento como dejar de transmitir, con esto podemos verificar donde está el posible fallo antes que el sistema de respaldo de energía deje de funcionar.

Figura 22-4: Sistema funcionando con baterías

Elaborado por: Erica Padilla, 2022

Gracias al uso del firewall y la redundancia de monitoreo con la cámara instalada como lo observamos en la figura 3-17 en el sistema eléctrico podemos prevenir el corte de servicio y realizar una acción de recuperación de servicio de manera más rápida, así aumentamos el nivel de disponibilidad del sistema de video vigilancia, es decir del funcionamiento de nuestra cámara láser.

Figura 23-4: Cámara de Torre (Erica Padilla, 2022)

Elaborado por: Erica Padilla, 2022

4.6. Fase 6. Obtener Beneficios

Para poder tener un mejor manejo de todo el sistema, se estableció determinar una persona encargada de la supervisión física del sistema eléctrico, el cual posee un medio de comunicación de radio frecuencia (radio móvil) para reportes inmediatos.

4.6.1. Actividad 1. Medición de disponibilidad mediante 2 ambientes

Para la evaluación del sistema se realizará una comparación porcentual de la disponibilidad alcanzada, ya que es el requerimiento principal de nuestro trabajo, se tomará 2 mediciones de eventos durante un periodo de 20 días, el mismo será medido en horas.

Generando así dos escenarios para la evaluación.

4.6.1.1. Población

Para medir la disponibilidad del sistema se tomará como población la continuidad del sistema de videovigilancia durante el periodo de 2 meses, los de mayor frecuencia en perdida de energía.

4.6.1.2. Muestra

- El tipo de muestra que se aplica es el no aleatorio por conveniencia donde se selecciona como único requerimiento la funcionalidad del sistema.
- Se considera los eventos presentados durante el periodo de 20 días.

4.6.1.3. Eventos Suscitados

Pérdida total de energía. - No existe energía a nivel de todo el territorio camaronero.

Perdida parcial de energía. - No existe energía en ciertos sectores del territorio, en nuestro caso no hay energía en la caseta de equipos por consecuencia la torre tampoco esta abastecida.

Perdida técnica de energía. - No existe energía en equipos determinados, es decir, dentro de la caseta tenemos inhibición de inversor, ya que por las caídas de tensión el equipo no da paso a la activación del sistema de baterías.

Perdida de desastre natural. - No existe energía por desastres naturales como rayos

CAPÍTULO V

5. PROPUESTA

5.1. Análisis de tiempos

Se evalúa el tiempo registrado en cada evento, durante la perdida de disponibilidad de nuestra cámara laser. En el periodo de 20 días, tendríamos un total de 480 horas de funcionamiento esperado.

Se analizará el valor porcentual de perdida según cada evento.

5.1.1. Análisis de tiempos sin la implementación del hardening

Tiempo de trabajo esperado= 480 horas

$$\text{Pérdida} = \frac{\text{tiempo perdidas horas}}{\text{Tiempo trabajo esperado}}$$

Pérdida % = Perdida *100

Evento 1. Pérdida Total de energía

$$\text{Perdida} = \frac{30 \text{ horas}}{480 \text{ horas}} = 0.0625$$

Perdida % = 0.0625 * 100= 6.25%

Evento 2. Pérdida parcial de energía

$$\text{Pérdida} = \frac{15 \text{ horas}}{480 \text{ horas}} = 0.0312$$

Pérdida % = 0.0312 * 100= 3.12%

Evento 3. Pérdida técnica de energía

$$\text{Pérdida} = \frac{4 \text{ horas}}{480 \text{ horas}} = 0.0083$$

Pérdida % = 0.0083 * 100= 0.83%

Evento 4. Pérdida de desastre natural

$$\text{Pérdida} = \frac{12 \text{ horas}}{480 \text{ horas}} = 0.0250$$

Pérdida % = 0.0250 * 100= 2.50%

Tabla 1-5: Pérdida de visualización de la cámara sin hardening

Tiempo de perdida de visualización de la cámara			
Eventos	**Numero de fallos**	**Datos en horas**	**Porcentaje horas**
Pérdida total de energía.	**2**	**30**	**6.25%**
Perdida parcial de energía.	**3**	**15**	**3.12%**
Perdida técnica de energía.	**1**	**4**	**0.83%**
Perdida de desastre natural.	**1**	**12**	**2.50%**
PERDIDA TOTAL	**7 fallos**	**61 horas**	**12.70%**

Elaborado por: Erica Padilla, 2022

Tiempo de funcionamiento = tiempo esperado – tiempo de pérdida total

Tiempo de funcionamiento = 480 horas – 61 horas

Tiempo de funcionamiento= 419 horas

Durante el periodo de 20 días para obtener una disponibilidad del 100% se debería tener 480 horas de trabajo continuo como tenemos una pérdida total de 61 horas, tenemos como resultados 419 horas de trabajo.

Disponibilidad sin implementación de hardening= Tiempo funcionamiento horas

Tiempo trabajo esperado horas

Disponibilidad sin implementación de hardening = 419 horas

480 horas

Disponibilidad sin implementación de hardening = 0.872

Disponibilidad sin implementación de hardening % = 0.0872 * 100

Disponibilidad sin implementación de hardening % = **87.29%**

Figura 1-5: Perdidas de funcionamiento sin hardening

Elaborado por: Erica Padilla, 2022

5.1.2. Análisis de tiempos con la implementación del hardening

Tiempo de trabajo esperado= 480 horas

Pérdida= tiempo perdidas horas

Tiempo trabajo esperado

Pérdida % = Perdida *100

Evento 1. Pérdida Total de energía

$$\text{Pérdida} = \frac{6 \text{ horas}}{480 \text{ horas}} = 0.0125$$

Pérdida % = 0.0125 * 100= 1.25%

Evento 2. Pérdida parcial de energía

$$\text{Pérdida} = \frac{6 \text{ horas}}{480 \text{ horas}} = 0.0125$$

Pérdida % = 0.0125 * 100= 1.25%

Evento 3. Pérdida técnica de energía

No existe evento

Evento 4. Pérdida de desastre natural

$$\text{Pérdida} = \frac{12 \text{ horas}}{480 \text{ horas}} = 0.0250$$

Pérdida % = 0.0250 * 100= 2.50%

Tabla 2-5: Pérdida de visualización con hardening

Tiempo de pérdida de visualización de la cámara			
Eventos	**Numero de fallos**	**Datos en horas**	**Porcentaje horas**
Pérdida total de energía.	**2**	**6**	**1.25%**
Pérdida parcial de energía.	**3**	**6**	**1.25%**
Pérdida técnica de energía.	**0**	**0**	**0%**
Pérdida de desastre natural.	**1**	**12**	**2.50%**
PÉRDIDA TOTAL	**6 fallos**	**24 horas**	**5%**

Elaborado por: Erica Padilla, 2022

La cámara laser tiene una pérdida de servicio del 5% con la implementación del hardening

Tiempo de funcionamiento = tiempo esperado – tiempo de pérdida total

Tiempo de funcionamiento = 480 horas – 24 horas

Tiempo de funcionamiento= 456 horas

DISPONIBILIDAD

$$\text{Disponibilidad sin implementación de hardening} = \frac{\text{Tiempo funcionamiento horas}}{\text{Tiempo trabajo esperado horas}}$$

$$\text{Disponibilidad sin implementación de hardening} = \frac{456 \text{ horas}}{480 \text{ horas}}$$

Disponibilidad sin implementación de hardening = 0.95

Disponibilidad sin implementación de hardening % = 0.95 * 100

Disponibilidad sin implementación de hardening % = **95%**

Figura 2-5: Disponibilidad con la implementación del hardening

Elaborado por: Erica Padilla, 2022

Tabla 3-5: Tabla comparativa de la disponibilidad

Sin la implementación del hardening	Con la implementación del hardening
87.29% horas	95% horas

Elaborado por: Erica Padilla, 2022

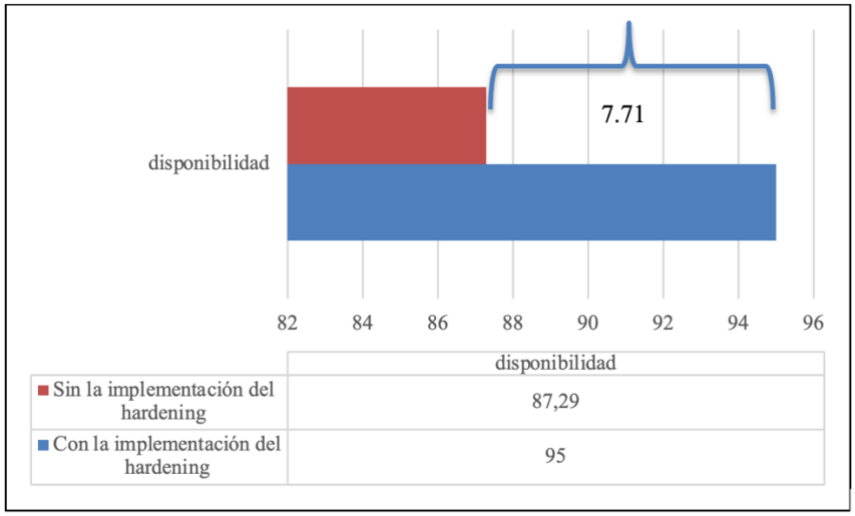

Figura 3-5: Incremento de disponibilidad con hardening

Elaborado por: Erica Padilla, 2022

Debido a la implementación del hardening, existe un incremento de 7.71 %, de funcionamiento en porcentajes horas, es decir que tiene más disponibilidad y menos perdidas en la cámara laser.

5.2. Planteamiento del problema

1. Planteamiento de Hipótesis

H_0: Al analizar los protocolos de comunicación en la transmisión de video vigilancia el uso de protocolos específicos garantiza la disponibilidad del servicio disminuyendo la perdida *en el sistema* sin *la implementación del Hardening en horas* ≤ 87.29

H1: Al analizar los protocolos de comunicación en la transmisión de video vigilancia el uso de protocolos específicos garantiza la disponibilidad del servicio disminuyendo la perdida *en el sistema* con $la\ implementación\ del\ Hardening\ en\ horas \leq 87.29$

2. Nivel de Significancia

$$\alpha = 0.05$$

3. Estadístico de Prueba

$\mu = Media\ poblacional$

$S = Error\ estándar\ de\ la\ muestra$

$n = Tamaño\ de\ la\ muestra$

$\bar{X} = Media\ de\ la\ distribucción\ de\ datos$

$$Media(X) = \bar{x} = \frac{\sum_{i=1}^{N} X_i}{N}$$

$$\bar{x} = \frac{30 + 15 + 4 + 12}{4} = 15.25$$

$$s = \sqrt{S^2} = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \mu)^2}{n-1}}$$

$$s = \sqrt{\frac{(30 - 87.29)^2 + (15 - 87.29)^2 + (4 - 87.29)^2 + (12 - 87.29)^2}{4-1}} = 10.87$$

Datos:

$\mu = 87.29$

$s = 10.87$

$n = 4$

$\bar{X} = 15.25$

$$t = \frac{\bar{X} - \mu}{\frac{S}{\sqrt{n}}}$$

$$t = \frac{15.25 - 87.29}{\frac{10.87}{\sqrt{4}}}$$

$$t = -16.038$$

4. Regla de Decisión

$$t \leq t_t : H_0 \; se \; rechaza$$

$$-16.038 < -2.353 : H_0 \; se \; rechaza$$
$$p = 0.0495 < 0.05 : H_0 \; se \; rechaza$$

5. Toma de Decisión

Existe suficiente prueba estadística para rechazar H0, es decir que los fallos en el sistema sin la implementación del Hardening aumentan en su porcentaje en horas, lo cual nos conlleva a comprobar la necesidad de la utilización del hardening, ya que se desea disminuir las perdidas.

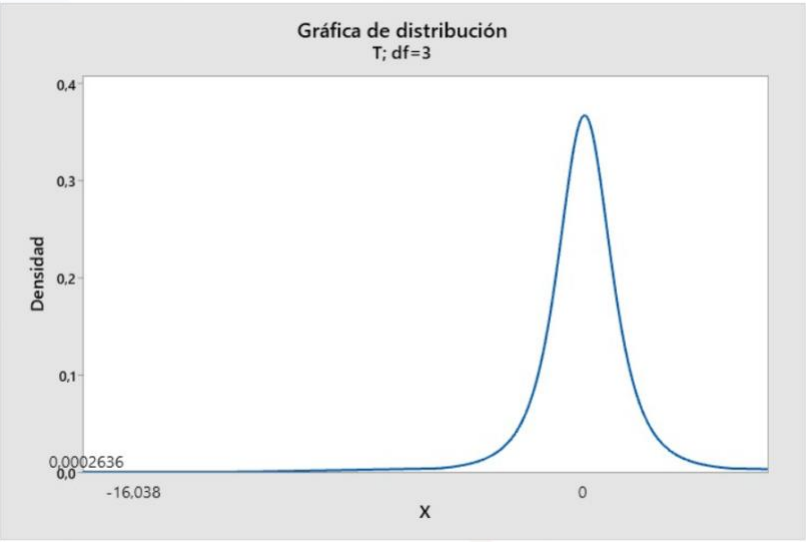

Figura 4-5: Grafica T-Student densidad

Elaborado por: Erica Padilla, 2022

Como podemos evidenciar, el uso de nuestro firewall reduce las vulnerabilidades en el sistema de video vigilancia, obteniendo un incremento de disponibilidad del 7.71 %, dando una confianza de aplicación de nuestro hardening.

CONCLUSIONES

- Las cámaras IP se han convertido en un dispositivo de respaldo para la seguridad, cuando estas se encuentran en correcto funcionamiento, es decir su disponibilidad es significativa, por ellos la importancia de tomar más medidas de seguridad en estos dispositivos, aumentar los requerimientos que aseguren la disponibilidad del servicio, ya que no se considera la seguridad en ellos, más se enfocan a su funcionalidad, es decir existen los protocolos de transmisión segura, pero estos no garantizan la disponibilidad.

- Dentro de la implementación de nuestro ambiente de pruebas, comprobamos el vínculo primordial con la seguridad y el aplicativo web de la cámara, ya que hemos comprobado que mediante ataques se rompe la seguridad y por consecuencia pierde disponibilidad la cámara.

- En nuestro proyecto no se puede permitir un cese de servicio ya que el giro del negocio, es decir el nivel de producción y cuidado acuícola se basa en el monitoreo de cámaras con sistema de video vigilancia, colocando el monitoreo del sistema de video vigilancia como el respaldo para el proceso del negocio, ya que en el proceso de cosecha este es vigilado mediante cámaras. En donde encontramos la necesidad de tener nuestro sistema funcionando 24/7 por ello se implementó un hardening con la ayuda de un firewall, el mismo que nos permite filtrar el acceso a únicamente al equipo de monitoreo, denegando el acceso al aplicativo de nuestra cámara a otros usuarios, ayudándonos en el control de uso del ancho de banda.

- Adicionalmente nuestro firewall se encuentra vigilando una cámara alterna la cual nos indica el estado de funcionamiento del sistema eléctrico, ya que por las fluctuaciones se inhiben los equipos y podemos realizar una acción de corrección inmediata. De esta manera incrementamos la disponibilidad. La misma que se evaluó en 2 escenarios, sin hardening y con hardening, dándonos como resultado un incremento de disponibilidad de 7.71%.

RECOMENDACIONES

- Se debe realizar un análisis previo del sistema de energía eléctrica que alimenta al sistema de video vigilancia, ya que muchos colapsos del sistema también varían por perdidas de voltaje.

- Incrementa el sistema de respaldo de baterías, el cual podría incrementar un valor porcentual mayor de disponibilidad.

- Se recomienda hacer una metodología de políticas de seguridad para un sistema de video vigilancia, el cual conste de un instructivo de normas de seguridad para cada empresa. El cual incluya reglas de acceso, usuarios, privilegios y manejo de dispositivos.

- Bloquear aplicativo web de la cámara para evitar consumo de recursos.

- Trabajar con un sistema uniforme, para evitar la activación de interoperabilidad ya que este protocolo nos deja una puerta de inseguridad al encontrarse activada para que el dispositivo sea visualizado por otro sistema.

GLOSARIO

Amenaza: Acción consistente en el anuncio de un mal futuro, injusto y aparentemente real, con el fin de intimidar el ánimo de aquel a quien se dirige.

Ataque cibernético: Un ciberataque o ataque informático, es cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo de tomar el control, desestabilizar o dañar un sistema informático (Nahun F, 2018).

Autenticación: La acción de verificar la elegibilidad del usuario para tener acceso a la información. Por lo general diseñada para proteger la actividad de login mal intencionada

Confidencialidad: Se refiere a la protección de información sensible contra divulgación no autorizada

Contraseña: Palabra o cadena de caracteres, normalmente secreta, para acceder a través de una barrera. Se usa como herramienta de seguridad para identificar usuarios de una aplicación, archivo o red. Puede tener la forma de una palabra o frase de carácter alfanumérico y se usa para prevenir accesos no autorizados a información confidencial

Denegación de servicios: es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado. (Europol, 2018)

Disponibilidad: Se refiere a la disponibilidad de la información cuando ésta es requerida para el proceso de negocio ahora y en el futuro

Firewall: Se trata de uno de los métodos usados para proteger una red de intrusiones no autorizadas. Esto se realiza a través de dos mecanismos: uno para bloquear el tráfico de la red, y otro para dejar fluir dicho tráfico, todo esto controlado para evitar accesos no deseados. El firewall da acceso a una maquina en una red local a Internet, pero Internet no ve más allá del firewall.

Hacker: Experto en informática capaz de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones.

Hardware: Es la parte física de un ordenador o sistema informático, está formado por los componentes eléctricos, electrónicos, electromecánicos y mecánicos, tales como circuitos de cables y circuitos de luz, placas, utensilios, cadenas y cualquier otro material, en estado físico, que sea necesario para hacer que el equipo funcione. El término viene del inglés, significa partes duras. (Significados.com, s.f.)

Protocolo: Un protocolo de comunicación está formado por un conjunto de reglas y formatos de mensajes establecidas a priori para que la comunicación entre el emisor y un receptor sea posible ϒ Las reglas definen la forma en que deben de efectuarse las comunicaciones de las redes, incluyendo la temporización, la secuencia, la revisión y la corrección de errores. ϒ Tres elementos clave: Sintaxis (formato de los mensajes: datos + comandos), Semántica (significado de los comandos), Secuenciamiento y temporarización (adecuado de las acciones que se toman respecto de los comandos). (Tolosa, 2014)

Red telemática: La Telemática cubre un campo científico y tecnológico de una considerable amplitud, englobando el estudio, diseño, gestión y aplicación de las redes y servicios de comunicaciones, para el transporte, almacenamiento y procesado de cualquier tipo de información (datos, voz, vídeo, etc.), incluyendo el análisis y diseño de tecnologías y sistemas de conmutación. (Tobar, 2010)

Riesgo: La probabilidad de ocurrencia de una acción o evento adverso

Sistema de Video Vigilancia IP: es una tecnología de vigilancia visual que combina los beneficios analógicos de los tradicionales CCTV (*Circuito Cerrado de Televisión*) con las ventajas digitales de las redes de comunicación IP (Internet Protocol), permitiendo la supervisión local y/o remota de imágenes y audio así como el tratamiento digital de las imágenes, para aplicaciones como el reconocimiento de matrículas o reconocimiento facial, entre otras. (Wikipedia, 2019)

Tecnología: La tecnología es la aplicación coordinada de un conjunto de conocimientos (ciencia) y habilidades (técnica) con el fin de crear una solución (tecnológica) que permita al ser humano satisfacer sus necesidades o resolver sus problemas. (Definición, 2012)

BIBLIOGRAFÍA

© 2010-2022 Dahua Technology Co., Ltd. (2020). *https://www.dahuasecurity.com*. Obtenido de https://www.dahuasecurity.com/la/products/All-Products

Alegre Ramos, M. D. P., & García-Cervigón Hurtado, A. (2011). Seguridad informática. Editorial Paraninfo.

Arcos, E. (2016). El Internet de las Cosas fue usado para el último gran ataque DDoS y no podemos hacer nada para impedirlo. Retrieved from https://hipertextual.com/2016/10/mirai-ddos-internet-cosas

AWS. (12 de octubre de 2021). *d1.awasstatic.com.* Obtenido de d1.awasstatic.com: https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf

Belcic, I. (7 de diciembre de 2021). *Avast*. Obtenido de https://www.avast.com/es-es/c-sql-injection

ESGEEKS. (s.f.). *Esgeeks*. Obtenido de https://esgeeks.com/definicion-ataque-fuerza-bruta/#:~:text=Definici%C3%B3n%20de%20Ataque%20de%20Fuerza%20Bruta%20En%20un,complejos%20algoritmos%3A%20es%20s%C3%B3lo%20un%20juego%20de%20adivinanzas.

Evans, D. (2011). Internet de las cosas. Cómo la próxima evolución de Internet lo cambia todo. Cisco Internet Bussiness Solutions Group-IBSG, 11(1), 4-11.

Fabian. (21 de enero de 2022). *ELADMINIS*. Obtenido de https://eladminis.com/definicion-de-desbordamiento-de-bufer/

García, G. A. (1 de Jan de 2003). *Tabula RASA*. Obtenido de Tabula RASA: https://revistas.unicolmayor.edu.co/index.php/tabularasa/article/view/1687

Hanacek, N. (24 de julio de 2013). *nist.gov*. Obtenido de https://www.nist.gov/industry-impacts/cybersecurity

Harán, J. M. (2019). Nueva variante de la botnet Mirai presenta nuevos exploits y apunta al sector empresarial. Retrieved from https://www.welivesecurity.com/la-es/2019/03/20/nueva-variante-botnet-mirai/

IBM. (14 de 04 de 2021). *IBM Documentacion.* Obtenido de IBM i: https://www.ibm.com/docs/es/i/7.2?topic=concepts-ip-filtering

ISACA. (2012). *cotana.informatica.edu.bo.* Obtenido de cotana.informatica.edu.bo: http://cotana.informatica.edu.bo/downloads/COBIT5-Framework-Spanish.pdf

ISACA. (2012). *www.isaca.org.* Obtenido de www.isaca.org/COBITuse: https://www.academia.edu/14438434/COBIT5_Implementation_Spanish

ISACA. (2013). *www.isaca.org.* Obtenido de www.isaca.org: https://usermanual.wiki/Document/selfassessmentguideusingcobit5resspa0116.1842760980.pdf

iso2700.es. (agosto de 2019). Obtenido de https://www.iso27000.es/iso27002.html

Jiménez, J. (13 de noviembre de 2020). *RZ redes zone*. Obtenido de https://www.redeszone.net/tutoriales/seguridad/evitar-secuestro-sesion/

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.

Kambourakis, G., Kolias, C., & Stavrou, A. (2017, October). The mirai botnet and the iot zombie armies. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM) (pp. 267-272). IEEE.

León, O. G., & Montero, I. (2003). Métodos de investigación en psicología y educación (No. 303.42). McGraw-Hill Interamericana,.

Merchan Carreño, J., & García Marcillo, M. (06 de MAYO de 2021). *http://repositorio.unesum.edu.ec/.* Obtenido de http://repositorio.unesum.edu.ec/: http://repositorio.unesum.edu.ec/handle/53000/2886

Miguel, L. P. (2017). DISEÑO DE PROCEDIMIENTOS DE SEGURIDAD BASADOS EN PRUEBAS DE. San Juan de Pasto, Colombia. Obtenido de https://repository.unad.edu.co/jspui/bitstream/10596/14929/1/1085285379.pdf

OWASP. (abril de 2017). *owasp.org*. Obtenido de owasp.org: https://owasp.org/www-pdf-archive/Est%C3%A1ndar_de_Verificaci%C3%B3n_de_Seguridad_en_Aplicaciones_3.0.1.pdf

owasp.org. (18 de julio de 2018). Obtenido de owasp.org: https://owasp.org/www-pdf-archive/Est%C3%A1ndar_de_Verificaci%C3%B3n_de_Seguridad_en_Aplicaciones_3.0.1.pdf

revistaseguridad360. (21 de enero de 2022). *revistaseguridad360*. Obtenido de revistaseguridad360.com: https://revistaseguridad360.com/destacados/que-es-onvif/

Rodríguez Macías, W. H. (2017). Análisis de las prácticas de innovación en sisitemas de seguridad de las empresas de sector camaronero de la Parroquia Taura provincia del Guayas (Bachelor's thesis, Universidad de Guayaquil Facualtad de Ciencias Administrativas).

Rodriguez, W. (2017). *"ANÁLISIS DE LAS PRÁCTICAS DE INNOVACIÓN EN SISTEMAS DE SEGURIDAD DE LAS EMPRESAS DEL SECTOR CAMARONERO DE LA PARROQUIA TAURA PROVINCIA DEL GUAYAS "*. Universidad de Guayaquil.

Sierra García, C. S. (2017). Propuesta del Sistema de Video Vigilancia en la Seguridad Ciudadana distrito de Pueblo Libre 2016-2020. peru.

(S/f). Owasp.org. Recuperado el 18 de julio de 2022, de https://owasp.org/www-pdf-archive/Est%C3%A1ndar_de_Verificaci%C3%B3n_de_Seguridad_en_Aplicaciones_3.0.1.pdf

(S/f-b). Oas.org. Recuperado el 18 de julio de 2022, de https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Villamar Chamba, G. P. (2018). Análisis y diseño de un sistema de seguridad de video vigilancia sobre IP para una industria de alimentos balanceados.

Tambe, A., Aung, Y. L., Sridharan, R., Ochoa, M., Tippenhauer, N. O., Shabtai, A., & Elovici, Y. (2019). Detection of threats to IoT devices using scalable VPN-forwarded honeypots.

CODASPY 2019 - Proceedings of the 9th ACM Conference on Data and Application Security and Privacy, 85–96. https://doi.org/10.1145/3292006.3300024

Todoelectronica. (22 de diciembre de 2019). Todoelectronica. Obtenido de INTRODUCCIÓN A LA VIDEOVIGILANCIA TIPOS DE CÁMARA DE VIGILANCIA Y SEGURIDAD,: https://www.todoelectronica.com/manuales/tipos_camars_seguridad.pdf

Tomás, E., & Ajanel, T. (2013). Diseño De La Investigación De Metodologías De Desarro Llo Para Integración De Cámaras De Vigilancia a Un Sistema De Gestión De Condominio. *Gestion De Condominios Con Camaras*. Retrieved from http://biblioteca.usac.edu.gt/tesis/08/08_0682_CS.pdf

Tolosa, G. (2014). Protocolos y Modelo OSI. Recuperado de http://www. tyr. unlu. edu. ar/TYR-publica/02-Protocolosy-OSI. pdf.

Zamudio, M. Z. (2020). seguridad informatica. tecnoseguro. https://www.tecnoseguro.com/analisis/seguridad-informatica/axis-practicas-ciberseguridad-proteccion-sistemas-videovigilancia-ip