UNIVERSIDAD DE LA SABANA

Facultad de Ingeniería

Maestría en Gerencia de Ingeniería

Elaboración de un plan de mitigación de riesgos de malware en IoT aplicado a un caso de estudio de una solución de gestión de salas de cirugía utilizando Delphi y simulación.

Chía, 26 de noviembre de 2020

Presentación de trabajos de grado

Protocolos e informes finales

ELABORACIÓN DE UN PLAN DE MITIGACIÓN DE RIESGOS DE MALWARE EN IOT APLICADO A UN CASO DE ESTUDIO DE UNA SOLUCIÓN DE GESTIÓN DE SALAS DE CIRUGÍA UTILIZANDO DELPHI Y SIMULACIÓN

Estudiante

ANDRES MANUEL BALLESTAS VIVAS

Tutor

LUIS CARLOS RABELO MENDIZÁBAL, PHD.

FACULTAD DE INGENIERÍA
MAESTRÍA EN GERENCIA INGENIERÍA
CHÍA, 26 de noviembre de 2020

Tabla de contenido

Índice de tablas

Índice de figuras

1. Introducción

Las revoluciones se han generado a lo largo de nuestra historia cuando tanto la tecnología como las nuevas formas en que las personas percibimos el mundo desencadenan cambios significativos no solo en los sistemas económicos sino también en las estructuras sociales. De los principales retos a los cuales nos enfrentamos hoy en día, uno de los más importantes es cómo entender y darle paso a las diferentes revoluciones que surgen y que significan una transformación de la humanidad. En la actualidad, estamos entrando en la cuarta revolución industrial, una revolución que cambiará esencialmente la forma en la que vivimos, trabajamos y nos conectamos o relacionamos los unos con los otros.

El proceso de los seres humanos para transformar su sociedad se debe en gran medida a su curiosidad por la evolución tecnológica. La cual, durante las últimas décadas, ha permitido a la humanidad cruzar nuevas fronteras en todos los sectores económicos permitiendo realizar trabajos en periodos más cortos y con mayor precisión (Sharma et al., 2019).

Después de la mecanización, electrificación y computación como etapas de la revolución industrial, la civilización vive una cuarta etapa conocida como el Internet de las cosas o IoT, en el cual, Internet se está transformando en un nuevo tipo de hardware y software que lo hace accesible para cualquiera, ya sea persona o industria. Adicionalmente, el Internet de las cosas (IoT) promete un gran futuro para Internet donde el tipo de comunicación es máquina-máquina (R. Khan et al., 2012).

El IoT consta de objetos, dispositivos y sensores, que pueden colocarse en la nube para la toma de decisiones y la ejecución de sistemas basados en acciones (R. Khan et al., 2012). Estos objetos físicos están equipados con sistemas de comunicación que pueden ser detectados por otros dispositivos o sensores inteligentes. Dichos sensores comunican información específica del objeto a través de Internet a computadores o

dispositivos móviles. El resultado del procesamiento se pasa un sistema de toma de decisiones que determina una acción automatizada a invocar. Se puede utilizar una combinación de diferentes sensores para el diseño de servicios inteligentes (R. Khan et al., 2012).

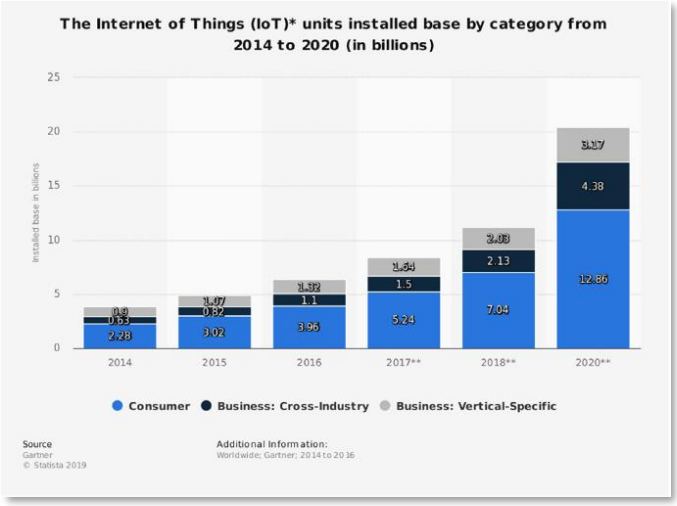


Figura 1. La curva de crecimiento de los dispositivos IoT.

Fuente: (*Internet of Things Units Installed Base by Category 2014-2020 | Statista*)

La (Figura 1) muestra que el número de dispositivos de IoT se está casi duplicando cada dos años, y se espera que llegue a 20 mil millones de dispositivos para este 2020 (Rao & Clarke, 2020).

Los recientes avances en este ámbito aceleran la aparición de plataformas IoT a gran escala. Con ellas se recolecta, procesa y analiza los datos en tiempo real para alimentar al ecosistema de soluciones inteligentes. El uso de esas plataformas como sensores de los objetos que nos rodean supone, en el futuro inmediato, una revolución en la forma de obtener, procesar y analizar información.

Sin embargo, la mayoría de estos dispositivos IoT son fáciles de hackear y comprometer. La mayoría de las veces, permitimos que un hacker tenga acceso por tener contraseñas fáciles de adivinar o porque nunca cambiamos la contraseña predeterminada de nuestro sistema o de los dispositivos IoT (Estrada et al., 2020).

Existen dos causales identificadas en los problemas de seguridad: la diversidad y la comunicación (Zhang et al., 2014). El problema de seguridad para los IoT es creado por las vulnerabilidades producidas en la fase de diseño del programa; Esto crea oportunidades para la instalación de malwares o puertas traseras. Por lo general, estos dispositivos de IoT tienen una capacidad de cómputo, almacenamiento y red limitada y, por lo tanto, son más vulnerables a los ataques que otros dispositivos de punto final, como teléfonos inteligentes, tabletas o computadoras (M. A. Khan & Salah, 2018).

En cuanto al medio de comunicación, el entorno de red para los IoT es heterogéneo. Varios canales de comunicación pueden enfrentar diferentes desafíos de seguridad por lo cual pasar por alto este contexto comprometería la disponibilidad de los dispositivos (Zhang et al., 2014).

El Internet de las cosas (IoT) abre oportunidades para dispositivos portátiles, electrodomésticos y software para compartir y comunicar información en Internet. Dado que los datos compartidos contienen una gran cantidad de información privada, preservar la seguridad de la información en los datos compartidos es un asunto importante que no puede ser descuidado (Zhang et al., 2014).

2. Problema

2.1. Contexto General

La revolución del Internet de las cosas (IoT) no solo ha asumido el reto de interconectar a toda una generación de dispositivos tradicionales, sino también trajo a Internet la amenaza de miles de millones de objetos mal protegidos y fácilmente interceptados (De Donno et al., 2018).

La tecnología del IoT funciona en tres capas: capa de recepción, capa de red y capa de aplicación. La capa de recepción involucra varios tipos de sensores de datos como RFID o Identificador por Radio Frecuencia, códigos de barras o cualquier otra red de sensores (Lan, 2012). El objetivo de esta capa es obtener información del entorno mediante el uso de sensores y luego enviarla a la capa de red la cual tiene como función transmitir los datos recopilados a cualquier sistema de procesamiento de información específico a través de Internet, red móvil o cualquier otro tipo de red confiable con el fin que la capa de aplicación desarrolle un entorno inteligente de la solución que se está buscando (Deogirikar & Vidhate, 2017).

Los objetivos de seguridad típicos de confidencialidad, integridad y disponibilidad también se aplican al IoT. Sin embargo, los IoT tienen más restricciones y limitaciones en términos de componentes, recursos computacionales y de energía (Mahmoud et al., 2016). Descubrir y analizar vulnerabilidades en cada capa en el IoT juega un papel importante en las investigaciones de seguridad actuales. Los tipos de vulnerabilidades encontradas van desde un mal diseño de software, como el uso de contraseñas débiles y codificadas hasta fallas de programación como desbordamientos de búfer e inyección de comandos (Wang et al., 2017).

Esta tendencia de inseguridad ha llevado a la popularidad los ataques distribuidos de denegación de servicio (DDoS). En el momento que la revolución de los IoT lleno a Internet con dispositivos mal protegidos produjo que los ataques fueran más accesibles,

poderosos y complejos y por lo tanto más difíciles de identificar y caracterizar (Peng et al., 2007). De hecho, la difusión de más dispositivos conectados y no seguros que alimentan el mercado ha significado más vectores de ataque y más posibilidades para que los hackers informáticos realicen diversos ataques, accedan a datos sensibles y permitan tomar control de los dispositivos (Hughes, 2016).

Mas aun, la sensibilidad de la información debe ser contextualizada en los casos donde se pudiera alterar, eliminar o suplantar con propósitos diferentes a los propósitos originales, aspectos que abarcaremos más adelante.

2.2. Contexto particular

Las diferentes practicas desarrolladas por los delincuentes informáticos para acceder, corromper y extraer información de sus víctimas, sean personas o empresas, comprenden un sin número de mecanismos que aprovechan las vulnerabilidades humanas y tecnológicas.

Botnet es un término que hace referencia a un conjunto o red de robots informáticos también conocidos como bots, que se ejecutan de manera autónoma y automática. Entre las diversas formas de malware, los botnets se han convertido en la amenaza más grave contra la seguridad cibernética, ya que proporcionan una plataforma distribuida para varias actividades ilegales, como el lanzamiento de ataques distribuidos de denegación de servicio contra objetivos críticos (Frank et al., 2017).

El valor más destacado de los botnets es la capacidad de proporcionar anonimato mediante el uso de una arquitectura de comando y control de varios niveles. Además, los bots individuales no son centralizados por quien los controla, y pueden estar ubicados en varios lugares en todo el mundo. Las diferencias en las zonas horarias, los idiomas y las leyes dificultan el seguimiento de actividades maliciosas de botnets a través de fronteras internacionales (Feily et al., 2009).

A pesar de la larga presencia de los botnets maliciosos, solo unos pocos estudios formales han examinado el problema. Hasta la fecha, se sabe muy poco sobre el comportamiento malicioso de los mismos. La detección y el seguimiento de botnets ha sido un tema de investigación importante en los últimos años. Se han propuesto diferentes soluciones en la academia (Zhaosheng et al., 2008).

Existen principalmente dos enfoques para la detección y el seguimiento. El primero se basa en la creación de redes de miel o señuelo, sin embargo, las redes trampa son principalmente útiles para comprender la tecnología y las características de la red bot, pero no necesariamente detectan la infección (Feily et al., 2009). Por otra parte, el otro enfoque para la detección de botnets se basa en el monitoreo y análisis pasivo del tráfico de red. Las técnicas de detección de botnets basadas en el monitoreo pasivo del tráfico han sido útiles para identificar la existencia de botnets (Feily et al., 2009).

Las vulnerabilidades de los dispositivos IoT son las más utilizadas por las botnets para lanzar una amplia gama de DDoS o ataques distribuidos de denegación de servicio (Angrishi, 2017). La mayoría de los ataques DDoS en los últimos tiempos se originan en 3 tipos de dispositivos, 96% dispositivos IoT, 4% enrutadores domésticos y menos del 1% servidores Linux comprometidos (Angrishi, 2017).

Las botnets IoT no solo afectan a los propietarios de los dispositivos IoT sino también a cualquier persona o compañía relacionada o conectada con los servicios que se disponen en Internet.

Un bot es software en un IoT que ejecuta tareas automáticas que le fueron ordenadas desde Internet, por un lado el dispositivo (IoT) como subsistema de adquisición de datos debe interactuar con el equipo tecnológico, que pueden ser controlados por diferentes sistemas CnC (servidores de Comando y Control, por sus siglas en ingles), tienen diferentes protocolos de transmisión de datos, etc. (Martinov et al., 2020)

En esencia un servidor CnC funciona como sistema que envía un conjunto de órdenes y funciones a un dispositivo de menos capacidad computacional como un IoT, quien las ejecuta a cabalidad y sin objeciones.

2.3. Ubicación del problema

En julio de 1999 se registró el primer ataque de DoS (ataque de denegación de servicio) al interior de la Universidad de Minnesota en Estados Unidos. Durante más de 2 décadas los siguientes ataques se fueron sofisticando y su impacto aumento con el crecimiento de Internet y más dispositivos conectados.

En septiembre de 2016, apareció una nueva amenaza en Internet que lanzó ataques de denegación de servicio contra varios dispositivos. Esta amenaza fue llamada Mirai, y aprovechó las débiles medidas de seguridad en los dispositivos IoT y las utilizó para lanzar ataques DDoS (Eustis, 2019). Se entiende por DDoS (ataque distribuido de denegación de servicio) a la técnica de ataque informático que satura un servicio en Internet. El código fuente de Mirai contenía una lista de 68 combinaciones diferentes de accesos de usuario y contraseña para varios fabricantes de dispositivos IoT. La lista incluía contraseñas predeterminadas para dispositivos tan variados como enrutadores, cámaras de seguridad, impresoras y DVR (Brian Krebs, 2016). El punto crítico se alcanzó a fines de 2016, Mirai logro infectar cientos de miles de dispositivos IoT en línea para luego realizar un ataque DDoS alcanzando una capacidad ofensiva de aproximadamente 1.2 terabits por segundo.

Telnet es uno de los protocolos de gestión de dispositivos más usado para conexiones remotas entre ordenadores, dispositivos y servidores. Telnet es un conjunto de conexiones utilizadas en las redes de área local e Internet para proporcionar comunicación interactiva basada en texto usando una conexión terminal virtual (Vyas & Shrimali, 2017). Usando principalmente para conectarse a un dispositivo y ejecutar comandos.

Mirai es una familia de virus que convierte el dispositivo infectado en bot para ejecutar ataques DDoS. Infecta dispositivos IoT con acceso remoto habilitado a través de telnet y los nombres de usuario y contraseña predeterminados. Mirai se divide en tres partes. El servidor CnC proporciona una terminal virtual para usuarios de botnet, mantiene evidencia de bots registrados y les pasa el comando de ataque. El controlador carga y ejecuta malware en dispositivos vulnerables reportados. El bot busca objetivos vulnerables y ejecuta ataques DoS a pedido (Sinanovic & Mrdovic, 2017). Mirai tiene un doble objetivo, en primera medida propaga la infección a dispositivos mal configurados y ataca un servidor de conexión tan pronto como reciba el comando correspondiente de la persona que controla el bot. El servidor proporciona al controlador una interfaz de administración centralizada para verificar el estado de la botnet y organizar nuevos ataques DDoS (Kolias et al., 2017).

Hoy en día, las mutaciones de Mirai se generan a diario, y el hecho de que puedan seguir proliferando e infligiendo daños reales utilizando los mismos métodos de intrusión que el malware original es indicativo de la negligencia crónica de los proveedores de dispositivos IoT al aplicar incluso prácticas de seguridad básicas (Kolias et al., 2017).

En este contexto, la presencia de malware en cualquier ambiente tecnológico de cualquier sector económico que utilice IoT podría estar en riesgo de ser afectado.

2.4. Planteamiento del problema

Según las estimaciones de Gartner, los dispositivos IoT superarán en número a los humanos 4 a 1 para 2020 (Hung, 2017). Esta expansión tendrá un fuerte efecto económico. Las tecnologías de IoT ofrecen enormes potenciales para los consumidores y la industria. Más precisamente, mejoran la calidad de vida, aumentan la eficiencia operativa y la productividad, permiten decisiones en tiempo real y crean nuevas oportunidades de negocio. Estos beneficios están llevando a un aumento exponencial

de la cantidad de dispositivos conectados que se espera que alcance decenas de miles de millones en los próximos años (Nebbione & Calzarossa, 2020).

El Instituto Global McKinsey predice que las tecnologías IoT podrían tener un impacto económico anual de 3.9 a 11.1 billones de dólares en todo el mundo para 2025 (Bauer et al., 2017).

Aunque todo este crecimiento de elementos y soluciones IoT suena interesante y alentador para el desarrollo y evolución de la raza humana, teniendo en mente que en la actualidad el uso de dispositivos tecnológicos se ha convertido en el común denominador de la vida cotidiana. Surge la siguiente pregunta alrededor de este tema:

¿Es posible elaborar un plan de mitigación de riesgos para una Solución de Gestión de Salas de Cirugía a partir del Análisis de Riesgos, la Metodología Delphi, la Dinámica de Sistemas y la Simulación de Eventos Discretos?

3. Justificación

En la actualidad, el alto número de dispositivos conectados a Internet dedicados a propósitos específicos está demostrando ser una amenaza real para la seguridad de los usuarios y compañías de todo el mundo. Pues si bien hace unos años los creadores de malware se centraban en comprometer computadoras de uso general, ahora se han dado cuenta que los dispositivos IoT tienen un gran papel que jugar (Armiñana Gorriz, 2018).

Las posibilidades son infinitas cuando se trata de IoT y las estadísticas definitivamente lo reflejan. China, América del Norte y Europa occidental constituyen el 67% de la base instalada de IoT. Morgan Stanley predice que el tamaño del mercado de IoT industrial alcanzará los $ 110 mil millones de dólares para 2020. IoT industrial representa más del 17% del número de proyectos de IoT en todo el mundo. El Internet industrial de las cosas a menudo se abrevia como "IIoT" (Ipropertymanagement.com, 2020).

Según cifras de iot-analytics, la mayoría de los proyectos de IoT identificados se encuentran en Smart City, seguidos de entornos industriales y proyectos de IoT de edificios conectados (Figura 2). América conforma la mayoría de esos proyectos (45%), seguida de Europa (35%) y Asia (16%). Existen grandes diferencias cuando se observan segmentos y regiones de IoT individuales. La mayoría de los proyectos de Smart City se ubican en Europa (45%), mientras que América, particularmente Norteamérica, son fuertes en salubridad (55%) y vehículos (54%). La región de Asia / Pacífico es particularmente fuerte en el área de proyectos de agricultura inteligente (31%) (IoT-Analytics, 2019).

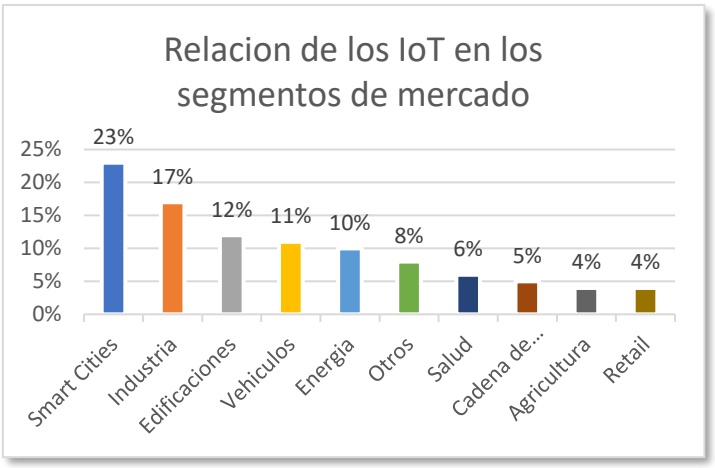


Figura 2. Relación de los IoT en los segmentos de mercado.

Fuente: Adaptado de (IoT-Analytics, 2019).

En el caso colombiano, el país cuenta con el Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IOT) iniciativa impulsada por Min Tic, y Colciencias, los cuales promueven la estrategia que busca posicionar a Colombia como líder regional en TIC. Este centro tiene como misión el desarrollo de productos y servicios innovadores basados en IOT para un mayor bienestar de la sociedad y una mayor competitividad de la economía nacional, adicional también busca el fortalecimiento del ecosistema de innovación y emprendimiento en IOT para la proyección del país a nivel internacional (Molina García, 2019). Las líneas de investigación son presentadas a continuación (Figura 3).

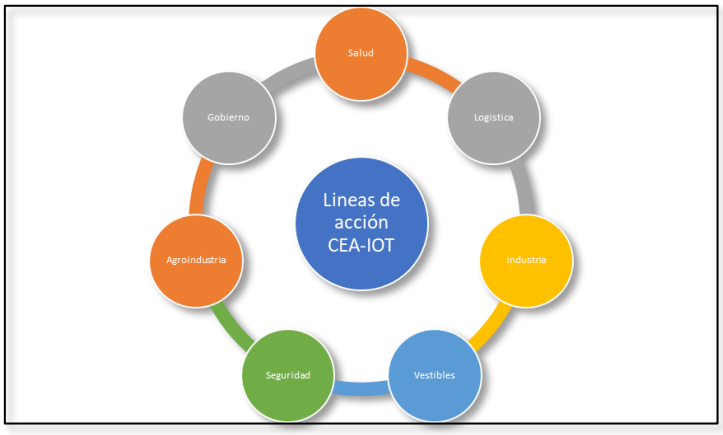


Figura 3. Líneas de investigación y desarrollo CEA-IOT

Fuente: Elaboración propia

Por otra parte, en los últimos años se han realizado estudios con el fin de revelar las debilidades y vulnerabilidades de los dispositivos IoT. Varios actores malintencionados dirigen su atención a las grandes cantidades de dispositivos IoT mal asegurados. Como consecuencia, hay una nueva y gran ola de malware de IoT y las expectativas son que las consecuencias sean más grandes e intensas.

La tendencia del malware IoT es bastante nueva en comparación con los tipos clásicos de malware, y la cantidad de tipologías principales de malware IoT es aún pequeña. Este trabajo trata justamente de lograr la aproximación más cercana para conocer la velocidad de propagación e impacto de malware en dispositivos o soluciones con IoT empleando un modelo de análisis de dinámica de sistemas, los modelos de simulación de eventos discretos y usando la metodología de análisis de riesgos, aplicándolos a un caso de estudio.

4. Objetivos

El objetivo principal de este trabajo es elaborar un Plan de Mitigación de Riesgos de Seguridad en una Solución de Gestión de Salas de Cirugía; partiendo de un Análisis de Malware que pueda afectar los dispositivos IoT, mediante el uso de la Metodología Delphi, la Dinámica de Sistemas y la Simulación de Eventos Discretos. Con el fin de dar alcance al objetivo propuesto están definidos los siguientes objetivos específicos:

4.1. Identificar una tipología de malware que pueda afectar severamente las soluciones de IoT, mediante la realización de un conceso entre expertos y desarrolladores de tecnología contra malware en este tipo de tecnologías a partir de la Metodología Delphi.

4.2. Identificar cual sector económico podría ser más susceptible de ser afectado por malware mediante la contextualización de las amenazas de malware en IoT.

4.3. Identificar el nivel de propagación de un malware en IoT mediante la evaluación en un modelo de simulación usando Dinámica de Sistemas.

4.4. Proponer un Plan de mitigación de Riesgos para la reducción del impacto de un malware en IoT como potencial amenaza para una Solución de Gestión de Salas de Cirugía usando un Modelo de Simulación de Eventos Discretos y un Análisis de Riesgos.

5. Marco Teórico

5.1. Marco conceptual

El Internet de las cosas - IoT puede considerarse una infraestructura de red dinámica y global que gestiona objetos auto configurables de una manera altamente inteligente. Esto, a su vez, permite la interconexión de dispositivos IoT que comparten su información para crear nuevas aplicaciones y servicios que pueden mejorar la vida humana (Shanbhag & Shankarmani, 2015). Originalmente, el concepto de IoT fue introducido por primera vez por Kevin Ashton, fundador del centro de autoidentificación del MIT en 1999. Más tarde, el concepto de IoT fue presentado oficialmente por la Unión Internacional de Telecomunicaciones (UIT) en 2005 (Atlam et al., 2018).

El IoT tiene muchas definiciones sugeridas por muchas organizaciones e investigadores. Sin embargo, la definición proporcionada por la UIT en 2012 es la más común : IoT es "Una infraestructura global para la sociedad de la información, que permite servicios avanzados mediante la interconexión de cosas (físicas y virtuales) basadas en tecnologías de información y comunicación interoperables existentes y en evolución" (ITU, 2012). El propósito básico de Internet de las Cosas es permitir que las cosas se conecten en cualquier momento y en cualquier lugar con cualquier cosa y cualquier persona que use cualquier ruta / red y para cualquier servicio.

Respecto a su estructura, el comité de arquitectura del Foro Mundial de IoT (IWF) lanzó un modelo de referencia de IoT en octubre de 2014 el cual funciona como un marco común para ayudar a la industria a acelerar las implementaciones de IoT. Este modelo de referencia está diseñado con siete capas (Tabla 1) para que cada capa proporcione información adicional para establecer una terminología común. También identifica dónde se optimizan tipos específicos de procesamiento en diferentes niveles del sistema y proporciona el primer paso para permitir a los proveedores crear productos de IoT que sean compatibles y puedan funcionar (Stallings, 2015).

Tabla 1. Capas de arquitectura IoT (basado en Middleware)

No.	Capa IoT	Funcionalidad
7	Colaboración y procesos	Esta capa permite que diferentes aplicaciones de IoT se comuniquen y colaboren entre sí para que los datos de IoT sean más útiles.
6	Aplicación	Esta capa incluye el componente de negocio para el cual está construido el IoT.
5	Abstracción de datos	Esta capa normaliza y da formato a la información almacenada para permitir que sea accesible a las aplicaciones IoT.
4	Almacenamiento	Esta capa es utilizada para el almacenamiento de la información que proviene de diferentes dispositivos IoT.
3	Computacional	Esta capa convierte la data transmitida por red en información ajustada para el almacenamiento y el procesamiento de alto nivel.
2	Conectividad	Esta capa permite que los diferentes dispositivos IoT se comuniquen usando sus respectivos mecanismos de interconexión.
1	Física	Esta capa contiene los dispositivos físicos y controladores que manejan los IoT.

Fuente: Tomado de (Stallings, 2015)

El IoT es una red heterogénea que involucra diferentes dispositivos, como dispositivos electrónicos, dispositivos móviles, equipos industriales y otros. Los diferentes dispositivos pueden tener diferentes plataformas de comunicación, redes, procesamiento de datos, capacidades de almacenamiento de datos y potencia de transmisión (Atlam et al., 2018). Todos estos dispositivos deben conectarse mediante protocolos de red y comunicación que les permitan comunicarse y cooperar juntos para compartir sus datos.

Dado que Internet se extendió inicialmente a través de la comunicación por cable, se podría argumentar que IoT también se puede implementar en la comunicación por cable (Suresh et al., 2014). Pero si consideramos la realidad, la comunicación por cable no se puede lograr en todas partes. La red cableada tiene sus propias desventajas considerando los problemas de movilidad y el costo de instalación. Una alternativa efectiva, de bajo costo y simple para implementar IoT sería el medio inalámbrico. A continuación, se presentan los diferentes medios de transmisión que son utilizados por los IoT (Tabla 2).

Tabla 2. Medios de transmisión utilizados por IoT

Medio	Descripción
Identificación por radiofrecuencia RFID	-(RFID) es una tecnología que utiliza radiofrecuencias para transmitir datos. Este proceso se ejecuta utilizando etiquetas RFID que se implementarían en los puntos respectivos. Estas etiquetas son de dos tipos; Las etiquetas activas son aquellas con una fuente de alimentación interna y las etiquetas pasivas son aquellas sin fuente de alimentación interna. Estas etiquetas se comunican con los lectores RFID. Los receptores RFID responden con una velocidad notable. de menos de 100 milisegundos cada vez. Estas tremendas aplicaciones y ventajas de RFID lo hacen viable para su uso en un entorno IoT.
Wi-Fi	-Es un medio inalámbrico aceptado a nivel mundial que se utiliza para enviar / recibir datos, señales, comandos y mucho más. Funciona en la banda de frecuencia 2.4GHz - 60GHz. Admite velocidades de datos que van desde 1Mb / s a 54Mb / s, pero también se han logrado velocidades de hasta 6,75Gb / s. -La instalación / mantenimiento simple y de bajo costo de dispositivos Wi-Fi ha aumentado su uso a lo largo de los años. Hoy en día es común ver una red Wi-Fi en lugares públicos, escuelas, colegios, hospitales, etc.… Tal alcance para Wi-Fi sería una ventaja adicional para el IoT, que requiere que su red esté extendida en todas partes.
Código de barras	Cualquier producto que esté etiquetado con un código de barras podría identificarse utilizando un lector. Por ejemplo, una cámara de teléfono móvil puede identificar los detalles de un producto utilizando un código QR. Esto permitiría la identificación global de los IoT y además mantendría las especificaciones sobre el mismo. El código de barras sería un adhesivo que se puede pegar en cualquier producto
Bluetooth	Bluetooth es un protocolo de comunicación de corto alcance que se considera el elemento clave para productos portátiles. La nueva versión de Bluetooth que se llama Bluetooth Smart o Bluetooth LowEnergy (BLE) es un protocolo importante para diferentes aplicaciones de IoT, ya que admite un consumo de energía reducido y puede integrarse con teléfonos inteligentes y otros dispositivos móviles.
ZigBee	-El protocolo ZigBee fue inventado por ZigBee Alliance que se basa en el estándar de redes inalámbricas IEEE802.15.4 de baja potencia. El propósito de este protocolo es establecer un estándar que proporcione un protocolo de comunicación de bajo costo para crear redes de área personal (PAN). -ZigBee es el protocolo de comunicación adecuado para aplicaciones que necesitan una velocidad de datos baja, mayor duración de la batería y dispositivos de red seguros.
NFC	Near Field Communication (NFC) es un protocolo de comunicación inalámbrica de muy corto alcance que proporciona un protocolo de comunicación bidireccional simple y seguro entre dispositivos electrónicos, especialmente para teléfonos inteligentes. También permite a los usuarios realizar transacciones de pago sin contacto, acceder a contenido digital y conectar dispositivos electrónicos. Básicamente, NFC facilita la conexión y el control de dispositivos IoT para compartir información a una distancia inferior a 4 cm
Z-wave	Z-Wave es un protocolo de comunicación de radiofrecuencia de baja potencia que se creó principalmente para la automatización del hogar. Proporciona una comunicación confiable y de baja latencia de pequeños paquetes de datos con velocidades de datos de hasta 100 kbits / s. Además, es un protocolo escalable y admite una topología de red de malla completa.

Fuente: Tomado de (Atlam et al., 2018)

La Internet Society proyecta que la IoT crecerá a 100 mil millones de dispositivos para el 2025 (Jerkins, 2017). El IoT tiene la capacidad de conectar objetos cotidianos. Ha introducido varias aplicaciones y servicios inteligentes, que han afectado la vida cotidiana de los usuarios (Figura 4). A continuación se describen los impactos de los IoT en diferentes sectores económicos y productivos (Atlam et al., 2018).

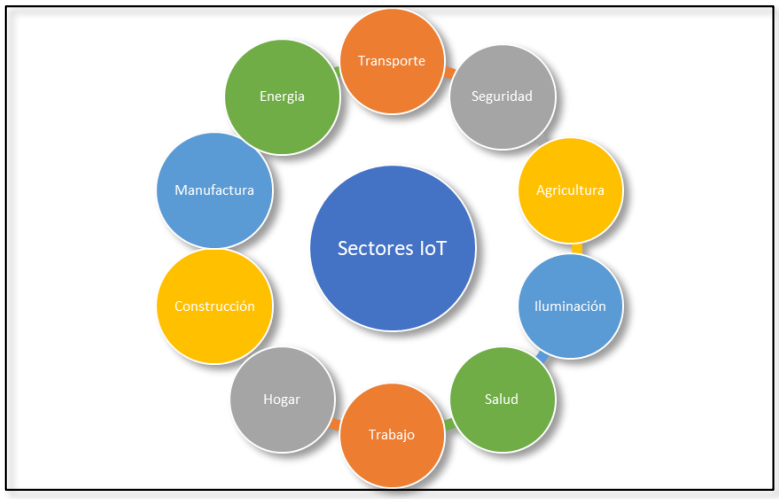


Figura 4. Sectores de implementación IoT

Fuente: Adaptado de (Atlam et al., 2018)

a) Salud: El IoT ha traído muchos beneficios y oportunidades al campo de la atención médica. Ayuda a desarrollar y mejorar los servicios de atención médica y a mantener el campo innovador. Por ejemplo, control inteligente de medicamentos / medicamentos y gestión hospitalaria. Además, el IoT agrega más beneficios al monitorear la salud individual en tiempo real. Además, las ambulancias pueden enviarse de inmediato a las escenas de accidentes y los pacientes pueden ser monitoreados en sus hogares con la misma eficacia que en los hospitales. Por ejemplo, un médico puede ser informado inmediatamente si el paciente sufre un ataque cardíaco y recibir detalles del suceso a través de Internet.

b) Ciudades Inteligentes: El concepto de ciudad inteligente se utiliza para describir el mejor uso de los recursos públicos, aumentar la calidad del servicio

presentado a los ciudadanos y, al mismo tiempo, reducir los costos operativos de las administraciones públicas.

El IoT ofrece varios beneficios en la gestión y optimización de los servicios públicos, como el transporte y el estacionamiento, iluminación, vigilancia y mantenimiento de áreas públicas, preservación del patrimonio cultural y recolección de basura. Además, la disponibilidad de diferentes tipos de datos recopilados por dispositivos IoT se puede utilizar para aumentar la conciencia de las personas sobre el estado de su ciudad y estimular la participación de los ciudadanos en la gestión de la administración pública.

c) Hogar: Actualmente, las personas pueden instalar electrodomésticos inteligentes dentro de sus hogares para controlar muchas de las tareas de la casa. Estos dispositivos inteligentes tienen la opción de un control remoto, lo que elimina la necesidad de estar cerca del dispositivo. Por lo tanto, estos dispositivos han permitido la automatización de las actividades del hogar mediante la adopción de varios dispositivos integrados.

d) Industria: En concepto de industria conectada es la visión de un entorno de fabricación donde cada máquina puede comunicarse con todas las demás máquinas de la planta. Este concepto integrado con IoT conectará, supervisará y controlará prácticamente cualquier cosa, en cualquier lugar para proporcionar productividad operativa y rentabilidad. Además, la integración de IoT con redes de sensores, conectividad inalámbrica, hardware innovador y comunicación de máquina a máquina (M2M) transformará por completo el proceso de automatización convencional de las industrias.

M2M, o máquina a máquina, es una comunicación directa entre dispositivos que utilizan canales de comunicación alámbricos o inalámbricos. M2M se refiere a la interacción de dos o más dispositivos/máquinas que están conectados entre sí. Estos dispositivos capturan datos y los comparten con otros dispositivos

conectados, creando una red inteligente de cosas o sistemas. Los dispositivos pueden ser sensores, actuadores, sistemas empotrados u otros elementos conectados (What Are the Differences Between M2M and IoT | Electronics For You).

e) Retail: Para los minoristas, IoT ofrece oportunidades ilimitadas para aumentar la eficiencia de la cadena de suministro, desarrollar nuevos servicios y remodelar las experiencias del cliente. Por ejemplo, las aplicaciones para el seguimiento de mercancías, el inventario en tiempo real, el intercambio de información entre proveedores y minoristas y las capacidades de entrega automatizadas mejorarán la oferta que el sector lleva a sus clientes.

f) Vehículos: Los automóviles conectados están equipados con acceso a Internet y pueden compartir su acceso con otros, al igual que conectarse a una red inalámbrica en un hogar u oficina. El automóvil conectado se considera la mejor manera de minimizar los accidentes, de modo que un piloto pueda operar el automóvil de forma remota para minimizar los accidentes automovilísticos y reducir los errores humanos. Estos automóviles sin conductor pueden proporcionar funciones más que solo de seguridad, ya que pueden ahorrar tiempo valioso, permitir ejecutar actividades en paralelo a la conducción e incluso reducir el estrés de conducir.

g) Parking: En los últimos tiempos, los sensores inteligentes de estacionamiento están conectados en el espacio de estacionamiento para detectar la llegada y salida de vehículos. Proporciona una solución de gestión eficiente para ayudar a los conductores a ahorrar tiempo y combustible. Proporciona a los conductores la información precisa sobre los espacios de estacionamiento y mantiene el sistema de tráfico sin problemas. También permite reservar antes de llegar al sitio de estacionamiento un espacio directamente desde el vehículo.

h) Energía: El IoT proporciona más información sobre los comportamientos de los proveedores y consumidores de electricidad de forma automatizada para mejorar la eficiencia energética. También proporciona a los consumidores una gestión inteligente del consumo de energía, con medidores inteligentes, electrodomésticos inteligentes y, recursos de energía renovable.

i) Medio ambiente: El elemento clave del sistema IoT son los sensores que recopilan información sobre el entorno circundante. Por lo tanto, con IoT, se puede proporcionar un sistema de información de alta velocidad. Esto permite que la entidad que monitorea los entornos en grandes áreas y los sensores desplegados en dicha área transmitan una gran cantidad de datos fácilmente, como el monitoreo de la fuente de contaminación, el monitoreo de la calidad del agua, el monitoreo de la calidad y humedad del aire, nivel de radiación solar, temperatura y, indicadores de radiación ultravioleta, entre otros.

j) Agricultura: Con la presencia de sensores en todas partes, los agricultores pueden usar la enorme información recopilada para obtener un mejor retorno de la inversión. Detectar la humedad del suelo y los nutrientes, controlar el uso del agua para el crecimiento de las plantas y determinar los fertilizantes personalizados son algunos de los usos simples de IoT en la agricultura. Además, se utilizaron muchas tecnologías inalámbricas en la agricultura, como la teledetección, el sistema de posicionamiento global (GPS) y el sistema de información geográfica (GIS). Esto a su vez reemplazará el trabajo humano con maquinaria automática que aumentará la productividad.

La seguridad es un problema alarmante en relación con la industria de IoT. Ningún sistema informático es 100% seguro y lo suficientemente maduro contra amenazas de seguridad. Dado que es probable que miles de millones de dispositivos se conecten a Internet en los próximos años, es necesario abordar las amenazas de seguridad. La integridad de los datos y los problemas de compatibilidad derribarían las economías de todo el mercado mundial si no se defendieran. Por ejemplo, todo lo que se ponga en

Internet permanecerá durante mucho tiempo (a veces para siempre). Esto podría afectar las normas de privacidad de individuos y organizaciones (Suresh et al., 2014).

Para afrontar este problema, entidades colegiadas y empresas privadas han definido un marco de referencia para la seguridad de los IoT, este marco está compuesto por los siguientes niveles (Stallings, 2015):

i. Objetos inteligentes y sistemas integrados: Este nivel consta de sensores, actuadores y otros sistemas integrados en la red de borde o periférica. Este es nivel de un IoT más vulnerable. Es posible que los dispositivos no estén en un entorno físicamente seguro y que necesiten funcionar durante tiempo prolongado. Además, los administradores de red deben preocuparse por la autenticidad e integridad de los datos generados por los sensores y por proteger a los actuadores y otros dispositivos inteligentes del uso no autorizado.

ii. Red Fog y Edge: Este nivel se refiere a la interconexión por cable e inalámbrica de dispositivos IoT. Además, se puede realizar una cierta cantidad de procesamiento y consolidación de datos a este nivel. Una preocupación clave es la gran variedad de tecnologías y protocolos de red que utilizan los diversos dispositivos de IoT y la necesidad de desarrollar y aplicar una política de seguridad uniforme frente a un ambiente muy heterogéneo.

iii. Red central: El nivel de red central proporciona rutas de datos entre las plataformas del centro de red y los dispositivos IoT. Los problemas de seguridad aquí son los que se enfrentan en las redes centrales tradicionales. Sin embargo, la gran cantidad de puntos finales para interactuar y gestionar, crean una carga de seguridad y volumen sustancial.

iv. Centro de datos / nube: Este nivel contiene la aplicación, el almacenamiento de datos y las plataformas de administración de red. IoT no introduce ningún

problema de seguridad nuevo en este nivel, aparte de la necesidad de lidiar con un gran número de puntos finales individuales.

A su vez estos niveles pueden estar afectados por diferentes vulnerabilidades y amenazas. Estas se resumen en la (Tabla 3). En esta tabla, las vulnerabilidades de IoT se clasifican en 6 grupos. Adicionalmente, se presentan las amenazas principales asociadas a dichas vulnerabilidades y se presentan las contramedidas que se deben tomar contra estas amenazas.

Tabla 3. Vulnerabilidades, amenazas y medidas en IoT

Vulnerabilidad	Amenaza	Medidas de mitigación
Insuficientes mecanismos de autenticación / autorización.	Acceso no autorizado o de alto nivel a los datos o al dispositivo. Inyección SQL. CSRF - Falsificación de petición en sitios cruzados.	-Cambiar las credenciales de usuario predeterminados durante la configuración inicial. -Hay que asegurar que la interfaz web no sea sensible a XSS, SQLi o CSRF. -Proporcionar el uso de contraseñas seguras. -Garantizar que las credenciales estén debidamente protegidas. -Aplicar autenticación de dos factores si es requerido. -Garantizar que solo los puertos necesarios estén expuestos y disponibles.
No son utilizadas técnicas de criptografía adecuadas.	Sniffing de datos. MITM - Ataque de intermediario (*Man in the middle*). Ataque Sybil.	-Usar otras técnicas de encriptación estándar de la industria para proteger los datos durante la migración si las tecnologías SSL o TLS no están disponibles. -Usar los estándares de cifrado aceptados y evitar los protocolos de cifrado especiales. -Cifrar de forma segura los datos recopilados en alguna transacción. -Garantizar IPSec (Protocolo de Seguridad de Internet).
Ciberataques	Denegación de servicio DoS. Código malicioso. Suplantación de identidad.	-Promover el uso de antivirus y firewall eficaces. -Utilizar el cifrado de datos. -Realizar la ejecución de autenticación, autorización e implementar mecanismos de control de acceso. -Asegurar el buen funcionamiento del IPS (Sistema de Prevención de Intrusos) e IDS (Sistema de Detección de Intrusos).
Privacidad	Recolección de información personal innecesaria. Falta de protección adecuada de los datos.	-Recopilar solo los datos que son críticos para la funcionalidad del dispositivo. -Cifrar de forma segura los datos recopilados. -Realizar una protección correcta del dispositivo y todos sus componentes.
Problemas relacionados con el software / firmware	Problemas en actualizaciones. El firmware contiene información confidencial.	-Permitir las actualizaciones al dispositivo. -Cifrar el archivo de actualización utilizando métodos de cifrado aceptados y transmitirlo a través de una conexión cifrada. -Garantizar que el firmware no incluya información susceptible.

Vulnerabilidad	Amenaza	Medidas de mitigación
Factores humanos	No acatar las reglas de gestión de seguridad. Ingeniería social. Fraude de correo electrónico. Falsificación web. Secuestro de sesión. Phishing. Spam.	-Examinar y controlar las prácticas y reglas de seguridad para desarrollar una documentación de política de seguridad efectiva. -Organizar actividades y programas educativos de sensibilización. -Garantizar el uso de antivirus y firewall eficaces. -Garantizar el uso de contraseña de un solo uso y algoritmo de cifrado.

Fuente: Tomado de (Makalesi et al., 2019)

El malware es la amenaza más grave para los dispositivos IoT, que puede destruir el dispositivo o, en algunos casos, puede cambiar el sistema a un estado privilegiado bajo la autoridad del atacante (Tabla 4) (Milosevic et al., 2017).

Tabla 4. Tipología de malware más comunes

Malware	Definición
Rootkits	Los rootkits son un tipo de malware que puede acceder a partes de software para las cuales regularmente no se tienen privilegios. El acceso al área privilegiada generalmente se habilita mediante un ataque al sistema, ya sea explotando vulnerabilidades del sistema o adivinando las contraseñas del usuario. Una vez que el atacante tiene acceso a los privilegios de raíz del sistema, el sistema está prácticamente bajo su control total y es propenso a una mayor manipulación. Debido a esto, la detección de rootkits es una tarea desafiante, y a veces la única forma de lidiar con esto es reemplazando el sistema operativo.
Ramsomware	El ransomware es un malware que bloquea el acceso al dispositivo del usuario y luego le pide que pague dinero, rescate, para permitir el uso normal. Existen diferentes formas de realizar dicho ataque al sistema, comenzando por bloquear la pantalla de un dispositivo o mediante el uso de un software antivirus falso que, una vez instalado en el dispositivo del usuario, generaría el mensaje de que el dispositivo está bajo ataque y solicitará dinero para eliminar la infección descubierta.
Bots	Los bots son malware de propagación automática con el objetivo de infectar la máquina host y luego conectarse a un servidor, bot master y seguir las órdenes obtenidas de él. Botnet es una red que consta de muchos dispositivos host infectados con bots, que está disponible para realizar ataques de denegación de servicio, enviar mensajes de spam o simplemente habilitar nuevas infecciones en los dispositivos host. Además, los bots recopilan información de los dispositivos host y la envían al bot master. La información recopilada puede estar relacionada con datos de usuarios privados, transacciones financieras, contraseñas de usuarios, etc.
Bombas lógicas	Las bombas lógicas son piezas de código insertadas intencionalmente en un sistema de software que activan una función maliciosa solo cuando se cumplen las condiciones especificadas. Cuando se activa, una bomba lógica puede realizar diferentes acciones: mostrar mensajes de spam, eliminar o corromper datos, ejecutar fragmentos de código malicioso o tener otros efectos no deseados.
Virus	Los virus son un tipo de malware que se propaga al insertarse en otro programa y propagarse junto con él. El nivel de gravedad de los virus puede variar de bajo, por ejemplo, corromper algunos archivos en el sistema, a muy grave que puede deshabilitar y dañar por completo el sistema operativo. Los virus se propagan

Malware	Definición
	junto con el programa al que están conectados. Puede suceder mediante el uso de redes Wi-Fi, Bluetooth, mensajes o archivos adjuntos de correo electrónico.
Gusanos	Los gusanos, a diferencia de los virus que dependen de un programa huésped para propagarse, operan de manera más independiente de otros archivos. Aun así, al igual que los virus, pueden auto replicarse y propagarse. En los dispositivos móviles, los gusanos se propagan sin el conocimiento del usuario, mediante el uso de canales de comunicación existentes: SMS, MMS y Bluetooth.
Troyanos	Los troyanos son un tipo de malware que aparece como un software legítimo, pero en realidad tiene intenciones maliciosas. Además, pueden abrir una puerta trasera en un sistema, lo que permite más ataques. Debido a su similitud con aplicaciones legítimas, la detección de troyanos es una tarea difícil.

Fuente: Tomado de (Milosevic et al., 2017)

Por otra parte, cuando se habla de malware en hardware, los atacantes han encontrado formas de actuar a nivel de chip, que es la parte integral de un sistema. Mediante el uso de varios métodos, un dispositivo o un sistema pueden quedar expuestos. Las modificaciones menores a un chip pueden ser la causa de numerosos ataques (Sklavos, 2017). Uno de los métodos más prácticos para comprometer la seguridad del dispositivo es mediante el uso de ataques de canal lateral - SCA.

Estos ataques tienen un objetivo común, recuperar información de las señales de salida, durante las operaciones del dispositivo. Esta información, junto con los cálculos apropiados, puede llevar a la recuperación de la clave secreta por el atacante. Los ataques de canal lateral se dividen en pasivos y activos. Los ataques pasivos están orientados principalmente a la recopilación de información. En este contexto, un ataque pasivo de canal lateral presupone la acción de recopilar información útil durante el proceso de operación. Por otro lado, aparte del proceso de recopilación de información, los ataques activos son más dinámicos, por lo que un atacante puede recuperar las claves secretas mediante la inyección de fallas en una operación normal (Bechtsoudis & Sklavos, 2010).

Cuando un ataque sucede, sin importar si es a nivel de hardware o software, requiere la realización de un análisis forense. El análisis forense de IoT consiste en una combinación de tres esquemas de análisis forense digital: análisis forense en la nube, análisis forense a nivel de dispositivo y análisis forense en red (Zawoad & Hasan, 2015).

a. Nivel de dispositivo: Este se realiza cuando un investigador puede necesitar recopilar datos de los dispositivos IoT, específicamente en su memoria local. El esquema forense a nivel de dispositivo se emplea cuando existe la necesidad de recopilar, de los dispositivos IoT, una evidencia vital.

b. Análisis de la red: Al utilizar los registros de la red, es imposible identificar las fuentes de los diferentes ataques. Como tal, los registros de red pueden servir como una herramienta crucial cuando se trata de declarar que un sospechoso es culpable o no.

c. Análisis de la nube: Entre los roles más cruciales en el área de análisis forense de IoT se encuentran los análisis forenses en la nube. Como la mayoría de los dispositivos IoT se caracterizan por un bajo almacenamiento y capacidad computacional, los datos generados desde dichos dispositivos IoT y las redes IoT se almacenan en la nube y de hecho se tratan en la nube. Esto se debe al hecho de que las soluciones en la nube brindan numerosos beneficios, como capacidad sustancial, escalabilidad y accesibilidad bajo demanda.

Independiente de esquema que se seleccione, y entendiendo que no hay un único procedimiento forense para efectuar dentro de las investigaciones digitales, numerosos profesionales en investigadores han alcanzado un consenso de las actividades más comunes a realizar (Alenezi et al., 2019):

a) Evaluación: Los examinadores que se especializan en informática forense deben analizar la evidencia digital rigurosamente en relación con el alcance del caso de investigación para decidir qué acción se debe tomar.

b) Adquisición: La naturaleza misma de la evidencia digital significa que es delicada y puede cambiarse, dañarse o destruirse si se maneja o examina de manera incorrecta. De hecho, la mejor práctica es examinar una copia de la

evidencia original. Dicha evidencia original debe obtenerse de manera que proteja y conserve la integridad de esta.

c) Examen: El proceso de examen busca extraer y evaluar evidencia digital. La extracción es simplemente la recuperación de datos de sus respectivos medios.

d) Análisis: Se refiere a los datos recuperados, específicamente interpretando y presentando dichos datos en un formato que sea útil y que tenga sentido.

e) Documentación e informes: Las observaciones y acciones deben documentarse durante cada etapa del procesamiento forense de la evidencia encontrada. Esto culminará en la compilación de un informe que detallará los hallazgos por escrito.

El aumento continuo de malware asociado con dispositivos IoT ha aumentado la necesidad de métodos de detección y protección estables y eficientes. En algunos casos, los números han demostrado que los métodos actuales de detección y protección no son lo suficientemente eficientes (Milosevic et al., 2017). Los métodos principales de detección de malware se dividen en dos (2) categorías: detección basada en firmas y detección basada en comportamiento.

En la (Figura 5) se muestran las técnicas de detección que pueden puede emplear uno de los tres enfoques diferentes: estático, dinámico o híbrido (Idika & A.P.Mathur, 2007).

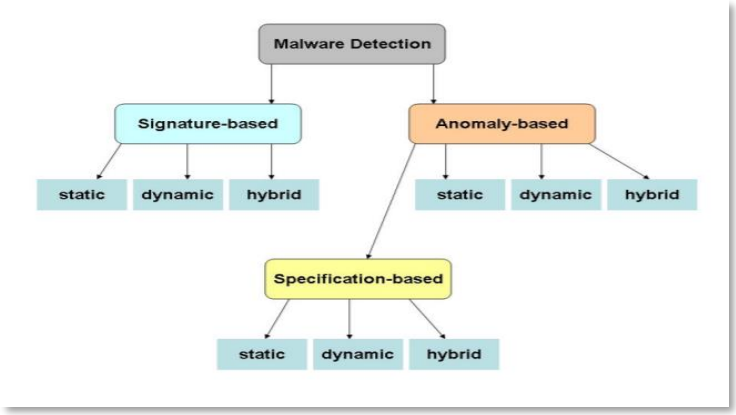


Figura 5. Una clasificación de las técnicas de detección de malware

Fuente: Tomado de (Idika & A.P.Mathur, 2007)

El sistema basado en firmas encuentra interrupciones utilizando una lista predefinida de ataques previamente identificados. A pesar de que esta forma de detección tiene la capacidad de identificar malware de diversa índole, requiere una revisión constante de la base de datos de firmware predefinido. Por otra parte, el sistema basado en comportamiento realiza la ejecución de una muestra en una situación de espacio aislado y los resultados de la ejecución se verifican y registran (Souri & Hosseini, 2018). A continuación, se presentan las principales ventajas y desventajas de los métodos (Tabla 5).

Tabla 5. Ventajas y desventajas de métodos de detección de malware

Método	Ventajas	Desventajas
Basado en firmas	-Facilidad en la ejecución -Identificación rápida -Método ampliamente accesible -Posibilidad de encontrar información completa sobre malware	-No puede identificar los malware polimórficos -Dificultad en replicar información en la enorme base de datos
Basado en Heurística	-Posibilidad de identificación de malware polimórficos -Cálculo de amenaza basado en malware conocido	-El cálculo de amenazas se basa en las firmas que el dispositivo conozca
Basado en comportamiento	-Posibilidad de detectar tipos de ataques de malware no conocidos -Detector de dependencia de flujo de datos -Detecta los malwares polimórficos	-Complejidad de almacenamiento para patrones de comportamiento -Complejidad de tiempo
Basado en Aprendizaje de Maquina	-Conocimiento de los métodos empleados por procesos de confianza	-Puede generar grandes cantidades de falsos positivos en caso de que el

Método	Ventajas	Desventajas
	para detección de procesos maliciosos o abuso de procesos benignos -Empleo de técnicas de aprendizaje comportamental de procesos para detección de amenazas desconocidas	método de aprendizaje no esté ajustado correctamente
Basado en Inteligencia Artificial	-Permite obtener mayor precisión en la detección -Permite predecir e identificar futuras amenazas ya que se basa en Frameworks de seguridad tales como MITRE ATT&CK	-Requiere grandes cantidades de variables y datos que debe computar y comparar
Basado en Consultas a Nubes de Reputación	-Permite anticiparse a la presencia de amenazas que han sido identificadas por otros sistemas -Permite estructurar una base de datos de amenazas basados en su reputación y nivel de riesgo	-Requiere la participación de sistemas a nivel global -Requiere de consulta permanente a los servicios en la nube

Fuente: Tomado de (Souri & Hosseini, 2018) y McAfee

Si hacemos referencia a los métodos que detección en dispositivos móviles (celulares) podríamos decir que se han propuesto diferentes enfoques estáticos y dinámicos para extraer información representativa del comportamiento de las aplicaciones en un dispositivo Android. La información extraída puede utilizarse para definir modelos capaces de distinguir entre aplicaciones benignas y maliciosas e identificar su clase de pertenencia. El análisis estático analiza el código desensamblado sin la ejecución de la aplicación, con el fin de capturar la información sintáctica y semántica, explotando las secuencias extraídas del API (Application Programming Interface por sus siglas en inglés, es un conjunto de funciones y procedimientos para la interconexión de programas), el gráfico de llamadas y los opcodes (instrucciones en lenguaje de maquina), útiles para inferir una base de datos de firmas necesarias para identificar ataques conocidos.

De otra mano, el análisis se ve afectado por el uso de técnicas de ofuscación y codificación. Además, no puede detectar el código malicioso cargado dinámicamente. Los enfoques de análisis dinámico supervisan los comportamientos y acciones realizados por las aplicaciones durante su ejecución en entornos virtuales, incluidas las llamadas al sistema, la actividad de la red, las operaciones de archivo y la modificación de los registros, pero es muy costoso desde el punto de vista informático.

Varios autores han propuesto métodos de análisis dinámico, explotando la secuencia y/o frecuencia de las llamadas a la API realizadas por una aplicación, con el fin de modelar el comportamiento de esta. Estos métodos parten de la base de que los programas maliciosos pueden utilizar diferentes llamadas en un orden diferente con respecto a las aplicaciones benignas, y que las llamadas a la API sensibles pueden ser invocadas con mayor frecuencia en las aplicaciones maliciosas. Por otro lado, las llamadas a la API más sensible constituyen sólo una pequeña parte de todas las llamadas a la API del Android (Ficco, 2019).

5.2. Estado del arte

El objetivo principal del estado del arte es identificar las principales amenazas de seguridad, vulnerabilidades, impactos y escenarios de ataque que afectan los dispositivos y redes de IoT en los últimos años, tomando los diferentes niveles de importancia y criticidad que diferentes agencias y empresas expertas en seguridad proporcionan anualmente.

El número de amenazas de seguridad dirigidas a dispositivos IoT ha aumentado en los últimos años. La (Tabla 6) ilustra algunos de los principales incidentes de seguridad de IoT que se han descubierto o han tenido lugar desde 2009, cabe señalar que esta lista no es exhaustiva, incluye solo los casos más relevantes.

Tabla 6. Línea de tiempo de algunos incidentes de ciber seguridad entre 2009-2018

Año	Incidente de seguridad
2009	-Hackeo de los medidores inteligentes de servicios públicos en Puerto Rico (USA). - Distribución de Stuxnet, el cual es un gusano informático altamente sofisticado diseñado para cazar maquinas específicas utilizada en la industria nuclear.
2013	-Intrusión a cámara de cuidados de bebes. El atacante tuvo oportunidad de controlar audio y micrófono -Violación de datos a Target™. Los atacantes quebraron la red a través de los IoT de climatización de las superficies.
2015	-Identificación de vulnerabilidades de los BMW Connected Drive (Ambiente controlado). Investigadores fueron capaces de imitar servidores de BMW para enviar instrucciones de desbloqueo remoto a vehículos.

Año	Incidente de seguridad
	-Secuestro remoto de vehículo Jeep (Ambiente controlado). A partir de un escenario de hacking ético fue posible obtener total control remoto sobre un vehículo Jeep -Hacking al sistema de mirilla del rifle de asalto TrackingPoint™ (Ambiente controlado). A partir de un escenario de hacking ético fue posible detectar vulnerabilidades del dispositivo vía Wi-Fi.
2016	-Ataque de DDoS al proveedor de hosting OVH a partir del botnet Mirai -Ataque de DDoS al portal de seguridad Krebs a partir del botnet Mirai -Distribución en la red del gusano Hajime el cual fue lanzado para bloquear los ataques de Mirai -Ataque de DDoS al proveedor de DNS Dyn a partir del botnet Mirai -Ataque de DDoS a la red de telecomunicaciones alemana Deutsche Telekom a partir del botnet Mirai -Filtración de la base de datos de la empresa de juguetes Cloudpets
2017	-Hacking al sistema de seguridad de habitaciones del hotel Jägerwirt en Austria -Falla de seguridad de la empresa de juguetes Cloudpets y Carla. -Distribución en la red del botnet Brickerbot el cual deshabilita el funcionamiento de dispositivos IoT con deficiencias de seguridad
2018	-El software de seguridad de dispositivos LoJack, fue hackeado por el grupo de espionaje cibernético "Fancy Bear". -Una demo de producto no segura de la firma de datos de geolocalización LocationSmart permitió a cualquier usuario buscar la ubicación de cualquier teléfono móvil sin necesidad de proporcionar una contraseña o cualquier otra credencial para cualquier teléfono en los cuatro principales operadores de Estados Unidos. -500 millones de consumidores, desde 2014, vieron comprometida su información en la violación de datos del Marriott-Starwood hecha pública en 2018.

Fuente: Tomado de (ENISA, 2017)

Los atacantes utilizan las amenazas caracterizadas para causar efectos en cascada a diferentes niveles en las infraestructuras de gobierno, empresas y hogares. Varias compañías relacionadas con la seguridad digital realizan diferentes investigaciones para determinar el estado del arte de las amenazas y afectaciones en toda la cadena tecnológica de estos sectores. Adicionalmente, el mejor lugar para comenzar el análisis de los hallazgos es examinar las amenazas percibidas por los ejecutivos a cargo de infraestructura crítica.

En los Estados Unidos, el Departamento de Seguridad Nacional o DHS por sus siglas en Ingles, incluye 16 sectores, cuyos activos, sistemas y redes, ya sean físicos o virtuales, se consideran tan vitales que su incapacidad o destrucción tendrían un efecto debilitante en la economía, salud pública y seguridad (Homeland Security, 2003). Según un reporte de Newsweek, a partir de un sondeo a 415 ejecutivos encuestados se

determinó los sectores con mayor criticidad en caso de amenaza por seguridad. La priorización puede verse en la siguiente ilustración (Figura 6).

Gemalto, en su reporte anual 2019-2020 realizó una encuesta a 950 responsables de la toma de decisiones de TI y negocios a nivel mundial, Gemalto descubrió que cuatro de cada cinco empresas (79%) piden a los gobiernos que intervengan en materia de seguridad, más de la mitad (59%) pide lineamientos y políticas más sólidas sobre la seguridad de IoT. De hecho, la mayoría (95%) de las empresas cree que debería haber regulaciones vigentes, un hallazgo que se replica también por los consumidores (95%) los cuales esperan que los dispositivos IoT se rijan por las regulaciones de seguridad establecidas por los gobiernos (Gemalto, 2019).

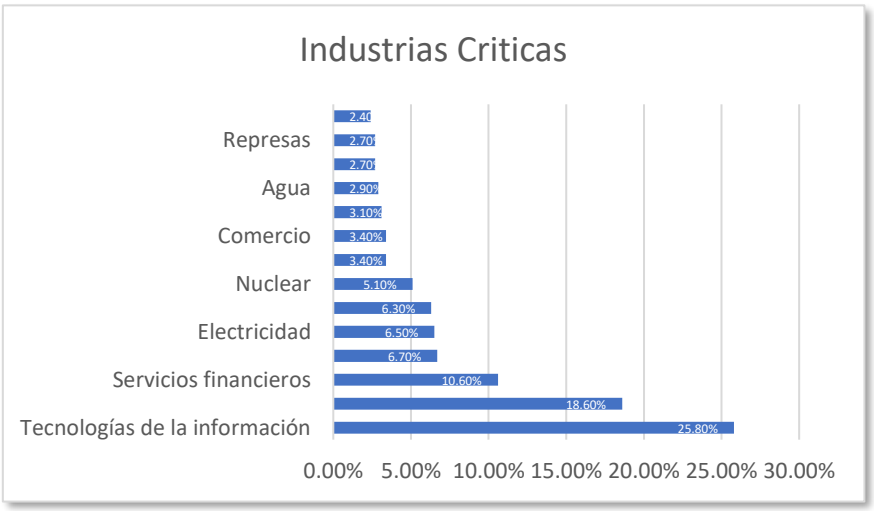


Figura 6. Industrias más impactadas por amenazas IoT

Fuente: Tomado de (Newsweek, 2020)

Dada la penetración cada vez mayor de IoT en todo el espectro de actividades diarias e infraestructuras críticas, la ocurrencia de incidentes de ciberseguridad tiene una tasa en aumento. Las amenazas continúan evolucionando y apuntan a los dispositivos IoT con nuevas técnicas (Figura 7), para 2020 es posible identificar estas amenazas en tres principales categorías: Exploits o agujeros de seguridad, Practicas relacionadas con el Usuario y Malware (Palo Alto, 2020).

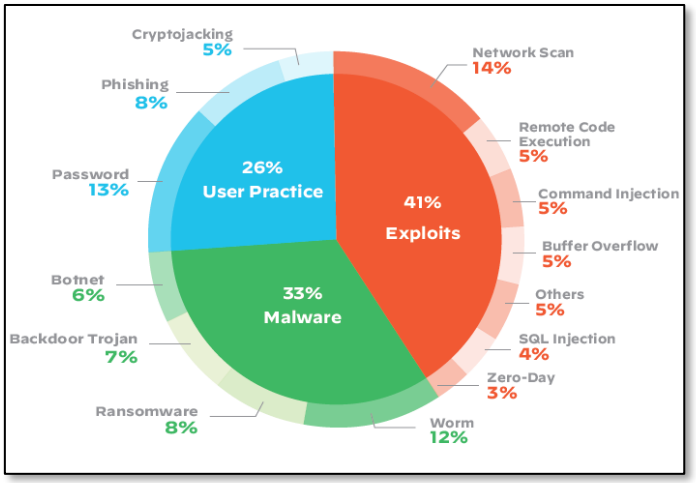


Figura 7. Desglose de las amenazas en IoT

Fuente: Basado en (Palo Alto, 2020)

- Exploits o vulnerabilidades identificadas en dispositivos: Si bien las políticas de seguridad de los dispositivos IoT los convierten en objetivos fáciles, en la mayoría de los casos, los dispositivos solo se usan como peldaños en una estrategia macro para atacar otros sistemas en una red. Las compañías de seguridad están viendo una gran cantidad de escaneos de red, de IPs, de puertos y de vulnerabilidad en redes, intentando identificar otros dispositivos y sistemas, buscando objetivos más grandes.

- Ataques de contraseña: Las contraseñas predeterminadas establecidas por los fabricantes y las prácticas de seguridad de contraseña deficientes continúan alimentando ataques relacionados con contraseña en dispositivos IoT. Hoy en día legislaciones regulatorias en materia de IoT como la SB-327 de California la cual prohíbe el uso de credenciales predeterminadas, permite una paulatina mitigación de la amenaza.

- Los gusanos IoT se están volviendo más comunes que las botnets IoT: Compañías expertas en seguridad observan un cambio desde el modus operandi de los atacantes (ejecutar botnets para realizar ataques distribuidos de denegación de servicio (DDoS) a través de dispositivos IoT) hacia el malware

que se propaga por la red a través de características similares a gusanos, lo que permite a los atacantes ejecutar código malicioso para realizar una gran variedad de nuevos y más complejos ataques.

6. Metodología

Para desarrollar adecuadamente la investigación propuesta, a continuación, se proponen las siguientes fases a desarrollar (Tabla 7):

Tabla 7. Metodología propuesta

Objetivo	Fase / Descripción	Actividades
1 Identificar la tipología de malware en IoT a través de consenso	En esta fase se espera realizar un consenso a través de un panel de expertos con el fin de identificar una tipología de malware a través de la Metodología Delphi para realizar el modelo de propagación.	-Establecer los perfiles del panel de expertos. -Establecer los criterios de ponderación. -Realizar las iteraciones para la selección -Realizar la caracterización de los malware encontrados
2 Sectores económicos y vulnerabilidades	En esta fase se espera elaborar una contextualización de 3 sectores económicos con uso de IoT y sus potenciales vulnerabilidades	-Realizar una definición de los 3 sectores con uso común de IoT. -Identificación de las potenciales vulnerabilidades encontradas en los 3 sectores. -Seleccionar un sector económico y un caso de estudio de Solución de Gestión de Salas de cirugía.
3 Elaborar los modelos de propagación de malware en IoT	En esta fase se realizarán varios modelos de propagación de malware en dispositivos IoT, el cual permitirá determinar la similitud de propagación del malware identificado en el Delphi	-Determinar los mecanismos de propagación empleados mediante los vectores de análisis de la investigación. -Desarrollar modelos de propagación en Dinámica de Sistemas -Adaptar el modelo de propagación a los Modelos de Simulación de Eventos Discretos al caso de estudio.
4 Realizar un análisis de riesgos para el caso de estudio	En esta fase se analizarán los riesgos asociados a una posible afectación en una solución de gestión de salas de cirugía	- Elaboración de las matrices de identificación, clasificación, priorización, impacto y probabilidad de riesgos -Elaboración de la matriz de riesgos para una solución de gestión de salas de cirugía.
5 Elaborar un plan de mitigación de riesgos para el caso de estudio	En la última fase se elaborará un plan de mitigación de riesgos para una solución de gestión de salas de cirugía	-Usar los hallazgos del Análisis de Riesgos, La Metodología Delphi, El Modelo de Dinámica de Sistemas y la Simulación de Eventos Discretos para desarrollar un plan de mitigación de riesgos para una solución de gestión de salas de cirugía.

Fuente: Elaboración propia

7. Desarrollo

7.1. Delphi

El Método Delphi, originado en la década de 1960, es una técnica utilizada para ayudar a construir escenarios presentes y futuros centrados en cuestiones puntuales con la ayuda de expertos en un tema específico. El método permite a alcanzar un consenso entre los participantes basado en todas las opiniones publicadas de diferentes experiencias y puntos de vista para construir un escenario común (Renzi & Freitas, 2015).

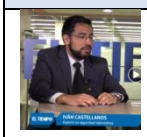
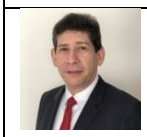
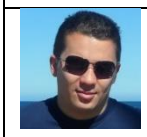
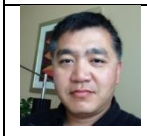
Entre los diseños de investigación de disertación típicos, el Método Delphi es un diseño particular que está ganando aceptación. Esta metodología permite el uso de un panel de expertos para lograr un consenso en la resolución de un problema, decidir el curso de acción más apropiado, o establecer la causalidad donde no existía ninguna anteriormente, particularmente en áreas de investigación empresarial o educativa. (Avella, 2016). El objetivo del método es llegar a un consenso entre los especialistas sobre un tema específico para crear un escenario. Es importante que cada participante no conozca la identidad de otros especialistas durante los procedimientos del método con el propósito de mantener las opiniones completamente formales e impersonales (Renzi & Freitas, 2015).

Para este proyecto, todo contacto y recolección de opiniones se produjo por correo electrónico, centralizado desde una sola cuenta. El uso del correo electrónico facilitó llegar a los 9 expertos ubicados geográficamente en diferentes locaciones. Aunque los expertos son de países diferentes, las preguntas se elaboraron en inglés. Todas las respuestas y opiniones de los especialistas fueron traducidas al español con el fin de ser plasmadas en este documento.

7.1.1. Selección del panel de expertos

La clave del éxito reside en los participantes, ya que los resultados del método dependen directamente del conocimiento de los especialistas sobre el tema y la cooperación entre todos los involucrados. Es esencial incluir personas que puedan contribuir de manera significativa a la investigación (Renzi & Freitas, 2015). La búsqueda de posibles participantes se dirigió a través de referencias personales y laborales dentro de la cadena de contactos asociados a temas de ciberseguridad y apropiación a tecnologías móviles y de IoT. Para la aplicación del método, se realizó el contacto y posterior ejercicio con 9 expertos en la materia, descritos en la (Tabla 8).

Tabla 8. Panelistas seleccionados

	Nombre	Empresa	Perfil
	Iván Camilo Castellanos	ETEK	Security Information Advisory Director en ETEK INTERNATIONAL CORPORATION
	David Pereira	SecPro	CEO SecPro / Consultor / CISO/ Speaker Internacional Council /Autor: Ciberseguridad al Alcance de todos.
	Gustavo Gómez	Microsoft	Ingeniero consultor en ciberseguridad y nuevas tecnologías, con más de quince años de experiencia en el sector de seguridad en TI.
	Carlos Castillo	McAfee	Ingeniero de sistemas, líder de equipo, con experiencia profesional focalizada en el campo del análisis de malware y su impacto en la seguridad informática, involucrado en diferentes roles técnicos.
	Fernando Ruiz	McAfee	Fernando es investigador móvil de malware en McAfee Labs y realiza análisis de amenazas y vulnerabilidades para dispositivos móviles, centrándose en el estudio y la detección de malware para Android.
	John Ying	McAfee	Director Mobile Software Development. Trabaja en la creación de aplicaciones de seguridad móvil para el consumidor y dirige una de las unidades de análisis de malware en McAfee.
	Ameya Sanzgiri	McAfee	Mobile Malware and Privacy Researcher en McAfee Participa en el análisis de malware y amenazas de privacidad y Exploits en plataformas móviles.

	Nombre	Empresa	Perfil
	Daryan Reinoso	Symantec	Manager Sales Engineering en Symantec con más 10 años en la industria de la Ciberseguridad, analista senior de grandes ataques y fraudes en América Latina.
	Jairo Mondragón	McAfee	CISO con más de 20 años ha laborado en el campo de la Tecnología y Seguridad de la Información en diferentes ámbitos siendo un consultor reconocido en Colombia en análisis de riesgos informáticos.

Fuente: Elaboración propia

7.1.2. Selección de los criterios

Después de la selección del panel de expertos, se realizó un proceso de identificación de las principales categorías de amenazas que afectan la seguridad de los IoT. Basados en el informe (ENISA, 2017) se encontraron 7 clasificaciones:

- Actividades malintencionadas
- Escuchas / Intercepción
- Cortes
- Daño y perdidas en activos IT
- Fallas y mal funcionamiento
- Desastre
- Ataques físicos

Luego se realizó un contraste del campo de experiencia de los panelistas contra las clasificaciones encontradas y se procedió a realizar un acotamiento del alcance para enfocarnos en la taxonomía de actividades malintencionadas. Esta categoría cuenta con las amenazas descritas en la (Tabla 9).

Tabla 9. Taxonomía de amenazas en IoT

Amenaza	Descripción
Malware	Programas de software diseñados para llevar a cabo acciones no deseadas y no autorizadas en un sistema sin el consentimiento del usuario, lo que resulta en daños, corrupción o robo de información. Su impacto puede ser alto.

Amenaza	Descripción
Exploid kits	Código diseñado para aprovechar una vulnerabilidad con el fin de obtener acceso a un sistema. Esta amenaza es difícil de detectar y en entornos de IoT su impacto varía de alto a crucial, dependiendo de los activos afectados.
Ataques dirigidos	Ataques diseñados para un objetivo específico, lanzados durante un largo período de tiempo y llevados a cabo en múltiples etapas. El objetivo principal es permanecer oculto y obtener la mayor cantidad de datos / información confidencial o control posible. Si bien el impacto de esta amenaza es medio, detectarlos suele ser muy difícil y lleva mucho tiempo.
DDoS	Múltiples sistemas atacan un solo objetivo para saturarlo y hacer que se bloquee. Esto se puede hacer haciendo muchas conexiones, inundando un canal de comunicación o reproduciendo las mismas comunicaciones una y otra vez.
Falsificación por dispositivos maliciosos	Esta amenaza es difícil de descubrir, ya que un dispositivo falsificado no se puede distinguir fácilmente del original. Estos dispositivos generalmente tienen puertas traseras y se pueden usar para realizar ataques a otros sistemas.
Ataques a la privacidad	Esta amenaza afecta tanto la privacidad del usuario como la exposición de elementos de la red a personal no autorizado.
Modificación de la información.	En este caso, el objetivo no es dañar los dispositivos, sino manipular la información para provocar el caos o adquirir ganancias monetarias.

Fuente: Tomado de (ENISA, 2017)

Con las amenazas clasificadas y evaluando la información encontrada en el marco teórico y el estado del arte se determinó finalmente seleccionar la amenaza por malware como tipología específica a trabar con el Método Delphi.

7.1.3. Ejecución de la metodología (versión en inglés)

A los expertos se les envío este correo electrónico describiendo la necesidad y su colaboración en la investigación.

Dear Expert

Let me introduce, I am Andres Ballestas, Master Engineering Management student at Universidad de la Sabana – Colombia. (https://www.unisabana.edu.co/programas/posgrados/facultad-de-ingenieria/maestria-en-gerencia-de-ingenieria/maestriaengerenciadeingenieria/)

Using the Delphi Method (https://en.wikipedia.org/wiki/Delphi_method) as panel expert technique like propose to you participate in this focus group.

My intention is select and identify malware candidate and use into IoT propagation model (https://en.wikipedia.org/wiki/Agent-based_model) in the research looking risks and recommendations.

Two questions select to you and waiting answers:

- In your opinion which could malware more critical for IoT environment?
- Which reasons do you consider in above selection? Which characteristics should mention support your opinion?

Many thanks for your participation and collaboration

Andrés Ballestas

Figura 8. Diseño del correo de presentación al panelista

Fuente: Elaboración propia.

7.1.4. Ejecución de la metodología (versión en español)

Estimado experto

Permítanme presentarme, soy Andrés Ballestas, estudiante de Maestría en Gerencia de Ingeniería en la Universidad de la Sabana - Colombia. (https://www.unisabana.edu.co/programas/posgrados/facultad-de-ingenieria/maestria-en-gerencia-de-ingenieria/maestriaengerenciadeingenieria/)

Utilizando el Método Delphi (https://en.wikipedia.org/wiki/Delphi_method) como técnica de experto en el panel como proponerle participar en este grupo de discusión.

Mi intención es seleccionar e identificar candidatos para malware y utilizarlos en el modelo de propagación de IoT (https://en.wikipedia.org/wiki/Agent-based_model) en la investigación buscando riesgos y recomendaciones.

Dos preguntas seleccionadas y esperando respuestas:

- En tu opinión, ¿qué malware podría ser más crítico para el entorno de la IoT?
- ¿Qué razones considera en la selección anterior? ¿Qué características deben mencionarse para apoyar su opinión?

Muchas gracias por tu participación y colaboración

Andrés Ballestas

Figura 9. Diseño del correo de presentación al panelista

Fuente: Elaboración propia.

7.1.5. Primera ronda

En el primer contacto con los panelistas, fue enviado un correo electrónico (Figura 8 y Figura 9) con dos propósitos definidos: identificar la criticidad de los malware dentro del ambiente IoT e, identificar la razón pertinente de la selección escogida. Los resultados de la primera ronda fueron consolidados y se encuentran representados en la (Tabla 10).

Tabla 10. Resultados obtenidos de la ronda 1

Participante	1er Opción	2do Opción	3er Opción	Justificación
Iván Camilo Castellanos	Mirai Botnet	Stuxnet	Bashlite	Debido a varias variantes y mutaciones encontradas.
David Pereira	Intel Spoiler	Meltdown	Mirai Botnet	Fuerza extremadamente bruta contra el dispositivo.
Gustavo Gómez	Emotet	muBot	Hydra	Se han utilizado para realizar algunos de los ataques DDoS más grandes y disruptivos.
Carlos Castillo	BrickerBot	Mirai Botnet	IoT Troop / Reaper	Realiza un ataque de denegación de servicio permanente (asalto que daña el hardware).
Fernando Ruiz	Mirai Botnet	Stuxnet	IoT Troop / Reaper	Código fuente lanzado al público que permite la creación fácil de múltiples variantes.
John Ying	Mirai Botnet	Stuxnet	BrickerBot	Mirai: malware simple relativamente, pero fue capaz de mostrar que incluso los dispositivos modernos necesitan ser parcheados muy bien
Ameya Sanzgiri	Stuxnet	Mirai Botnet	BrickerBot	Era una pieza maliciosa de código extremadamente encubierto que era complejo en su funcionamiento y avanzado en su intención maliciosa. También fue el primer precursor de un malware dirigido a dispositivos comerciales de IoT. El sigilo del código lo

Participante	1er Opción	2do Opción	3er Opción	Justificación
				convirtió en una de las pruebas de concepto más críticas de la devastación en un entorno de IoT.
Daryan Reinoso	TrickBot	Psyb0t	Moose/Elan	El sigilo del código lo convirtió en una de las pruebas de concepto más críticas de la devastación en un entorno de IoT
Jairo Mondragón	Moose/Elan	Meltdown	Mirai Botnet	Porque contienen nuevos métodos DDoS no utilizados previamente por las variantes de Mirai

Fuente: Elaboración propia

7.1.6. Segunda ronda

La siguiente dinámica propuesta a los panelistas fue realizar una priorización de criticidad de malware a partir de una lista previamente definida. El objetivo era identificar si existía un punto disruptivo en la elección original de los malware o por el contrario se sostenían con la selección inicial. El resultado de la segunda ronda fue consolidado y se encuentra representado en la (Tabla 11).

Tabla 11. Resultados obtenidos de la ronda 2

Participante	Listado de opciones				
	1er Opción	2do Opción	3er Opción	4ta Opción	5ta Opción
Iván Camilo Castellanos	Meltdown	BrickerBot	Mirai Botnet	Stuxnet	Bashlite
David Pereira	Psyb0t	Intel Spoiler	Meltdown	Mirai Botnet	Stuxnet
Gustavo Gómez	Emotet	muBot	Hydra	Stuxnet	Mirai Botnet
Carlos Castillo	Moose/Elan	Mirai Botnet	BrickerBot	Iot Troop / Reaper	Intel Spoiler
Fernando Ruiz	Moose/Elan	Stuxnet	IoT Troop / Reaper	Mirai Botnet	BrickerBot
John Ying	Stuxnet	Hydra	Mirai Botnet	Iot Troop / Reaper	BrickerBot
Ameya Sanzgiri	Bashlite	Mirai Botnet	Stuxnet	BrickerBot	muBot
Daryan Reinoso	Mirai Botnet	Psyb0t	Moose/Elan	TrickBot	Intel Spoiler
Jairo Mondragón	Moose/Elan	Stuxnet	Mirai Botnet	Emotet	Meltdown

Fuente: Elaboración propia

7.1.7. Tercera ronda

Finalmente, con los resultados obtenidos en la ronda anterior se realizó una socialización a los panelistas de las respuestas presentadas por todo el equipo. Para no afectar el resultado de la última dinámica, se decidió anonimizar los resultados para prevenir un sesgo involuntario.

En la última fase y con todos los insumos socializados, se les permitió a los panelistas elegir a su consideración cual era para ellos el malware que generaba más impacto en el ambiente IoT. Los resultados fueron consolidados y presentados en la siguiente (Tabla 12).

Tabla 12. Resultados obtenidos de la ronda 3

Participante	Selección final
Iván Camilo Castellanos	Mirai Botnet
David Pereira	Mirai Botnet
Gustavo Gómez	Stuxnet
Carlos Castillo	Iot Troop /Reaper
Fernando Ruiz	Mirai Botnet
John Ying	Mirai Botnet
Ameya Sanzgiri	Stuxnet
Daryan Reinoso	Mirai Botnet
Jairo Mondragón	Mirai Botnet

Fuente: Elaboración propia

Los resultados encontrados permitieron identificar una clara tendencia de preferencia en Mirai Botnet (67%) seguido de Stuxnet (22%) y IoT Troop (11%) como malware con mayor impacto. Finalmente, la ficha técnica de participación de los panelistas es presentada en la (Tabla 13).

Tabla 13. Participación de los panelistas

Tema	No. Expertos Ronda I	% Tasa de respuesta	No. Expertos Ronda II	% Tasa de respuesta	No. Expertos Ronda III	% Tasa de respuesta
Malware críticos en IoT	9	100%	9	100%	9	100%

Fuente: Elaboración propia

7.2. Caracterización de los malware definidos

El malware es la amenaza más grave para los dispositivos IoT, los cuales pueden destruir el dispositivo o, en algunos casos, puede cambiar el sistema a un estado privilegiado bajo la autoridad del atacante. Cuando se habla de malware en hardware, los atacantes han encontrado formas de actuar a nivel de chip, que es la parte integral de un sistema. Mediante el uso de varios métodos, un dispositivo o un sistema pueden quedar expuestos (Sklavos, 2017).

El propósito de este objetivo es realizar una caracterización del listado seleccionado por el panel de expertos incluyendo la definición, tipología y, modo de propagación y ataque.

7.2.1. Stuxnet

Stuxnet es un gusano sofisticado diseñado para apuntar solo a sistemas específicos SCADA (Supervisory Control And Data Acquisition por sus siglas en ingles es una tecnología de control industrial) de Siemens. Hace uso de cuatro vulnerabilidades tipo día-cero los cuales son ataques que hacen uso de una vulnerabilidad de seguridad en una aplicación, antes de que los desarrolladores de la aplicación la conozcan (Paul & Yadegari, 2013).

A diferencia de la mayoría de los programas maliciosos, Stuxnet está orientado a sistemas de control industrial, que se utilizan ampliamente en fábricas, líneas de ensamblaje, refinerías y plantas de energía. Ataca a computadores con sistema operativo MS Windows que programan controladores lógicos específicos de Siemens y equipos especializados que controlan procesos físicos automatizados, como brazos de robot, en sistemas de control industrial (Chen & Abu-Nimeh, 2011).

Stuxnet apunta a equipos vulnerables que ejecutan el software de control WinCC / Step 7, que normalmente se utiliza para programar PLC. Cuando un computador infectado

se conecta a un PLC Siemens, Stuxnet instala un archivo .dll malicioso, reemplazando el archivo .dll original del PLC. El archivo .dll malicioso permite a Stuxnet monitorear e interceptar toda comunicación entre el equipo y el PLC. Dependiendo de las condiciones específicas del PLC, Stuxnet inyecta su propio código en el PLC de manera indetectable por el operador (Chen & Abu-Nimeh, 2011).

En julio de 2010 Stuxnet ataco las instalaciones nucleares de Irán Los expertos en seguridad informática de este país en conjunto con compañías de ciberseguridad determinaron que Stuxnet apuntaba principalmente a las instalaciones de uranio en Natanz, lo que afecta la velocidad de las centrífugas. Su velocidad de rotación primero aumentaba y luego decrecía con el fin de introducir distorsiones y perturbar su comportamiento normal. Se supone que el 10% de las centrifugadoras en Natanz fueron visto afectadas por este gusano de 2009 a 2010 (Masood et al., 2011). Hay 6 etapas principales del gusano Stuxnet detalladas en (Tabla 14).

Tabla 14. Etapas de ejecución del Stuxnet

Etapa	Descripción
Infección	Stuxnet entra al sistema vía memoria USB y procede a infectar todas las maquinas que corren bajo sistema operativo MS Windows, Por medio de la falsificación de certificado digital, este gusano tiene la capacidad de evadir sistemas de detección automática.
Búsqueda	Stuxnet comprueba si una maquina hace parte de los sistemas de control industrial creados por Siemens como los sistemas desarrollados en Irán para manejar las centrifugas de alta velocidad utilizadas en la industria nuclear.
Actualización	Si el sistema no es un objetivo, no realiza ninguna afectación al equipo. Si lo fuera, el gusano intenta acceder a internet para descargar la última versión de sí mismo.
Captura	El gusano compromete los controladores lógicos de sus sistemas objetivo a partir de explotar las vulnerabilidades tipo día-0 (Zero-day) que no hayan sido identificados por los expertos en seguridad.
Control	En un inicio, Stuxnet espía las operaciones del sistema objetivo. Posteriormente, utiliza dicha información para tomar control de las centrifugas y hacerlas fallar.
Engaño y destrucción	En paralelo al control, el gusano provee falsa información a los controladores asegurando confusión e imposibilidad de realizar algún tipo de acción concreta.

Fuente: Basado en (IEEE, 2013)

En julio de 2010, Symantec configuró un sistema para monitorear el tráfico a los servidores de comando y control (CnC) de Stuxnet. Esto permitió observar las tasas de infección e identificar las ubicaciones de las computadoras infectadas. Los datos enviados de vuelta a los servidores de CnC se encontraban encriptados e incluyen datos

como la dirección IP interna y externa, el nombre de la computadora, la versión del sistema operativo y si está ejecutando el software de control industrial SIMATIC Step 7 de Siemens (Falliere et al., 2011). A partir de un análisis de 40,000 direcciones IP externas únicas, de más de 155 países. Al observar el porcentaje de hosts infectados por país (Figura 10), se muestra que aproximadamente el 60% de los infectados se encuentran en Irán seguido de Indonesia e India.

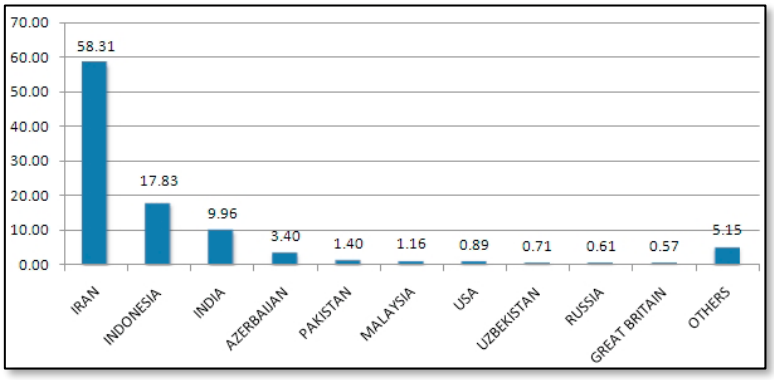


Figura 10. Distribución geográfica de las infecciones

Fuente: Tomado de (Falliere et al., 2011)

Ya sea que se trate de plantas nucleares, electricidad, telecomunicaciones, transporte u otros servicios esenciales, muchas actividades del gobierno central dependen de infraestructuras críticas que son predominantemente propiedad y operadas por el sector privado. Si la infraestructura crítica se ve afectado por un gusano Stuxnet o un código malicioso similar, las interrupciones podrían obstaculizar la capacidad del gobierno de proporcionar servicios esenciales por largos períodos de tiempo. Tal suceso también podría degradar la capacidad del gobierno para mantener objetivos de seguridad y, por lo tanto, hacer que la nación sea más vulnerable a una variedad de amenazas extranjeras y nacionales o contribuir a una pérdida de confianza pública en el estado.

7.2.2. IoT Troop /Reaper

El 20 de octubre de 2017, la firma china de seguridad cibernética Netlab 360 informó una nueva botnet dirigida a dispositivos IoT. Esta empresa llamó a la botnet IoT_reaper,

la cual desde entonces se conoce como Reaper ó IoT Troop. En su primer reporte, la compañía identificó 10,000 dispositivos infectados que estaban controlados únicamente por un servidor de Comando y Control – CnC. Solo cinco días después, el número había aumentado a 28,000 incluidos nuevos servidores (Rhebo, 2019).

Reaper IoT está basada en una metodología parecida al del malware Mirai, red utilizada principalmente para realizar ataques de denegación de servicio (DDoS) mediante dispositivos del IoT. Dentro de las diferencias, se encuentran métodos de programación distintos. Por un parte, Mirai analiza los puertos de los dispositivos Telnet para intentar iniciar sesión mediante una lista preestablecida de credenciales. Reaper, en tanto, no se basa únicamente en un escáner, sino que explota vulnerabilidades directamente para hacerse del control de los artefactos sin parches de seguridad y, tras obtener acceso, los agrega a su infraestructura para aprovechar su hardware y funciones (Muñoz, 2017).

Reaper también es especialmente preocupante porque está construido alrededor de un motor Lua combinado con scripts adicionales para ejecutar sus ataques. Lua es un lenguaje de programación integrado diseñado para permitir que se ejecuten scripts. Por lo tanto, su marco flexible permite que su código puede actualizarse fácilmente para incluir más opciones de ataque malicioso. Lo que claramente lo convierte en un paso más en la evolución de los ataques basados en IoT (FortiGuard SE Team, 2017).

Los investigadores han descubierto que miles de dispositivos han sido infectados y más de dos millones están en cola para ser infectados. En una primera fase, los investigadores solo pudieron identificar que el botnet se centró en aumentar su número de propagación y no se ha visto ninguna carga maliciosa. Sin embargo, el código para el malware es modular, donde los componentes se pueden cargar para expandir las capacidades de la botnet, lo que hace que el potencial de alguien que use la botnet para otros ataques sea muy alto (Perez, 2017).

En la (Figura 11) se puede observar el flujo de propagación de botnet Reaper, este malware realiza sus actividades mediante tres componentes definidos: Escaneo, ataque por vectores y, comando y control (CnC).

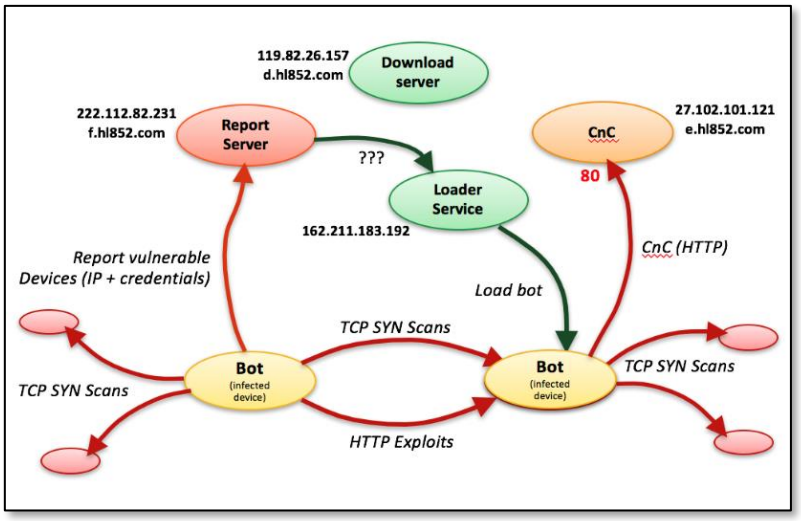


Figura 11. Flujo de propagación del botnet Reaper

Fuente: Tomado de (Radware, 2017)

- Escaneo: Reaper realiza un escaneo antes de entregar la carga útil. La primera ola consiste en escaneos SYN en diversos puertos TCP, la primera ola de escaneos se realiza con una IP de origen y un puerto de origen idénticos en cada paquete SYN. Es probable que el escaneo sea un intento de tomar huellas digitales de los dispositivos. Una vez que encuentra un dispositivo IoT, su dirección IP pasa al proceso de explotación del equipo.

- Ataque por vectores: Reaper comienza su última fase de escaneo una vez que la IP pasa al proceso de explotación de vulnerabilidades. A diferencia de las anteriores botnets de IoT o las variantes de Mirai, Reaper no aprovecha la fuerza bruta de Telnet con credenciales predeterminadas, sino que aprovecha las debilidades basadas en HTTP de vulnerabilidades conocidas en IoT. Reaper escanea los puertos TCP e intenta abrir el puerto del servidor y ejecutar uno de los nueve Exploits incluidos en la botnet (Radware, 2017).

- Comando y control: Reaper utiliza una IP y dominio fijo en su servidor CnC, que reside en e.hl852.com. La comunicación de los dispositivos infectados al servidor central se realiza cada 10 segundos. Una vez que la botnet se actualiza con los scripts de ataque, los comandos se ejecutan a través de este canal.

7.2.3. Mirai Botnet

Los ataques DDoS no son nuevos ni sofisticados. El atacante envía una gran cantidad de tráfico a su objetivo lo que hace que el sistema de la víctima se ralentice y finalmente se bloquee. Para este principio existen variantes más o menos distintas, pero básicamente, es una batalla del tamaño del canal de datos entre el atacante y la víctima. Si el objetivo tiene una mayor capacidad para recibir y procesar datos, ganará. Por el contrario, si el atacante puede enviar más datos de los que la víctima puede procesar, la victoria habrá sido para el malware El atacante puede diseñar una estrategia de construir un tráfico de datos gigante, pero ese método sería costoso. Es mucho más inteligente reclutar millones de computadores y dispositivos vulnerables en Internet (Schneier, 2016).

Mirai es un malware que infecta dispositivos inteligentes que se ejecutan en procesadores ARC, convirtiéndolos en una red de bots controlados de forma remota. Esta red de bots, llamada botnet, a menudo se usa para lanzar ataques DDoS. En septiembre de 2016, los autores del malware Mirai lanzaron un ataque DDoS en el sitio web de un manejo en seguridad. Una semana después, lanzaron el código fuente al mundo, posiblemente en un intento de ocultar los orígenes de ese ataque. Este código fue replicado rápidamente por otros cibercriminales, y se cree que está detrás del ataque masivo que derribó al proveedor de servicios de registro de dominio, Dyn, en octubre de 2016 (Cloudflare, 2019).

El ataque contra Dyn cerró varios sitios ampliamente utilizados entre ellos Twitter, Spotify, Netflix, GitHub, Amazon y Reddit. La mayoría logró volver a la normalidad después de considerables horas de interrupción del servicio. El ataque global de

denegación de servicio en la infraestructura de administración de DNS de Dyn fue tan impactante porque atacó la arquitectura de Internet que une a todos esos sitios: el sistema de nombres de dominio o DNS, que redirige a los usuarios de Internet desde direcciones web simples, como amazon.com, a los servidores web reales de las empresas (SCmagazine, 2016).

Estos ataques fueron habilitados tanto por la enorme cantidad de módems, cámaras y diferentes dispositivos conectados a la web que se encontraban bajo el control de Mirai, como por el hecho de que un hacker conocido como "Anna-senpai" tomo la decisión de liberar el código en septiembre de 2016. Si bien no hay nada particularmente novedoso sobre el software de Mirai y el mecanismo que utiliza para realizar los ataques de denegación de servicio, ha demostrado ser notablemente flexible y adaptable. Como resultado, los atacantes pueden desarrollar diferentes cepas que pueden hacerse cargo de nuevos dispositivos de IoT vulnerables y aumentar la población (y el poder de cómputo) a los que pueden recurrir las botnets de Mirai (Newman, 2016).

Mirai escanea Internet para dispositivos IoT que se ejecutan en el procesador ARC. Este procesador ejecuta una versión simplificada del sistema operativo Linux. Si no se cambia la llave predeterminada de nombre de usuario y contraseña, Mirai puede iniciar sesión en el dispositivo e infectarlo (Cloudflare, 2019).

Una botnet Mirai se compone de cuatro componentes principales: El bot es el malware que infecta los dispositivos. Su doble objetivo es propagar la infección a dispositivos mal configurados y atacar un servidor de destino tan pronto como reciba el comando correspondiente de la persona que controla el bot, o botmaster. El servidor de comando y control (CnC) proporciona al botmaster una interfaz de administración centralizada para verificar el estado de la botnet y organizar nuevos ataques DDoS. Por lo general, la comunicación con otras partes de la infraestructura se realiza a través de la red anónima Tor. El cargador facilita la difusión de ejecutables dirigidos a diferentes plataformas (18 en total, incluidos ARM, MIPS y x86) al comunicarse directamente con las nuevas víctimas. El servidor de informes mantiene una base de datos con

detalles sobre todos los dispositivos en la botnet. Los recién infectados generalmente se comunican directamente con él (Kolias et al., 2017).

Las utilidades distribuidas con el código fuente de Mirai incluyen programas para encriptar cadenas de inclusión en el código fuente del bot. Las cadenas cifradas incluyen las direcciones IP de los servidores de CnC. Esta táctica, junto con otras como eliminar el binario del bot, se utilizan para frustrar la ingeniería de código inverso del binario del malware (Jerkins, 2017).

A continuación, se presenta las etapas de ejecución de Mirai (Figura 12). Cada una de estas etapas se encuentra descrita paso a paso en la (Tabla 15).

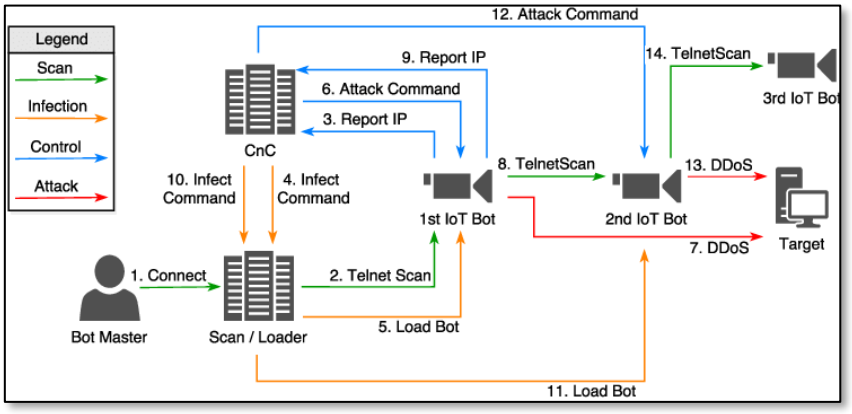


Figura 12. Flujo de ejecución del Mirai Botnet
Fuente: Tomado de (McDermott et al., 2018)

Tabla 15. Descripción de las etapas de ejecución del Mirai Botnet

Etapa	Descripción
1	Un atacante (botmaster) inicia el proceso conectándose al servidor de escaneado.
2	Se inicia el codigo ./loader para ejecutar el módulo scanner.c, y escanea Internet en busca de dispositivos IoT vulnerables con servicios Telnet y puertos 23 o 2323 abiertos.
3	Al detectar un dispositivo vulnerable, el malware intenta forzar un inicio de sesión exitoso utilizando una lista de 62 nombres de usuario y contraseñas predeterminados conocidos. Si tiene éxito, las credenciales de inicio de sesión y la información del dispositivo se envían de vuelta al servidor de control, y el servidor de escaneo las utilizará más adelante para iniciar sesión y entregar el malware al dispositivo vulnerable.
4	Se envía un comando de infección desde el servidor de control al servidor escaneo que contiene toda la información necesaria, como detalles de inicio de sesión,

Etapa	Descripción
	dirección IP, arquitectura de hardware. Mirai admite múltiples arquitecturas de hardware, incluidos ARM, MIPS, Sparc y PowerPC.
5	El servidor de escaneo utiliza esta información para iniciar sesión e indicar al dispositivo vulnerable que establezca un puente de comunicación, descargue y ejecute el archivo binario. Una vez ejecutado, el primer dispositivo IoT infectado se convierte en parte de la botnet Mirai y puede comunicarse con el servidor de control. El binario de malware se elimina y se ejecuta solo en la memoria, para evitar la detección.
6	El botmaster ahora puede emitir comandos de ataque, especificando parámetros como la duración del ataque y el objetivo
7	El malware incluye 10 tipos de ataques DDoS, que incluyen sobrecarga a los: UDP, DNS, así como los paquetes SYN, ACK los cuales pueden ser usados para atacar un objetivo en Internet.
8	El primer bot ahora intenta repetir el proceso de infección y propagar la red de bots escaneando en Internet dispositivos de IoT vulnerables adicionales con servicios Telnet y puertos 23 o 2323 abiertos
9	La nueva información vulnerable del dispositivo IoT se devuelve al servidor de control
10	Se emite un nuevo comando de infección al servidor de escaneo
11	El archivo binario de hardware se carga en el dispositivo IoT vulnerable recién descubierto
12	El comando de ataque relevante se emite desde el servidor de control
13	El ataque es ejecutado por el segundo bot recién infectado, junto con el primer bot
14	Se repite la búsqueda de dispositivos IoT vulnerables adicionales para expandir aún más la botnet.

Fuente: Elaboración propia, basado en (McDermott et al., 2018)

Por motivos desconocidos el código fuente de Mirai fue filtrado a la red, lo cual permite realizar una taxonomía a profundidad de los componentes de malware. La primera característica por denotar es el script de compilación. Mirai compila su código fuente para diez tipos de arquitecturas diferentes. Adicionalmente, se pueden identificar tres claros componentes del código: bot, servidor CnC y cargador (Sinanovic & Mrdovic, 2017).

Bot fue escrito completamente en lenguaje de programación C. Comenzando en el archivo main.c, se puede identificar que Mirai elimina su archivo .exe una vez que se inicia, permaneciendo solo en la memoria RAM. Esta es una de sus formas de evitar la detección. Dado que no se garantiza la persistencia, el malware deshabilita el temporizador de vigilancia en el dispositivo infectado, evitando que se reinicie. Luego, busca y elimina otra instancia del mismo malware que ya se está ejecutando en el mismo dispositivo. Mirai define un nombre aleatorio del proceso con el fin de dificultar la detección, luego se conecta al servidor CnC y espera a que se ejecuten los comandos.

Hay tres módulos que se ejecutan junto al proceso principal: attack, killer y scanner (Sinanovic & Mrdovic, 2017).

i. Attack: El módulo de ataque analiza el comando cuando se recibe e inicia el ataque DoS. Diez métodos de ataque DoS se implementan en diez funciones diferentes. El módulo decide a qué función llamar en función del comando emitido y detiene su ejecución una vez que expira el tiempo de duración.

ii. Killer: El módulo Killer mata los procesos que contienen los puertos 22, 23 y 80 y reserva estos puertos evitando que las aplicaciones canceladas se reinicien. Después de eso, escanea continuamente la memoria tratando de encontrar y eliminar malware similar creado e iniciado por otros atacantes.

iii. Scanner: El módulo del escáner utiliza telnet y una dirección IP pública generada aleatoriamente para buscar otros dispositivos IoT vulnerables. Los nombres de usuario y las contraseñas de Telnet se toman de la tabla que contiene 62 combinaciones predeterminadas de fábrica. Si la conexión con un dispositivo aleatorio se establece con éxito, la dirección IP del dispositivo IoT vulnerable se envía al servidor con el nombre de usuario y la contraseña correspondientes.

El servidor CnC está escrito en el lenguaje de programación Google Go. Primero se conecta a una base de datos MySql usando credenciales predefinidas. Luego crea dos sockets de escucha, uno toma el puerto 23 para telnet y otro toma el puerto 101 para API. Cuando se establece la conexión, el controlador inicial decide si se trata de una conexión del usuario registrado en el CnC o es un nuevo registro de bot. El controlador de usuario genera una solicitud de nombre de usuario y contraseña a través de Telnet. Si el usuario es administrador, puede usar comandos para agregar un nuevo usuario o ejecutar los comandos de ataque estándar (Sinanovic & Mrdovic, 2017).

Finalmente, el cargador está escrito en lenguaje de programación C. Primero crea un servidor para descargar cargas útiles pre compiladas para varias arquitecturas, luego comienza a actuar como un servidor de informes, escuchando los dispositivos IoT vulnerables descubiertos que pueden verse comprometidos. Cuando se recibe información sobre el objetivo potencial, el cargador se conecta a él a través de Telnet, descarga y ejecuta la carga útil contra el dispositivo comprometido, convirtiéndolo en un nuevo bot (Sinanovic & Mrdovic, 2017).

Una de las razones por las que Mirai es tan difícil de contener es que acecha en los dispositivos y, en general, no afecta notablemente su rendimiento. No hay razón para que el usuario promedio o las empresas que no toman como relevante los asuntos de ciberseguridad piense que sus dispositivos son potencialmente parte de una botnet activa. E incluso si lo fuera, no hay mucho que puedan hacer al respecto, ya que no tienen una forma directa de interactuar con el producto infectado (Newman, 2016).

7.2.4. Algunos efectos de los ataques de malware

Por más de 20 años tanto entidades del gobierno como de las empresas privadas han investigado sobre las amenazas en ciberseguridad en las infraestructuras de TI de los sectores de la economía. Nos encargamos ahora de empezar a explorar las nuevas dimensiones del potencial sobre los sectores con dispositivos o redes IoT.

El alcance de los daños ocasionados por software malicioso depende del objetivo de infección, es decir, un ordenador o dispositivo doméstico o una red empresarial. Las consecuencias de los daños también pueden variar en función del tipo de malware, además de la naturaleza de los datos almacenados en el dispositivo (Kaspersky Lab, 2016). Dado que la naturaleza de Reaper y Mirai es similar, y se encuentra mayor documentación técnica y académica de este último, la caracterización y posterior categorización de riesgo se realizará con los casos de Stuxnet (tipo Worm) y Mirai (tipo botnet). En la (Tabla 16) se refleja los efectos de los ataques de malware en los sectores sociopolíticos, económicos, tecnológicos e internacionales.

Tabla 16. Efectos de los ataques de malware Mirai / Stuxnet

Efectos/Malware	Stuxnet Worm Caso Irán	Mirai Botnet Caso Krebs on Security
Socio políticos	Des acreditamiento del gobierno local por falta de acciones y decisiones en la fase de contención del malware. Sensación de inseguridad en la población por las medidas de ciberseguridad y la postura contra los perpetradores.	Afectación en la red de telecomunicaciones de Alemania y Reino Unido. Solicitud de generación de cargos penales a los creadores del código fuente del malware.
Económicos	Imposibilidad de compra de suministros a consecuencia del embargo económico que tiene. Afectación en el presupuesto del plan nuclear para solventar la situación. Bajos rendimientos de productividad de la planta nuclear de Natanz.	Afectación en comercios electrónicos lo que origino grandes pérdidas en ventas de productos. Afectación en empresas de servicios generando desconfianza en el uso de ciertos portales web.
Tecnológicos	Daño directo a las centrifugas de la planta nuclear. Generación de parches de seguridad para las vulnerabilidades explotadas. Reglas más estrictas para la gestión de certificados de los controladores.	Generación de nuevas variantes del malware a partir de la liberación del código fuente. Nuevos protocolos en los firmwares de los IoT para dificultar el acceso a las credenciales de usuario.
Internacionales	Retraso en el programa de enriquecimiento de uranio y alivio en las tensiones internacionales. Inversión financiera en asuntos de ciberseguridad para protección de ataques externos. Posibilidad de comercializar variantes del malware para fines terroristas.	Identificación de vacíos legales para tomar acciones en caso de ataques transnacionales.

Fuente: Elaboración propia

7.3. Sectores de estudio, implicaciones y vulnerabilidades

El crecimiento de la Internet de las Cosas (IoT) traerá consigo la promesa de una amplia gama de nuevos sistemas y se espera que sean alrededor de 57 mil millones de dispositivos conectados inteligentes para 2025 y equipos industriales (Cha et al., 2017). Las repercusiones abarcan industrias y regiones. El costo de los sensores, la potencia de procesamiento y el ancho de banda para conectar dispositivos se ha reducido lo suficiente como para impulsar una implementación generalizada (Jankowski, 2014).

Si bien estos habilitadores hacen posible el auge del IoT, su éxito a largo plazo depende de los casos de uso que ayudan a aprovechar el potencial económico de conectar miles de millones de dispositivos, ya sea para mejorar la calidad de vida o ahorrar dinero

(Jankowski, 2014). El alcance de este documento se centra en tres sectores claves de alto consumo de dispositivos del Internet de las Cosas: IIoT, los cuales son los dispositivos empleados en el sector industrial, IoMT que es la rama de internet de las cosas orientadas al sector salud y, hogares inteligentes que son los dispositivos de mayor versatilidad en el consumo masivo de personas.

7.3.1. IIoT - Industrial Internet of Things

El Internet industrial de las cosas (IIoT) conecta máquinas, analítica y personas para crear ideas poderosas con dispositivos de última generación con el fin de impulsar decisiones comerciales más inteligentes, rápidas y mejores. El IIoT está formado por máquinas interconectadas y dispositivos IoT que pueden monitorear, recopilar, intercambiar y analizar datos. Al combinar las comunicaciones de máquina a máquina con análisis, las empresas pueden obtener los beneficios de una eficiencia, productividad y rendimiento incomparables (Humphrey, 2018).

Las redes de IoT industriales implementan dispositivos de IoT heterogéneos para cumplir con una amplia gama de requisitos del usuario. Estos dispositivos generalmente se agrupan de proveedores de nube de IoT privados o públicos. Un número significativo de proveedores de IoT en la nube integran teléfonos inteligentes para superar la latencia de los dispositivos IoT y los problemas de baja potencia de cálculo. Sin embargo, la integración de dispositivos móviles con redes de IoT industriales expone a los dispositivos de IoT a importantes amenazas de malware. El malware móvil es la mayor amenaza para la seguridad de los datos de IoT, la información personal, la identidad y la información corporativa / financiera del usuario (Sharmeen et al., 2018). en la (Tabla 17) se pueden apreciar diversas potenciales vulnerabilidades asociadas al IoT del sector industrial.

Tabla 17. Vulnerabilidades asociadas a los IIoT

Vulnerabilidad	Descripción
(1) Integridad de los Firmware y boot seguro	El boot seguro utiliza técnicas asociadas con un firmware cifrado, asegurando que un dispositivo solo ejecute código generado por el OEM (fabricante) del dispositivo u otra parte confiable. El uso de la tecnología de boot seguro evita que los atacantes reemplacen el firmware con conjuntos de instrucciones maliciosas, evitando así los ataques. Desafortunadamente, no todos los conjuntos de chips IIoT están equipados con capacidades de arranque seguro. En tal escenario, es importante asegurarse de que los dispositivos IIoT solo puedan comunicarse con servicios autorizados para evitar el riesgo de reemplazar el firmware con conjuntos de instrucciones maliciosas.
(2) Falta de autenticación mutua	-Cada vez que un actuador inteligente en la planta de fabricación se conecta a la red, debe autenticarse antes de recibir o transmitir datos. Esto garantiza que los datos se originen en un dispositivo legítimo y no en una fuente fraudulenta. La autenticación segura y mutua, donde dos entidades (dispositivo y servicio) deben demostrar su identidad entre sí, ayuda a proteger contra ataques maliciosos. -Los algoritmos criptográficos que involucran claves simétricas o claves asimétricas se pueden utilizar para la autenticación bidireccional. Por ejemplo, el algoritmo de hash seguro (SHA-x) junto con el código autenticado de mensaje basado en hash (HMAC) se puede usar para claves simétricas y el algoritmo de firma digital de curva elíptica (ECDSA) para claves asimétricas.
(3) Comunicación segura (cifrado de extremo a extremo)	Las capacidades de comunicación segura protegen los datos en tránsito entre un dispositivo y su infraestructura de servicio tanto local como en la nube. El cifrado garantiza que solo aquellos con una clave de descifrada secreta puedan acceder a los datos transmitidos con el fin de poder proteger la información de las escuchas digitales.
(4) Debilidades en los procesos de monitoreo y análisis	El monitoreo captura datos sobre el estado general de un sistema industrial, incluidos los dispositivos de punto final y el tráfico de conectividad. Luego, los datos se analizan para detectar posibles violaciones de seguridad o posibles amenazas del sistema. Una vez detectado, se debe ejecutar una amplia gama de acciones formuladas en el contexto de una política general de seguridad del sistema, como revocar las credenciales del dispositivo o poner en cuarentena un dispositivo IoT basado en un comportamiento anómalo. Es fundamental asegurarse que los dispositivos de los puntos finales estén protegidos contra posibles manipulaciones y manipulación de datos, lo que podría dar como resultado un informe incorrecto de los eventos.
(5) Fallas en el ciclo de vida de la gestión de seguridad	La función de gestión del ciclo de vida permite a los proveedores de servicios y OEM controlar los aspectos de seguridad de los dispositivos IoT cuando están en funcionamiento. Las fallas de renovación de credenciales del dispositivo durante la recuperación ante desastres cibernéticos generan futuras vulnerabilidades a todo el sistema. Además, el desmantelamiento seguro de dispositivos asegura que los equipos desechados no se reutilizarán y explotarán para conectarse a un servicio sin autorización.

Fuente: Elaboración propia, basado en (Rambus, 2020)

7.3.2. IoMT - Internet of Medical Things

El IoT ofrece una amplia gama de posibilidades de aplicación que abarcan varios dominios, incluido el entorno personal, hogar, transporte, logística y atención médica. Un dominio clave que se está siendo fuertemente impactado por los IoT es el cuidado

de la salud. La aplicación de IoT en el dominio médico se conoce como Internet of Medical Things (Limaye & Adegbija, 2017).

Existe una creciente demanda en el desarrollo de soluciones de atención médica eficientes y rentables que faciliten a los hospitales y proveedores de salud la posibilidad de realizar diagnósticos y tratamientos a pacientes. Los diferentes dispositivos médicos, sensores y elementos de diagnóstico pueden considerarse dispositivos u objetos IoT. Por lo tanto, tienen el potencial de proporcionar un entorno de atención médica sin interrupciones (Nausheen & Begum, 2018).

El IoMT es una red de dispositivos y aplicaciones médicas conectadas cuyo propósito es proporcionar servicios de atención médica mejores y más personalizados. Esta tecnología está ganando tracción debido a la aparición de productos innovadores, como dispositivos portátiles de ultrasonido e imágenes de resonancia magnética (MRI), dispositivos portátiles, que permitirán agilizar los procesos médicos, tales como diagnósticos médicos, seguimiento y monitoreo remoto de pacientes (Limaye & Adegbija, 2017).

Aunque los IoT pueden proporcionar soluciones simples y menos costosas para conectar de forma inalámbrica dispositivos de monitoreo de salud en el hogar con registros de salud personales y hospitales, el desarrollo exitoso y la implementación de servicios basados en IoT requieren de garantías asociadas a la seguridad y la privacidad, en la (Tabla 18) se pueden apreciar diversas potenciales vulnerabilidades asociadas a IoT del sector salud.

Tabla 18. Vulnerabilidades generales asociadas a los IoMT (M)

Vulnerabilidad	Descripción
(1) Privacidad del paciente y protección de la propiedad intelectual	-Es posible extraer código de una aplicación de salud móvil desprotegida mediante el uso de ingeniería inversa para obtener acceso al código original y, por lo tanto, alterar la aplicación para robar datos confidenciales del paciente o robar la propiedad intelectual. Con respecto a la implementación de aplicaciones, el iOS de Apple tiene una política cerrada que involucra a la tienda oficial, mientras que Android tiene una política abierta que permite tiendas de terceros e instalación de aplicaciones a través de APKs.

Vulnerabilidad	Descripción
	-Dicha arquitectura de código abierto hace que la plataforma sea estructuralmente vulnerable y facilita el comportamiento malicioso en los dispositivos. Cuando los usuarios instalan las aplicaciones, se les pide que otorguen permisos respecto al acceso a las áreas específicas del dispositivo. La mayoría de los usuarios desconocen las implicaciones de los permisos de Android y sus efectos en el dispositivo cuando dan su consentimiento durante la instalación.
(2) Seguridad del paciente	-Es posible alterar las aplicaciones que se comunican con dispositivos de salud portátiles, después de aplicar ingeniería inversa, de manera que puedan causar daños físicos. Los datos biométricos recopilados mediante los IoT ofrecen oportunidades para que los atacantes accedan a información confidencial. Por ejemplo, en el momento de suministrar una dosis de medicamentos o una redirección la aplicación financiera a través del dispositivo. -Por lo general, los dispositivos portátiles transmiten los datos recolectados a los teléfonos inteligentes que utilizan la red Bluetooth y es probable que estos dispositivos sean atacados por brechas de seguridad y puedan ser propensos a amenazas adicionales.
(3) Manipulación de claves y acceso no autorizado	-Los dispositivos médicos internos (IMD) también pueden estar expuestos a ataques maliciosos creados por atacantes por medio de software maligno o fallas en el firmware. Estos dispositivos consisten en un transceptor de radio para comunicarse con un dispositivo externo llamado "Programador" el cual emite comandos para configurar los parámetros del dispositivo y recuperar datos médicos. Los IMD son monitoreados y operados remotamente por los cuidadores de salud del paciente a través de redes o internet. -Los paquetes transmitidos pueden ser escuchados y exponer la privacidad del paciente, como falsificar, manipular y reproducir los mensajes. Además, dado que se accede de forma remota a los datos del paciente, también existe la posibilidad de ataques cibernéticos a los datos del paciente o las credenciales del usuario. -Los esquemas actuales de control de acceso de IMD se centran en dos modelos de ataque genéricos. En el primer tipo de ataques, un programador no autorizado accede a los datos médicos que residen en el IMD que envía comandos maliciosos o modifica las configuraciones del dispositivo. En el segundo tipo de ataques, un programador no autorizado accede ilegítimamente a IMD e inicia la ejecución continua de cálculos de autenticación para agotar la batería y poner en riesgo al paciente.

Fuente: Elaboración propia, basado en (Nausheen & Begum, 2018)

7.3.3. Smart Homes

Un hogar inteligente brinda a los usuarios un amplio acceso a muchos aspectos de su hogar, incluso desde una ubicación remota. Por ejemplo, los usuarios pueden monitorear su hogar en tiempo real a través de una aplicación móvil o interfaz web. También pueden iniciar ciertas acciones de forma remota, como comunicarse con sus

hijos utilizando un juguete inteligente o desbloquear una cerradura inteligente para un amigo de confianza (Chang, 2019).

En los últimos tiempos, los consumidores han visto múltiples productos que se anuncian como dispositivos inteligentes para inmuebles. Estos productos prometen hacer que los hogares sean más cómodos, seguros, automatizados y controlados de forma remota. A esta nueva realidad de procesamiento de información se le dio el nombre de "Smart Homes". Lamentablemente conformes al uso de estos productos, se han publicado muchos casos que exponen serias vulnerabilidades de seguridad en muchos dispositivos de IoT, y algunos de ellos están siendo explotados para hacer ataques DDoS (Costa et al., 2019).

Las vulnerabilidades existentes, la configuración deficiente y el uso de contraseñas predeterminadas se encuentran entre los factores que pueden ayudar a un atacante a comprometer al menos un dispositivo en un sistema doméstico inteligente. Una vez que se compromete un solo dispositivo, es posible tomar una serie de acciones orientadas a las capacidades y funciones del dispositivo (Chang, 2019). En la (Tabla 19) se pueden apreciar diversas potenciales vulnerabilidades asociadas a IoT del enfocadas a hogares inteligentes.

Tabla 19.Vulnerabilidades asociadas a los Smart Home IoT

Vulnerabilidad	Descripción
(1) Acceso remoto	Algunos dispositivos IoT tienen un protocolo de acceso remoto disponible, como Telnet o SSH. De hecho, muchos dispositivos que formaron la red de arranque Mirai se infectaron porque tenían su servicio Telnet expuesto a Internet con credenciales predeterminadas. Los ataques más comunes a este tipo de servicios son Brute-Force o Dictionary-Attacks.
(2) Firmware	La exploración del firmware de un dispositivo IoT es una de las formas más comunes de identificar sus vulnerabilidades. Dado que algunos de estos dispositivos cuentan con una versión reducida del sistema operativo Linux, su estructura de archivos y servicios son muy similares a la versión de escritorio. Una de las vulnerabilidades más comunes encontradas es la exposición de información confidencial como las credenciales de inicio de sesión.
(3) Aplicaciones móviles	Algunas aplicaciones móviles también exponen información confidencial que puede ayudar a explotar otras vulnerabilidades en el ecosistema. Muchas veces, el código fuente de las aplicaciones de Android se puede extraer del archivo de instalación del APK conteniendo código malicioso.

Vulnerabilidad	Descripción
(4) Aplicaciones Web	Las aplicaciones web todavía están presentes en algunos dispositivos IoT. Sus vulnerabilidades se pueden identificar con las mismas herramientas utilizadas para sitios web comunes o aplicaciones web que no son IoT. Las aplicaciones web de dispositivos IoT expuestas a Internet son una grave amenaza para la seguridad de IoT si no están protegidas adecuadamente.

Fuente: Elaboración propia, basado en (Costa et al., 2019)

7.4. Selección de un Sector Económico

Según el informe de IBM Security y el Ponemom Institute "Cost of a Data Breach Report 2020" que reclutó a 524 organizaciones que experimentaron violaciones de datos entre agosto de 2019 y abril de 2020. La investigación cubrió un amplio conjunto de empresas, las organizaciones del estudio comprenden diversos tamaños, que abarcan 17 países y regiones, así como 17 industrias. Los investigadores del Ponemom Institute entrevistaron a más de 3.200 personas que conocían los incidentes de violación de datos en sus organizaciones y se encontró que el sector más afectado por brechas de seguridad fue el de atención médica (IBM, 2019).

En la (Figura 13) se muestran los sectores económicos evaluados por IBM y el impacto económico en términos de brechas de seguridad explotadas por delincuentes informáticos.

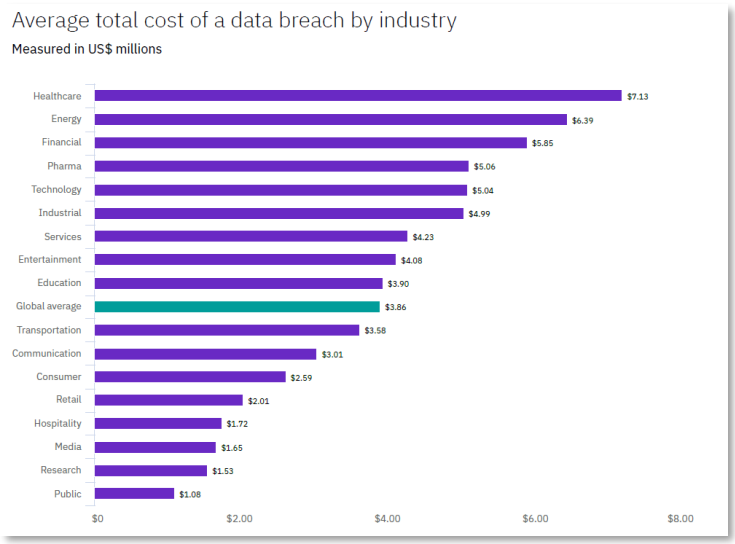


Figura 13. Media de costos incurridos por brechas de seguridad explotadas.

Fuente: Tomado de (IBM, 2019)

Además, en el estudio se refleja que a lo largo de los últimos 5 años los costos medios destinados a cubrir las brechas de seguridad, el sector salud tuvo como tendencia ubicarse siempre en la parte superior de la gráfica (Figura 14).

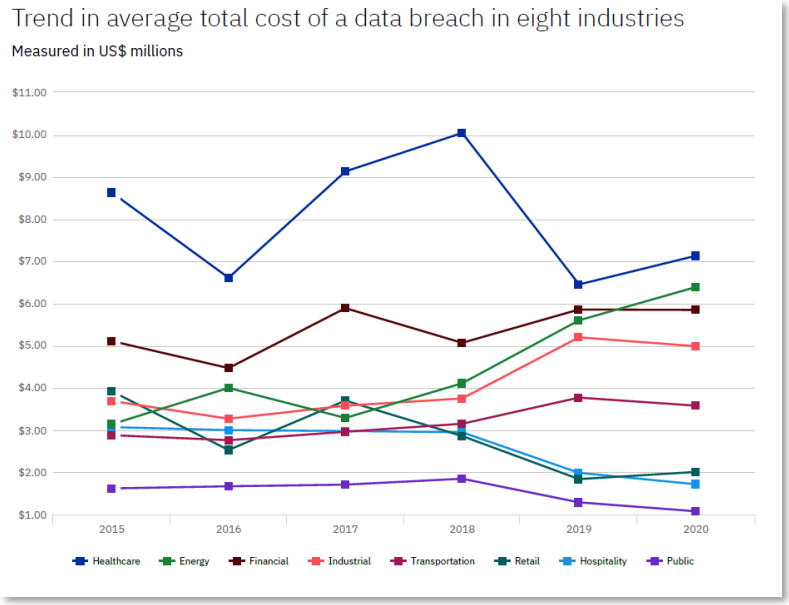


Figura 14. Tendencia de costos incurridos en brechas de seguridad por sectores económicos.

Fuente: Tomado de (IBM, 2019)

Así mismo el estudio encontró que el tiempo medio para identificar y contener una brecha de seguridad en el sector salud fue de 329 días (IBM, 2019).

Utilizando como referencia la anterior información, nuestra intención es concentrarnos en el sector salud y particularmente evaluar una solución tecnológica que contenga dispositivos IT y IoT.

7.5. Modelos de propagación y Mirai Botnet

La propagación es un proceso que en el común de las ocasiones es difícil de detectar y observar. Esto se debe a que surgen diferentes vulnerabilidades en diferentes tecnologías, servicios o funciones que pueden servir como vectores de propagación.

Adicionalmente, las industrias y gobiernos carecen de experiencia en la implementación generalizada de nuevas tecnologías como los IoT (Acarali et al., 2019). En consecuencia, el proceso de propagación inicial tiende a analizarse en retrospectiva, solo después de que se haya identificado una infección existente. Por lo tanto, es requerido implementar enfoques de modelación basados para predecir la dinámica de propagación de los malware y sus respectivos impactos.

El análisis dinámico de códigos maliciosos permite conocer de una manera rápida y efectiva qué acciones realiza una amenaza en el sistema. De esta forma se puede obtener información acerca de los archivos creados, conexiones de red o modificaciones en el registro. Para lograr este fin existe una gran cantidad de recursos y herramientas que brindan la posibilidad de analizar una amenaza a través de diferentes enfoques. La lucha contra el malware se lleva a cabo en diferentes frentes: desde la identificación de amenazas y vulnerabilidades en materia de ciberseguridad, la concientización al usuario para que adopte buenas prácticas, hasta el desarrollo de software antimalware por parte de las empresas especializadas, pasando por el establecimiento de políticas de seguridad adecuadas en los distintos sectores. Sin embargo, una de las herramientas y, ocasionalmente poco usada es la simulación de propagación de malware (Fuster et al., 2014). La simulación es frecuentemente utilizada en campos relacionados a la propagación de enfermedades infecciosas y puede aplicarse también para identificar comportamiento de la propagación del código malicioso en una red lo cual es de gran utilidad para los gerentes de ingeniería y equipos técnicos para tomar decisiones adecuadas respecto a la contención de la propagación o, al menos, la minimización de sus efectos.

Los modelos matemáticos desarrollados para estudiar la propagación de malware se basan en los modelos diseñados para estudiar la diseminación de las enfermedades infecciosas esto debido a las similitudes entre el comportamiento de los virus biológicos, bacterias, hongos y el del malware como botnets, gusanos o troyanos. Así pues, muchas de las propiedades y características de los primeros se traducen y tienen su reflejo en los segundos (Fuster et al., 2014).

7.5.1. Que es simulación y sus paradigmas

El modelado de simulación es el proceso de creación y análisis de un prototipo digital de un modelo físico para predecir su comportamiento en el mundo real. A su vez, está igualmente definido como una técnica numérica para realizar experimentos dentro de un ambiente digital, dichos experimentos involucran ciertos tipos de modelos matemáticos y lógicos que describen el comportamiento de sistemas de negocios, económicos, sociales, biológicos a través de ciertos periodos de tiempos (Coss, 2005). Dentro del proceso de simulación se encuentran definidos tres paradigmas: simulación de eventos discretos, dinámica de sistemas, y simulación basada en agentes. Hemos desarrollado una matriz de comparativa de los paradigmas (Tabla 20).

Simulación de Eventos Discretos

La simulación de eventos discretos es probablemente la técnica de simulación más utilizada en la investigación operativa. Como su nombre indica, modela un proceso como una serie de eventos discretos. Esto significa que se piensa que las entidades se mueven entre diferentes estados a medida que pasa el tiempo. Las entidades ingresan al sistema y visitan algunos de los estados, no necesariamente solo una vez, antes de abandonar el sistema (Maidstone, 2012).

Dinámica de sistemas

Otra técnica de simulación ampliamente utilizada es la dinámica de sistemas. Esta adopta un enfoque ligeramente diferente a la simulación de eventos discretos, centrándose más en los flujos alrededor de las redes que en el comportamiento individual de las entidades. Dinámica de sistemas considera tres objetos principales: existencias, flujos y retrasos. Las existencias son almacenes básicos de objetos, los flujos definen el movimiento de artículos entre diferentes stocks en el sistema. Por último, los retrasos son los tiempos de demora entre el sistema que mide algo y la actuación sobre esa medida (Maidstone, 2012).

Simulación basada en agentes

La simulación basada en agentes es un método relativamente nuevo, este modela sistemas compuestos por agentes autónomos que siguen una serie de reglas predefinidas para lograr sus objetivos mientras interactúan entre sí y con su entorno (Maidstone, 2012). El modelado y la simulación basados en agentes se han utilizado en una amplia gama de áreas de aplicación como un paradigma de modelado efectivo (Tabla 20). Este paradigma se utiliza como un enfoque útil para modelar la dinámica de propagación en redes complejas compuestas de agentes autónomos que interactúan entre sí, dichos agentes tienen comportamientos dinámicos, que actúan por un conjunto de reglas interactuando con otros agentes, aprendiendo de sus experiencias y adaptándose mejor a su entorno (Hosseini et al., 2016).

Tabla 20. Comparativa de los paradigmas de simulación

Aspecto	Dinámica de sistemas	Simulación de Eventos Discretos	Simulación basada en agentes
Visión del modelo	Sucesión de niveles y tasas interconectados por relaciones casuales	Entidades fluyendo a través de una red de actividades y colas	Conjunto de agentes interactuando entre ellos y el entorno
Causante del comportamiento del sistema	Los bucles de realimentación: la estructura del sistema determina su comportamiento a través del tiempo	La ocurrencia de los eventos: éstos cambian el estado del sistema	Las interacciones entre los agentes: simples reglas en cada agente dan origen al comportamiento colectivo
Estructura del sistema	La estructura del sistema es fija, no se pueden añadir nuevos niveles o flujos ni conectar nuevas relaciones causales durante la simulación.	El flujograma del proceso es fijo, durante la simulación no se pueden agregar nuevas actividades o cambiar las reglas de decisión que ya han sido preestablecidas.	La estructura del sistema no es fija, cambia a lo largo del tiempo, donde nuevos agentes pueden ser creados y sus interrelaciones modificadas durante la simulación.
Resolución	Nivel macro: entidades agrupadas y homogéneas	Nivel micro: entidades individuales (pasivas) y heterogéneas.	Nivel micro: entidades individuales (activas) y heterogéneas.
Naturaleza de los datos	Determinístico: los mismos datos de entrada generan los mismos resultados	Estocástico: trabaja con variables aleatorias. El análisis de resultados requiere replicaciones independientes	Estocástico: mayormente las reglas de decisión están basadas en funciones de probabilidad.
Manejo del tiempo	Continuo: utiliza el método de avance del tiempo por incremento fijo	Discreto: utiliza el método de avance de tiempo del siguiente evento	Continuo/Discreto: puede implementarse en un modelo cualquiera de los dos métodos de avance de tiempo: por

Aspecto	Dinámica de sistemas	Simulación de Eventos Discretos	Simulación basada en agentes
			incremento fijo o del siguiente evento
Formulación matemática	Ecuaciones diferenciales de primer orden las cuales representan a las tasas y los niveles acumulan las tasas mediante ecuaciones de integración	Combinación de expresiones matemáticas con operadores lógicos	Combinación de expresiones matemáticas con operadores lógicos y reglas de decisión
Dependencia de la trayectoria	Estados futuros del sistema dependen sólo del estado actual	Estados futuros del sistema dependen sólo del estado actual	Estados futuros del sistema dependen del estado actual y de otros estados anteriores y decisiones previas
Enfoque jerárquico	Estratégico: donde es más común encontrar problemas más relacionados con la complejidad determinística producto de políticas	Operacional: donde es más común encontrar problemas asociados con efectos aleatorios interconectados	Operacional/Estratégico.

Fuente : Tomado de (Sarmiento-Vásquez, 2016)

7.5.2. Dinámica de Sistemas

Una de las disciplinas cobijadas por el marco general del pensamiento sistémico es la Dinámica de Sistemas, la cual se plantea como "una forma o un paradigma de pensamiento que se expresa a través de cierto sistema de convenciones, es decir a través de un lenguaje particular" (Hugo Hernando et al., 2010). La Dinámica de Sistemas es un enfoque de simulación matemática utilizado para modelar sistemas complejos no lineales que pueden representarse mediante bucles a lo largo del tiempo. La Dinámica de Sistemas se utiliza cuando las soluciones de forma cerrada no son realistas o la solución satisfactoria puede ser representada en un mejor modelo para sistemas cambiantes y necesitan realizar análisis de escenarios (Hsu et al., 2016). El enfoque de Dinámica de Sistemas se centra en las relaciones causales que ligan las variables observables. Estas relaciones pueden expresarse fácilmente con ecuaciones algebraicas y es la particularización de valores que satisfacen estas ecuaciones lo que genera la dinámica global del sistema (Izquierdo et al., 2008).

La Dinámica de Sistemas (DS) puede explicar cómo las dependencias entre varios activos cibernéticos y físicos y el comportamiento del proceso cambian con el tiempo.

El enfoque fue propuesto originalmente por Forrester a mediados de la década de 1950 como una metodología de modelado formal para comprender el comportamiento de los sistemas complejos a lo largo del tiempo. Desde entonces, el enfoque se ha aplicado en una variedad de dominios, incluidos procesos industriales, sistemas socioeconómicos, análisis y diseño de políticas (Genge et al., 2015). En la actualidad existen herramientas computacionales que permiten apoyar el proceso de modelado y simulación con DS. Las herramientas software para DS han posibilitado el uso y la difusión de la DS en diversos sectores como en la educación, investigación, la empresa, lo ambiental, lo sociales, entre otros (Hugo Hernando et al., 2010).

Reforzar los controles de ciberseguridad contra los atacantes implica temas complejos como las personas, los procesos y la tecnología. La Dinámica de Sistemas permite comprender las interrelaciones entre distintos indicadores a fin de determinar la posibilidad de una violación de la seguridad a través del desarrollo de tendencias y patrones. Adicionalmente, la Dinámica de Sistemas está orientado a ser un enfoque de modelado de riesgo el cual puede señalar los primeros signos de amenazas maliciosas al agregar propiedades asociativas de diferentes elementos de riesgo (Fagade et al., 2017).

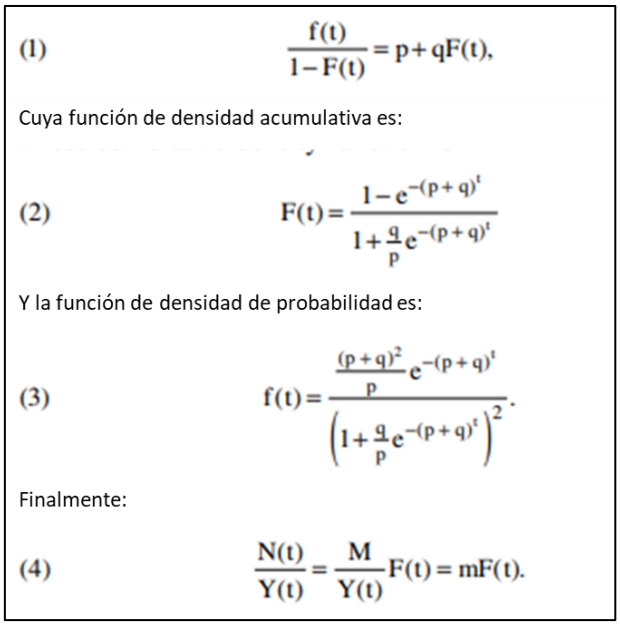
Dentro de las herramientas más utilizadas en el ámbito académico y empresarial, son conocidas las siguientes: AnyLogic, iThink/Stella, Powersim, Simile y Vensim. Estas herramientas de software ofrecen diferentes servicios, por medio de un entorno intuitivo para el usuario. Para modelos complejos estas herramientas son de gran de ayuda para el entendimiento del comportamiento, depuración y ajuste de los modelos de simulación (Hugo Hernando et al., 2010).

7.5.3. Modelo Bass

El modelo Bass fue desarrollado por Frank Bass. Consiste en una ecuación diferencial simple que describe el proceso de cómo se adoptan nuevos productos en una población. El modelo presenta una justificación de cómo interactúan los adoptantes actuales y los

adoptantes potenciales de un nuevo producto. La premisa básica del modelo es que los adoptantes pueden clasificarse como innovadores o como imitadores y la velocidad y el momento de la adopción dependen de su grado de innovación y el grado de imitación entre los adoptantes. El modelo Bass (Figura 15) se ha utilizado ampliamente en pronósticos, especialmente en pronósticos de ventas de productos nuevos y pronósticos de tecnología. Matemáticamente, la difusión básica de Bass es una ecuación de Riccati con coeficientes constantes. El modelo Bass es un hito en la corriente de estudios de administración y marketing que aseguraba que el principal poder de difusión de la innovación era de los medios de comunicación y el boca a boca. Más tarde, muchos académicos ampliaron el modelo de Bass para analizar los problemas relacionados con la difusión de nuevos productos o tecnologías (Hu et al., 2018).

El modelo de Bass supone que las influencias subjetivas externas e internas que funcionan a través de los efectos de red afectan las interdependencias del consumidor. La suposición subyacente del modelo es que la función de riesgo (la probabilidad de que una persona adopte el producto en el momento *t*, dado que todavía no lo ha adoptado) es la siguiente (Huang & Chen, 2010):



(1) $$\frac{f(t)}{1-F(t)} = p + qF(t),$$

Cuya función de densidad acumulativa es:

(2) $$F(t) = \frac{1-e^{-(p+q)t}}{1+\frac{q}{p}e^{-(p+q)t}}$$

Y la función de densidad de probabilidad es:

(3) $$f(t) = \frac{\frac{(p+q)^2}{p}e^{-(p+q)t}}{\left(1+\frac{q}{p}e^{-(p+q)t}\right)^2}.$$

Finalmente:

(4) $$\frac{N(t)}{Y(t)} = \frac{M}{Y(t)}F(t) = mF(t).$$

Figura 15. Ecuaciones del modelo Bass
Fuente: Tomado de (Huang & Chen, 2010)

En estas ecuaciones, *p* captura influencias externas, *q* captura influencias internas, N (t) es el número acumulado de adoptantes en el momento *t*, Y (t) es la población en el sistema de mercado de interés en el momento *t*, M es el número esperado de adoptantes del mercado a largo plazo, y *m* es el nivel de penetración final esperado del mercado. Numerosas publicaciones académicas han utilizado con éxito el modelo en cientos de categorías que van desde bienes de consumo envasados hasta artículos duraderos para el hogar y desde servicios hasta productos industriales. El modelo Bass es uno de los pocos modelos en ciencias del marketing que es lo suficientemente robusto y ha acumulado una cantidad sustancial de estudios empíricos de tal manera que es posible una generalización empírica (Huang & Chen, 2010).

El modelo Bass es una base fundamental que se utiliza para el modelado también de la difusión de enfermedades como el Covid-19 y de ataques de malware.

7.5.4. Modelo SEIR

Los modelos comportamentales simplifican el modelado matemático de enfermedades infecciosas. La población se asigna a compartimentos con etiquetas, por ejemplo, *S*, *I* o

R (Susceptible, Infeccioso o Recuperado). Las personas pueden progresar entre los distintos estados. El orden de las etiquetas generalmente muestra los patrones de flujo entre los estados; por ejemplo, SEIS significa Susceptible, Expuesto, Infeccioso, luego Susceptible nuevamente. Los modelos se ejecutan en mayor frecuencia con ecuaciones diferenciales ordinarias, pero también se pueden usar con un marco estocástico, que es más realista pero mucho más complicado de analizar. Los modelos intentan predecir cosas como cómo se propaga una enfermedad, o el número total de infectados, o la duración de una epidemia, y estimar varios parámetros epidemiológicos como el número reproductivo.

La acción de los malware a través de una red puede estudiarse mediante el uso de modelos epidemiológicos para la propagación de enfermedades. Basado en el modelo SEIR, es posible establecer modelos dinámicos para la propagación de objetos maliciosos, proporcionando estimaciones de las evoluciones temporales de los nodos infectados dependiendo de los parámetros y los aspectos topológicos de la red (Mishra & Jha, 2010)

El modelo SEIR fue creado con el objetivo de analizar la propagación del virus en redes, particularmente, sociales. Cada nodo en la figura representa a un usuario. El borde conecta el nodo *i* y el nodo *j* representa que el usuario *i* y el usuario *j* que tienen relación. Este modelo define el número de usuarios en la lista de contactos como el grado de este nodo. De acuerdo con las reglas de propagación del virus, los nodos son divididos en cuatro categorías: susceptibles (S), expuestos (E), infecciosos (I) y recuperados (R). Los nodos susceptibles representan aquellos que son capaces de contraer virus; los nodos expuestos representan a quienes están infectados, pero aún no son infecciosos; los puntos infecciosos representan a aquellos infectados y capaces de transmitir la enfermedad; y los nodos recuperados representan a aquellos que son inmunes permanentemente (S & L, 2015). El modelo SEIR define las reglas de propagación de virus de la siguiente manera:

- Si un nodo susceptible contacta con un nodo infeccioso, entonces la probabilidad de que el nodo susceptible se transmita a un nodo expuesto es *P*.
- Un nodo expuesto transmitirá a un nodo infeccioso con la velocidad sin contacto con ningún otro nodo.
- Un nodo infeccioso no propagará virus sin cesar. Un nodo infeccioso transmitirá a un nodo recuperado con la velocidad, sin contacto con ningún otro nodo.

Adicionalmente, el modelo SEIR sirve para analizar la dinámica de contagio de temas coyunturales como la pandemia SARS-Covid 2. La (Figura 16) muestra cómo las personas se mueven a través de cada estado del modelo. La línea discontinua muestra cómo el modelo SEIR se convierte en un modelo SEIRS (Susceptible - Expuesto - Infeccioso - Recuperado - Susceptible), donde las personas recuperadas pueden volverse susceptibles nuevamente ya que no está científicamente comprobado que la recuperación confiera inmunidad (Institute for Disease Modeling, 2020).

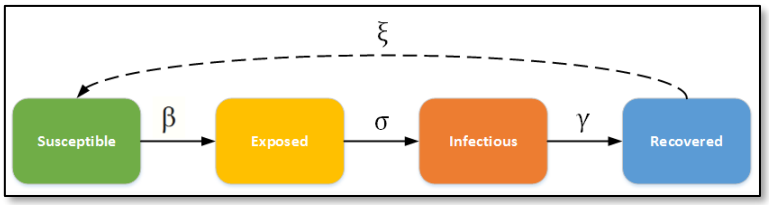


Figura 16. Modelo SEIR
Fuente: Tomado de (Institute for Disease Modeling, 2020)

La tasa infecciosa, β beta, controla la tasa de propagación que representa la probabilidad de transmitir enfermedades entre un individuo susceptible e infeccioso. La tasa de incubación, σ sigma, es la tasa de individuos latentes que se vuelven infecciosos (la duración promedio de la incubación es 1 / σ, sigma). La tasa de recuperación, γ gamma = 1 / D, está determinada por la duración promedio, D, de la infección. Para el modelo SEIRS, ξ (xi) es la tasa que los individuos recuperados regresan al estado susceptible debido a la pérdida de inmunidad (Institute for Disease Modeling, 2020).

7.5.5. Investigaciones y ecuaciones diferenciales para SEIR y botnets

El modelo IoT-BAI utiliza una variación del proceso epidémico SEIRS (Susceptible-Expuesto-Infectado-Recuperado-Susceptible) con el fin de identificar el modelo de propagación y los diferentes estados de los dispositivos en una red. Para la ejecución del modelo, están establecidos los siguientes parámetros representados en la (Tabla 21).

Tabla 21. Parámetros modelo IoT-BAI

Parámetro	Descripción
α	Velocidad de contacto
β	Tasa Expuesto-Infectado
Φ_1	Tasa Infectado-Recuperado (Fase de crecimiento)
Φ_2	Tasa Expuesto-Recuperado (Fase de crecimiento)
Φ_3	Tasa Susceptible-Recuperado (Fase de crecimiento)
Φ'_1	Tasa Infectado-Recuperado (Fase de reducción)
Φ'_2	Tasa Expuesto-Recuperado (Fase de reducción)
Φ'_3	Tasa Susceptible-Recuperado (Fase de reducción)
μ	Tasa de Recuperado-Susceptible
λ	Tasa de nuevos huéspedes
Υ	Tasa de protección de nuevos huéspedes
N	Población total
BRP	Tiempo final de la fase de reducción del botnet

Fuente: Tomado de (Gardner et al., 2017)

Las transiciones básicas son las siguientes: para pasar de Susceptible a Expuesto, un huésped infectado debe haber contactado con un equipo sin malware. Cada huésped infectado puede contactar hasta α equipos por hora. Los contactos se hacen al azar en toda la población. Por lo tanto, algunos de los equipos se encuentran en estados distintos de Susceptible cuando se contactan con ellos (Gardner et al., 2017).

Al no tomarse medidas, la proporción de equipos susceptibles que están expuestos es la proporción de huéspedes infectados a la población total multiplicada por la tasa de contacto. La situación puede surgir cuando el número de huéspedes infectados es tan alto que la proporción de estos con respecto a la población total multiplicada por la tasa de contacto es mayor que 1.0, lo que aquí se conoce como el punto de saturación. En este caso, se supone que todos los equipos susceptibles están en transición a ser expuestos (Gardner et al., 2017).

β, representa la tasa de transición de los huéspedes de expuestos a infectados. Esto representa la vulnerabilidad de los equipos al malware. En el caso específico de Mirai,

el malware estaba específicamente dirigido a dispositivos IoT no seguros. Los parámetros Φ_1; Φ_2; Φ_3 son las tasas de recuperación de infectados, expuestos y susceptibles, respectivamente, durante la fase de crecimiento del botnet. En este modelo, estos representan las tasas que los usuarios reinician sus dispositivos y sus contraseñas. La fase de reducción de botnet se ingresa cuando el número de hosts infectados excede el umbral de ataque y continúa durante el tiempo de reducción de botnet (Gardner et al., 2017).

μ representa la tasa de transición de huéspedes de recuperado a susceptible. Esta es la tasa por la que los usuarios no protegen sus dispositivos después de las actualizaciones de software y restablece o permite que los firewalls se vean comprometidos sin reparación. Finalmente, λ representa la tasa de nuevos equipos que ingresan a la población como dispositivos inicialmente susceptibles. Usando el enfoque de análisis clásico para modelos epidémicos, se define el siguiente conjunto de ecuaciones diferenciales representados en la (Tabla 22).

Tabla 22. Ecuaciones asociadas al modelo IoT-BAI

(1)

$$\frac{dS}{dt} = \lambda(1-\gamma) + \mu R(t) - \frac{\alpha I(t) S(t)}{N(t)} - \Phi_3 S(t)$$

(2)

$$\frac{dE}{dt} = \frac{\alpha I(t) S(t)}{N(t)} - (\beta + \Phi_2) E(t)$$

(3)

$$\frac{dI}{dt} = \beta \mathrm{E(t)} - \Phi_1 I(t)$$

(4)

$$\frac{dR}{dt} = \lambda\gamma + \Phi_1 I(t) + \Phi_2 E(t) + \Phi_3 S(t) - \mu R(t)$$

Donde:

(5)

$$N(t) = I(t) + E(t) + S(t) + R(t)$$

Fuente: Tomado de (Gardner et al., 2017)

7.5.6. Parámetros y desarrollo del modelo de propagación

El objetivo de esta sección es modelar un incidente de Botnet utilizando Dinámica de Sistemas debido a los rasgos de esta forma de simulación. También se introdujo previamente que la mayoría de los modelos utilizan ecuaciones diferenciales.

Después de muchos meses de investigación sobre modelos de propagación en dinámica de sistemas y no encontrar referentes para ser usados en este documento, decidimos elaborar el modelo nosotros mismos.

Después de estudiar el modelo IOT-BAI que es el más avanzado y apoyado por varios contratos con la Fundación Nacional de Ciencias (*National Science Foundation*) de USA, se decidió representarlo como un modelo de Dinámica de Sistemas. La (Figura 17) muestra el modelo y basados en las (Tabla 21), (Tabla 22) y (Figura 16. Este es el primer modelo de Dinámica de Sistemas que hemos observado para esta situación.

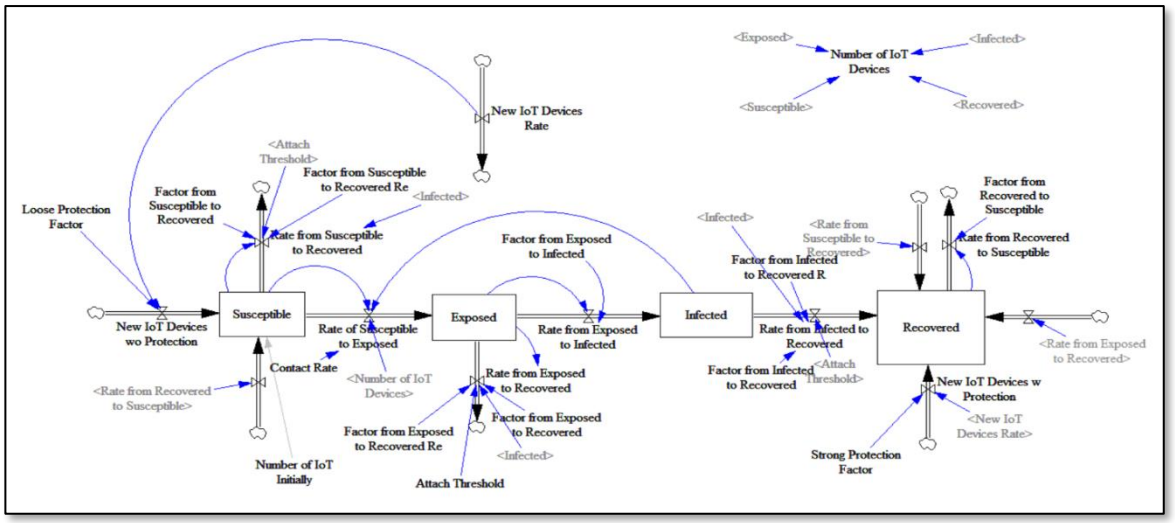


Figura 17. Modelo de Dinámica de Sistemas SEIR para modelar Botnets

Fuente: Elaboración propia

También, recopilamos información del Mirai Botnet para poder reproducirlo y así estudiarlo y analizar cómo se hubieran podido contrarrestar sus ataques. Después de una búsqueda y ver docenas de artículos no se pudo encontrar la información del

número de dispositivos infectados por hora. Así que decidimos buscar información de ataques similares y se logró encontrar información sobre el Sartori Botnet, como variante de Mirai Botnet.

El 15 de junio de 2018, se detectó un aumento del escaneo de actividad maliciosa y el Sartori Botnet infectó una variedad de dispositivos IoT para aprovechar vulnerabilidades recientemente descubiertas (Figura 18). La carga útil, nunca vista, es entregada por el infame Sartori Botnet, aprovechando una forma de propagación de estilo gusano. Se observó un aumento exponencial en el número de fuentes de ataque repartidas por todo el mundo y alcanzando un máximo de más de 2500 atacantes en solo período de 24 horas (Figura 19) (Figura 20) (Figura 21).

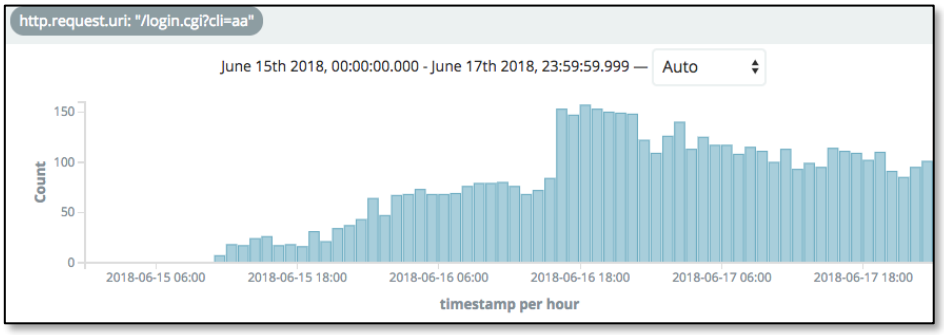


Figura 18. Ataque a dispositivos D-Link del 16 de julio de 2018

Fuente: Tomado de (Radware, 2018)

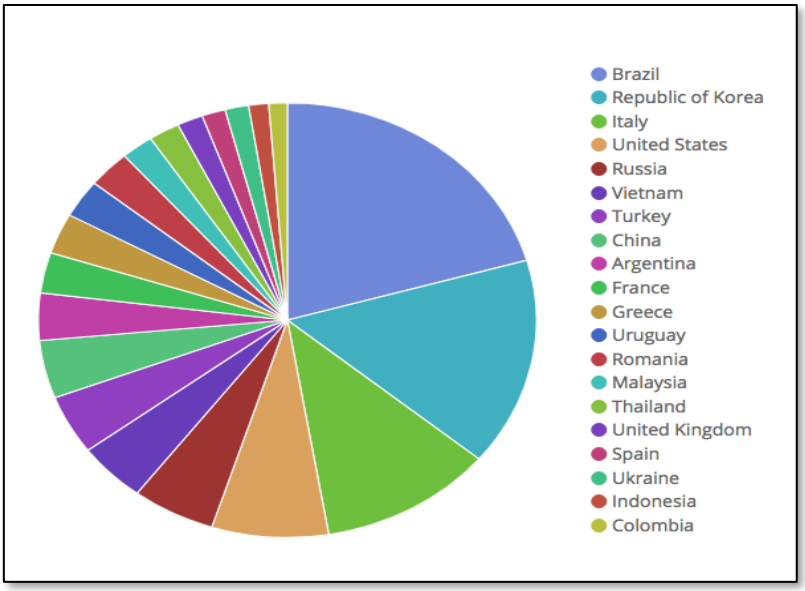


Figura 19. Grafica de Infecciones por país

Fuente: Tomado de (Radware, 2018)

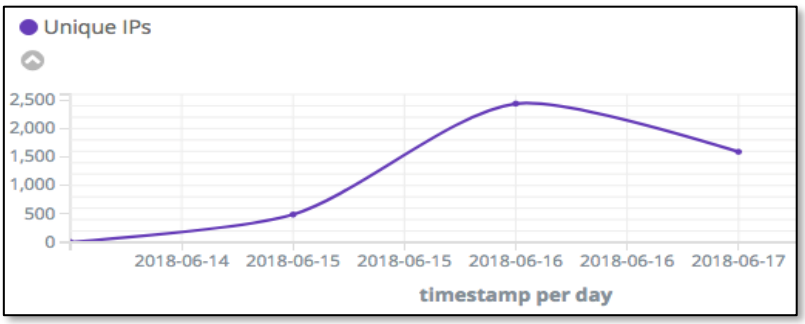


Figura 20. IPs infectados durante un periodo de 72 horas en junio del 2018

Fuente: Tomado de (Radware, 2018)

Lo interesante es que el Sartori Botnet solo atacaba el enrutador D-Link DSL-2750B y también como las cámaras XiongMai uc-httpd 1.0.0 que tuvieron que ser retiradas del mercado por la Compañía China XiongMai (Figura 19), aproximadamente 10,000 de estas cámaras.

Figura 21. Dispositivos explotados por el Sartori Botnet

Fuente: Basado en (Radware, 2018)

Estudiando los parámetros, pudimos en forma sistemática reducir el modelo de la (Figura 17) y empezar a ver como reproducíamos la curva de infección de la (Figura 20).

Se utilizó una de las adiciones de Vensim (www.vensim.com), para hacer optimización estocástica. El Markovian Chain Monte Carlo Simulation (Chib & Greenberg, 1996) fue usado para que los rangos propuestos de la investigación se ajustaran y pudiéramos reproducirla. La (Figura 22) y (Figura 23) muestran el modelo y también la reproducción del ataque del Sartori Botnet con muy buena exactitud.

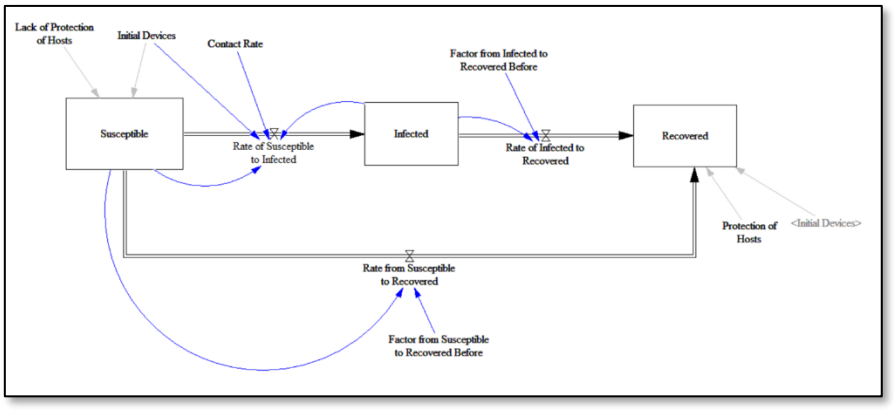


Figura 22. Modelo de Dinámica de Sistemas SIR para modelar el Sartori Botnet

Fuente: Elaboración propia

El modelo utiliza una ecuación diferencial para los susceptibles, otra ecuación diferencial para los infectados, y la tercera para los aparatos recobrados. El parámetro

por obtener de la optimización estocástica fue el *Factor de Susceptible a Recobrados* ("Factor from Susceptible to Recovered Before") que el inverso denota una constante de tiempo. El rango de este factor basados en la literatura (Wang et al., 2017) iba de 0.01/horas a menos de 0.2/horas. La optimización encontró para este factor el valor de 0.033/horas. También, la optimización encontró el valor del Factor de Infectados a Recobrados ("Factor from Infected to Recovered Before") que resultó en 0.5/horas (y el rango fue de 0.02/horas a 0.2/horas de acuerdo con la literatura (Wang et al., 2017)).

Otro valor importante fue encontrar la tasa de contacto y la optimización encontró que fue de 0.45 (que es bastante alta debido a las vulnerabilidades encontradas en los aparatos atacados). Por su parte, la (Figura 23) muestra el resultado después de la optimización estocástica. La línea roja es la curva real de la propagación del Sartori Botnet y la línea verde de la gráfica muestra los reproducido por el modelo de Dinámica de Sistemas desarrollado.

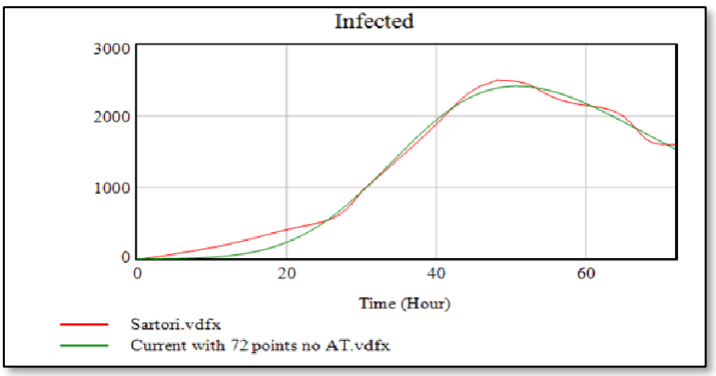


Figura 23. Resultados encontrados en la simulación de Sartori Botnet

Fuente: Elaboración propia

7.5.7. Análisis de sensibilidad aplicado al modelo

Se hicieron dos análisis de sensibilidad. Uno de ellos fue asumir que había un umbral de ataque (limite) con los cuales las actividades de ataques para tratar de infectar a las cámaras y enrutadores es detectada. Este umbral de ataque ("Attack Threshold") es una cantidad de direcciones IP únicas dentro de un intervalo de cuatro horas que podría

indicar que hay un ataque que se está desarrollando. O sea que aumento repentino de direcciones IP únicas dentro de un período de cuatro horas podría indicar un ataque DDoS. Esto se puede hacer con sistemas de "honeypots" y como lo que hace la compañía Akamai (Akamai, 2020) con sus centros de seguridad en el cual llevan estadísticas y tablero con métricas respectivas en tiempo real ("real-time").

Un "honeypot" es un conjunto de computadoras o sistema informático destinado para imitar objetivos probables de ataques cibernéticos. Se puede usar para detectar ataques o desviarlos de un objetivo legítimo. También se puede utilizar para obtener información sobre cómo operan los ciberdelincuentes (Loras R, 2000). Los "honeypots" son un tipo de tecnología de engaño que le permite comprender los patrones de comportamiento del atacante. Los equipos de seguridad pueden usar "honeypots" para investigar las infracciones de ciberseguridad para recopilar información sobre cómo operan los delincuentes cibernéticos. También reducen el riesgo de falsos positivos, en comparación con las medidas tradicionales de ciberseguridad, porque es poco probable que atraigan actividades legítimas (Imperva, 2020).

Hay dos tipos principales de diseños de "honeypots":

- Honeypots de producción: sirven como sistemas señuelo dentro de redes y servidores completamente operativos, a menudo como parte de un sistema de detección de intrusos (IDS). Desvían la atención criminal del sistema real mientras analizan la actividad maliciosa para ayudar a mitigar las vulnerabilidades.

- Honeypots de investigación, utilizados con fines educativos y para mejorar la seguridad. Contienen datos rastreables que puede rastrear cuando son robados para analizar el ataque (Loras R, 2000).

Como se puede ver en la (Figura 25) el modelo y los resultados para los umbrales de ataque de 1000 y 1500 IP infectados. La (Figura 26) muestra las gráficas y la línea azul corresponde a una respuesta al ataque cuando llega a 1000 IP infectados y la línea roja a una respuesta al ataque cuando el umbral de ataque llega a 1500 IP infectados.

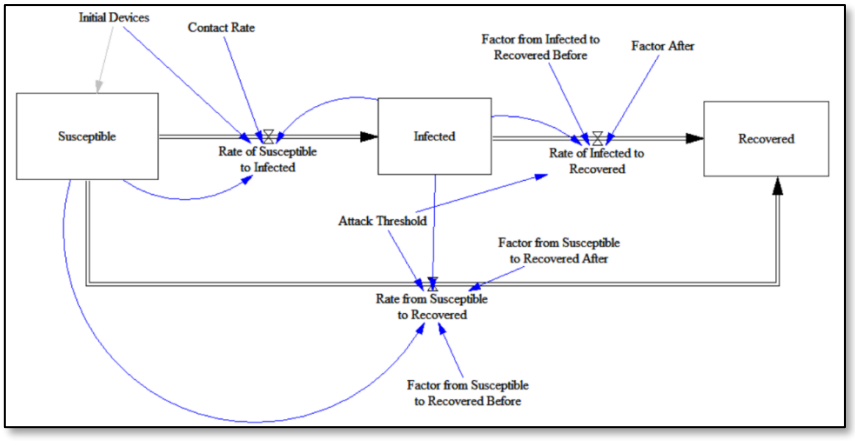


Figura 24. Modelo modificado para implementar el umbral "Attack Threshold"

Fuente: Elaboración propia

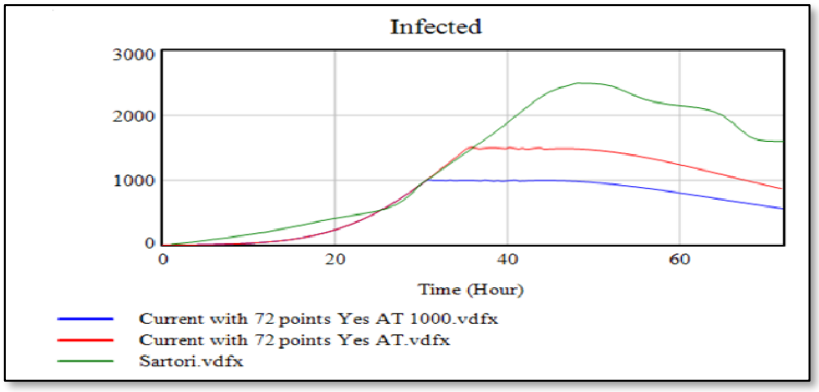


Figura 25. Resultados de la simulación en umbral de 1500 dispositivos.

Fuente: Elaboración propia

Se puede ver lo eficiente de este umbral, pero puede ser costoso el desarrollo de centros de seguridad con los respectivos sensores en la red. Al igual tener una red numerosa de "honeypots" también puede llegar a ser muy costoso.

El segundo experimento asume que de la población de 50,000 D-Link DSL-2750B enrutadores también como las cámaras XiongMai uc-httpd 1.0.0 un 20% de ellas tenían un buen mantenimiento desde el punto de vista de implementación de prácticas de ciberseguridad. O sea, que posiblemente las contraseñas seguían las políticas adecuadas y se renovaban las contraseñas periódicamente. Se puede ver en la (Figura 26) que solo con un 20% de aparatos que siguieran posiblemente los procesos adecuados de seguridad se reduciría drásticamente el número de IPs infectados.

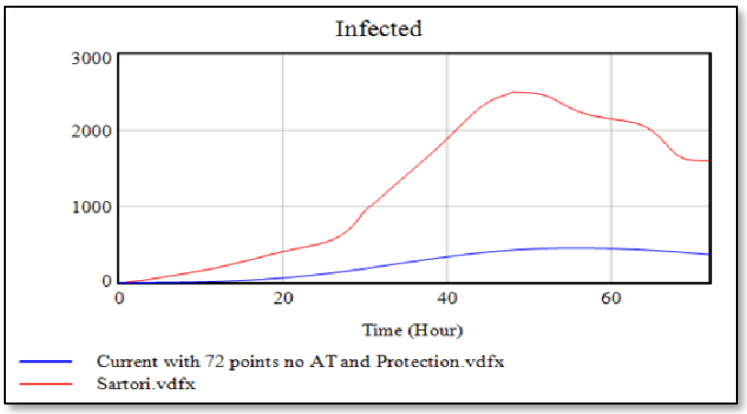


Figura 26. Resultados de la simulación con cambio en seguridad.
Fuente: Elaboración propia

La (Figura 26) nos muestra el resultado con la línea azul que muestra los IPs que serían infectados si el 20% de los ruteadores D-Link DSL-2750B enrutadores también como las cámaras XiongMai uc-httpd siguieran un esquema responsable/disciplinado de políticas de ciberseguridad. Esto también incluye el desarrollo de “patches” y una política disciplinada de hacer renovarlos regularmente.

Estos hallazgos nos llevaron a concluir que el comportamiento de la propagación de Sartori Botnet y el modelo de dinámico de sistemas son muy similares lo que nos permite reusarlo para generar otros modelos de simulación y otros casos de propagación de botnets.

7.6. Caso de estudio: Solución de Gestión de Salas de Cirugía

Cada día más, las soluciones tecnológicas que se utilizan en los diferentes ámbitos económicos empiezan a incorporar nuevos dispositivos como los IoT. Es palpable la presencia de IoT en el sector salud y por supuesto en clínicas y hospitales pues su inmensa ayuda en los ciclos de atención a los pacientes los convierte en una herramienta imprescindible.

Hoy en día, la información sobre los tiempos, procedimientos y los procesos internos en una Clínica u Hospital le permiten a la entidad medica recopilar, identificar y analizar sus puntos flacos y gordos, todo esto para buscar mejorar u optimizar el servicio hacia sus clientes, aunque muy seguramente la construcción de todo un ciclo de mejora continua les tome algunos años. Desde la atención básica en urgencias hasta procesos de cirugías y hospitalización de pacientes en Unidades especiales como las UCI, será común exigir documentar, digitalizar y automatizar los procesos y procedimientos.

Una solución de medición, control y análisis del uso de salas de cirugía en una clínica u hospital es una herramienta tecnológica de apoyo a la coordinación del entorno de ingreso, valoración, salas de cirugía, optimizando el tiempo de atención y la comunicación hacia los equipos asistenciales, pacientes y familiares involucrados.

7.6.1. Beneficios de la Solución de Gestión de Salas de Cirugía

a. Tomar decisiones en tiempo real
b. Optimizar los flujos de trabajo del personal asistencial
c. Disminuir el tiempo de recambio en salas
d. Comunicar información del paciente al familiar
e. Mejorar la satisfacción del paciente y su equipo asistencial

7.6.2. Diagrama de alto nivel de una Solución de Gestión de Salas de Cirugías

A continuación, se presenta el diagrama de alto nivel por capas y equipos que están presentes en una solución de gestión de salas de cirugía (Figura 27).

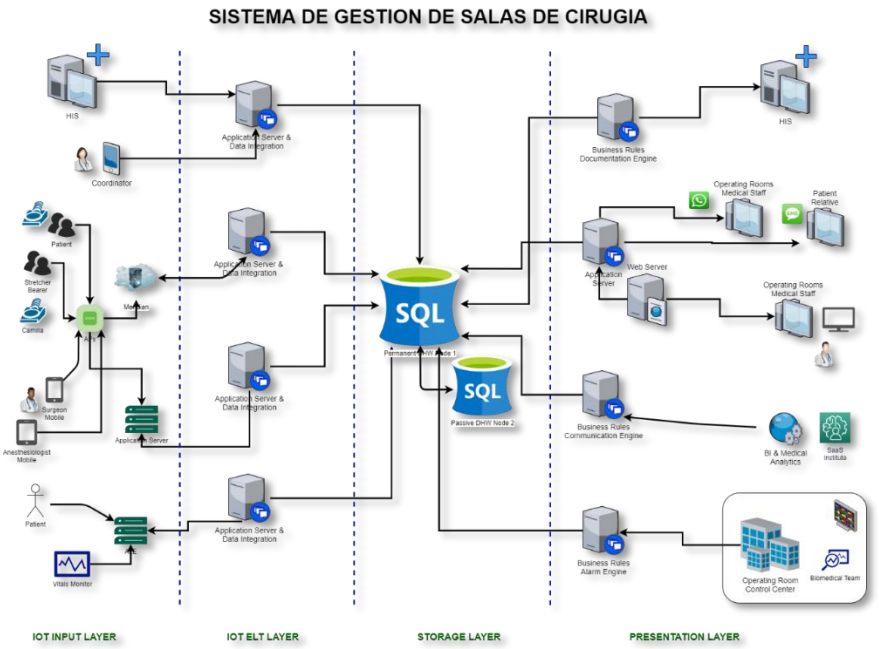


Figura 27. Diagrama de alto nivel de una Solución de Gestión de Salas de Cirugía

Fuente: Adaptado de la una solución de la Compañía SAS

A partir del diagrama anterior hemos construido una matriz de los dispositivos (Tabla 23), y una breve descripción de sus funciones y características de la solución, para iniciar la identificación de los potenciales riesgos.

Tabla 23. Descripción de dispositivos y equipos de la solución

Capa	Equipo / Dispositivo	Que hace y que información Entrega y/o Recibe	Protocolo de red	Sistema Operativo	Virtual	Recursos / Puertos	Medio	Autenticación / Acceso
IOT INPUT LAYER	HIS	Información sobre el paciente y la programación de su cirugía, hay datos personales, procedimientos a realizar, datos del cirujano, anestesiólogo	TCP/IP	Granja de servidores Windows u otro	No	445 (SMB)	Ethernet	Con usuario y contraseña
IOT ELT LAYER	Data Integration 1	Extrae la información del HIS, analiza y selecciona la	TCP/IP	CentOS	Si usa VMWARE	22	Ethernet	Con usuario y contraseña

Capa	Equipo / Dispositivo	Que hace y que información Entrega y/o Recibe	Protocolo de red	Sistema Operativo	Virtual	Recursos / Puertos	Medio	Autenticación / Acceso
		que es necesaria para el proceso						
IOT INPUT LAYER	Localizadores	Entrega y recibe información nueva al DB a través de un App y corrige información sobre las salas y pacientes	TCP/IP	Android / iOS	No	N.D	Wireless	Con usuario y contraseña
IOT INPUT LAYER	Tag Paciente	Envía información de ubicación del paciente, MAC Address, Id y potencia	Bluetooth	N.D	No	N.D	Wireless	N.D
IOT INPUT LAYER	Tag Camillero	Envía información de ubicación del camillero, MAC Address, Id y potencia	Bluetooth	N.D	No	N.D	Wireless	N.D
IOT INPUT LAYER	Tag Camilla	Envía información de ubicación de la camilla, MAC Address, Id y potencia	Bluetooth	N.D	No	N.D	Wireless	N.D
IOT ELT LAYER	Meridian	Solución de trazabilidad de activos como los Tags, identifica la localización de los tags a través de la información del APN	TCP/IP	N.D	No	Puertos de red	Ethernet	Con usuario y contraseña
IOT INPUT LAYER	APN	Registra los Tags, Recibe de los Tags la potencia y el movimiento, tiene el mapa de las salas y envía esta información a Meridian	Bluetooth - TCP/IP	N.D	No	N.D	Wireless / Ethernet	N.D
IOT ELT LAYER	Data Integration 2	Recibe información desde Meridian de la localización del tag para insertarlo en la DB	TCP/IP	CentOS	Si usa VMWARE	22	Ethernet	Con usuario y contraseña
IOT INPUT LAYER	Dispositivo Movil de Cirujano 1	Envía la geolocalización al ALE para saber que el medico está en el área de cobertura de la WiFi de la clínica	TCP/IP	Android / iOS	No	Puertos de red	Wireless	Con usuario y contraseña
IOT INPUT LAYER	Dispositivo Movil de Cirujano 2	Envía la geolocalización al ALE para saber que el medico está en el área de cobertura de la WiFi de la clínica	TCP/IP	Android / iOS	No	Puertos de red	Wireless	Con usuario y contraseña
IOT ELT LAYER	ALE (RTLS)	Recopila la información de las MAC de los Dispositivo Movil de Cirujano 1 y 2 , lo geolocaliza	TCP/IP	CentOS	Si usa VMWARE	22, 2345	Ethernet	N.D
IOT ELT LAYER	AIRWAVE	Imagen de Aruba similar al ALE que permite configurar y registrar los APs y los SW LAN	TCP/IP	CentOS	Si usa VMWARE	22	Ethernet	Con usuario y contraseña
IOT ELT LAYER	Smartlinx	Servidor de Captura de información medica	TCP/IP	Windows	No	Puertos de red	Ethernet	Con usuario y contraseña
IOT INPUT LAYER	Anesthesia machine	Ventilador mecánico para la respiración del paciente y a través de el se suministra la anestesia	HL7	N.D	No	N.D	Serial	N.D
IOT INPUT LAYER	Vitals Monitor	Monitor de signos vitales, oximetría etc.	HL7	N.D	No	N.D	Serial	N.D
IOT ELT LAYER	Capsule AON	Multipuerto de conexión serial a ethernet, sus funciones es servir de puente entre equipo médico y equipos de la solución	HL7 - TCP/IP	N.D	No	90,019,020	Serial / Ethernet	N.D

Capa	Equipo / Dispositivo	Que hace y que información Entrega y/o Recibe	Protocolo de red	Sistema Operativo	Virtual	Recursos / Puertos	Medio	Autenticación / Acceso
IOT ELT LAYER	Capsule MDIP	Identificación, clasificación de señales que vienen de los equipos de sala como anestesia y monitor de signos vitales además recibe toda la información de estado del dispositivo, energía, baterías, que tiene y que no conectado, configuración, etc.	TCP/IP	Windows Server	No	Directorio Activo	Ethernet	Con usuario y contraseña
RULES LAYER	Data Integration 3	Servidores de mediación para la capa ETL entre los otros equipos, exponen un Json de mediador de información	TCP/IP	Linux	Si usa VMWARE	22	Ethernet	Con usuario y contraseña
RULES LAYER	Data Integration 4	Servidores de mediación para la capa ETL entre los otros equipos, exponen un Json de mediador de información	TCP/IP	Linux	Si usa VMWARE	22	Ethernet	Con usuario y contraseña
STORAGE LAYER	DB1	Bases de datos de toda la información recopilada en IoT input y Layer	TCP/IP	CentOS	No	22, 5443	Ethernet	Con usuario y contraseña
STORAGE LAYER	DB2	Bases de datos de toda la información recopilada en IoT input y Layer	TCP/IP	CentOS	No	22, 5443	Ethernet	Con usuario y contraseña
STORAGE LAYER	DB3	Bases de datos de toda la información recopilada en IoT input y Layer	TCP/IP	CentOS	No	225,443	Ethernet	Con usuario y contraseña
RULES LAYER	Business Rule Documentation Engine	Servidor mediador de la información de la DB hacia servicios de terceros, expone o usa generalmente Json	TCP/IP	CentOS	Si usa VMWARE	443	Ethernet	Con usuario y contraseña
RULES LAYER	Aplication Server	Servidor que expone un servicio web donde informa estado de la cirugía, tiempos de salas y recambio.	TCP/IP	CentOS	Si usa VMWARE	22,80,443	Ethernet	Con usuario y contraseña

Fuente: Elaboración propia basado en información de la compañía SAS

7.7. Análisis de los procesos de la Solución de Gestión de Salas de Cirugías utilizando Simulación de Eventos Discretos

Asumiendo que un malware similar al Sartori Botnet atacara la Solución de Gestión de Salas de Cirugía descrito anteriormente y siguiendo los flujos de la información y de procesos de la (Figura 27) y la (Tabla 23) se decidió a hacer un modelo de simulación de eventos discretos. Este modelo de simulación de eventos discretos nos diría del impacto en las salas de cirugía de las políticas y mecanismos de ciberseguridad. Se escogió el modelo de simulación de eventos discretos ya que es el mejor para modelar procesos (en este caso de cirugías) y también los modelos de simulación de eventos

discretos son los más utilizados para modelar hospitales, salas de emergencia, y de cirugías (Zhang 2018). Ya tenido los parámetros de propagación de un malware como el Sartori Botnet fue solo disponer de esas probabilidades.

La plataforma de simulación de eventos discretos que se utilizo fue la de Simio que es una de las líderes en esta área (www.simio.com). Simio está orientado a objectos y es reconocida para simular salas de hospitales (*Healthcare Modeling and Decision Making During Pandemics: A Case Study*). El modelo represento los flujos de la (Figura 27) y la (Tabla 23) como está demostrado en las (Figura 28 y Figura 29) que muestran los componentes de información y los componentes físicos de la cirugía que también fueron animados para poder validarlos con expertos.

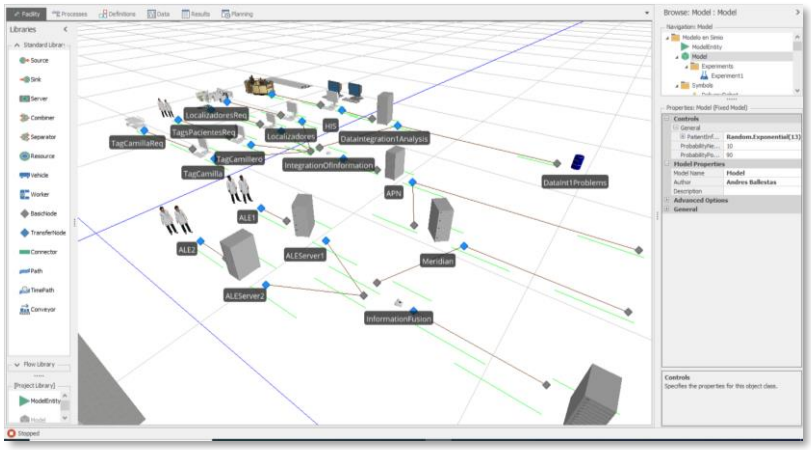


Figura 28. Representación de los componentes de información y de las tecnologías de información para el sistema IoT para cirugías.

Fuente: Elaboración propia.

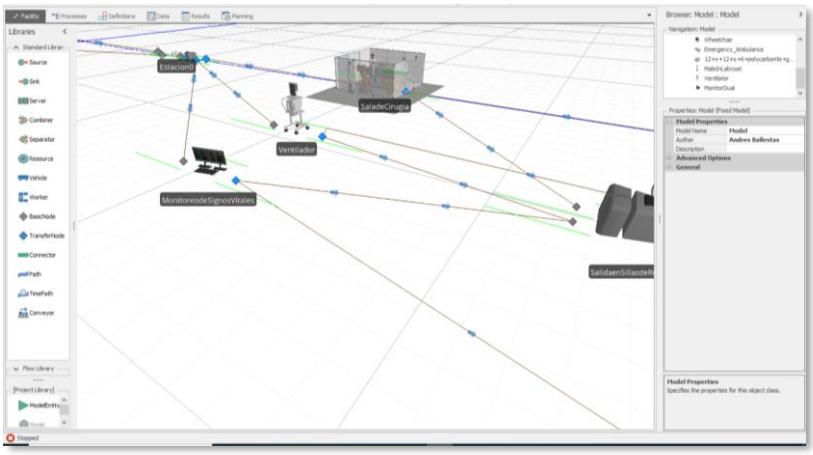


Figura 29. Representación y animación en 3D en el modelo de la parte física de una sala de cirugía con el equipo respectivo necesitado.

Fuente: Elaboración propia.

Los diferentes tiempos utilizados fueron analizados con expertos en medicina y en tecnologías de la información en hospitales. Por ejemplo, la sala que recibe información de los pacientes por teléfono o por internet para un hospital con capacidad para 15 salas de cirugías simultaneas puede modelarse con una distribución exponencial con un tiempo promedio de 13 a15 minutos (Figura 28). También, es importante decir que las salas de cirugías trabajan de lunes a Domingo y en los siguientes turnos:

- De 6:30am a 7:30pm, 15 salas de cirugía
- De 7:30pm a 5:00am, 5 salas de cirugía

Para la cirugía asistida por robots hay buenas referencias de hospitales de Orlando (Florida) como el Orlando Health (que está considerado en algunas áreas en el Tier 1 de hospitales con uso de nuevas tecnologías) y que suministraron información sobre tiempos mínimos de aproximadamente 141 minutos, los tiempos más probables como 182 minutos, y tiempos máximos de 250 minutos (utilizando como ejemplo procedimientos urológicos) y lo que refleja una distribución triangular.

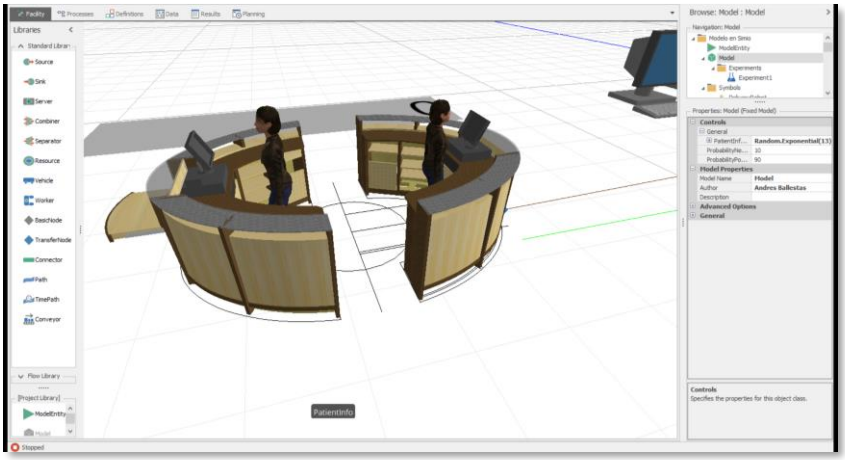


Figura 30. Registración de los pacientes e inicialización del proceso de cirugía de un paciente en el modelo de simulación de eventos discretos.

Fuente: Elaboración propia utilizando la plataforma SIMIO de simulación.

7.8. El análisis con el modelo de simulación de eventos discretos

Se ejecuta con tres escenarios tales como una política débil de ciberseguridad lo que significa que se tienen pocos controles en actualizaciones de seguridad, una política mediana que supone la implementación de algún control de actualización de seguridad, y una política de alta seguridad (muy estricta) donde todos los grupos están concientizados y siguen los procedimientos con absoluta disciplina – no estamos considerando infiltración por un error humano en el sistema (algún recurso que involuntariamente permita acceso de un tercero).

Se ejecutó el modelo 200 veces (réplicas) para cada uno de los escenarios (debido a las variaciones estadísticas) y para un periodo de 2 meses. Un mes se utilizó para conseguir la estabilización del sistema y las estadísticas solo correspondieron al segundo mes. La comparación de los 3 escenarios para el numero de cirugías exitosas o sea aquellas que fueron hechas sin interrupción al momento adecuado y que el equipo IoT funcionó bien fue de 2069 en promedio en un mes para el escenario de una ciberseguridad de nivel fuerte y bien disciplinada. El intervalo de confiabilidad del promedio fue del 95% de 2063 a 2075 con una desviación standard de 6 – básicamente el hospital en las salas de

cirugía tiene un número aproximado mensual entre 2050 a 2100 cirugías. Cuando el nivel de ciberseguridad fue medio, entonces el promedio de cirugías exitosas fue de 2010 y con una desviación estándar de 6 (y el intervalo de confiabilidad del promedio del 95%). Finalmente, cuando el nivel de ciberseguridad fue de políticas débiles y muy relajado el promedio de cirugías exitosas fue de 1074 con una desviación standard de 4 (y el intervalo de confiabilidad del promedio del 95%).

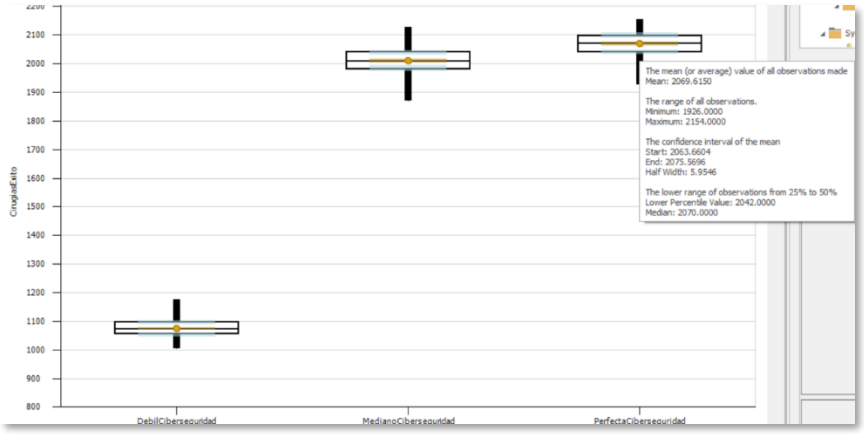


Figura 31. Número de Cirugías Exitosas es mayor con una ciberseguridad disciplinada y bien ejecutada (en promedio con 3315 cirugías exitosas).

Fuente: Elaboración propia usando SIMIO para la simulación.

Otra medida fue la del número de historias clínicas de los pacientes comprometidos desde el punto de vista de CIA (Confidentiality, Integrity & Availability, por sus siglas en ingles). Este número de incidentes de CIA fue de 0 (en un mes) para el escenario de una ciberseguridad de nivel fuerte y bien disciplinada. Cuando el nivel de ciberseguridad fue medio, entonces el promedio de incidentes de CIA fue de 41 y con una desviación estándar de 2 (y el intervalo de confiabilidad del promedio del 95%).

Finalmente, cuando el nivel de ciberseguridad fue de políticas débiles y muy relajado el promedio de incidentes mensual fue de 771 con una desviación standard de 4 (y el intervalo de confiabilidad del promedio fue del 95%, ejecutando 200 réplicas - (Figura 32)).

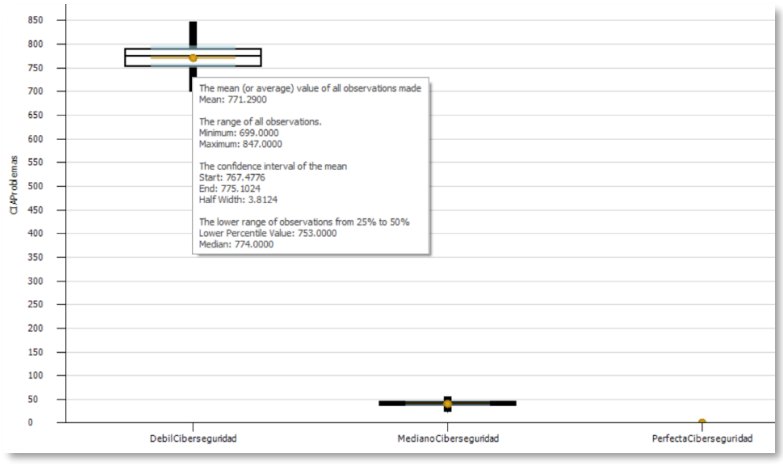


Figura 32. El número de incidencias de CIA con la información de los pacientes para cada escenario de ciberseguridad, usando 200 réplicas de ejecución.

Fuente: Elaboración propia usando SIMIO para la simulación.

Otra medida investigada fue el de cirugías con problemas. Cirugías con problemas fue en las cuales los diferentes aparatos de IoT envueltos en la cirugía demostraron problemas. Estos problemas del equipo pudieron afectar el éxito de una cirugía (esto también incluye que el tiempo se extendió debido a problemas con el equipo). Este número de cirugías con problemas fue de 0 (en un mes) para el escenario de una ciberseguridad de nivel fuerte y bien disciplinada. Cuando el nivel de ciberseguridad fue medio, entonces el promedio de cirugías con problemas fue de 25 y con una desviación estándar de 1 (y el intervalo de confiabilidad del promedio del 95% - (Figura 33)). Finalmente, cuando el nivel de ciberseguridad fue de políticas débiles y muy relajado el promedio mensual de cirugías con problemas fue de 226 con una desviación standard de 2 (y el intervalo de confiabilidad del promedio del 95%).

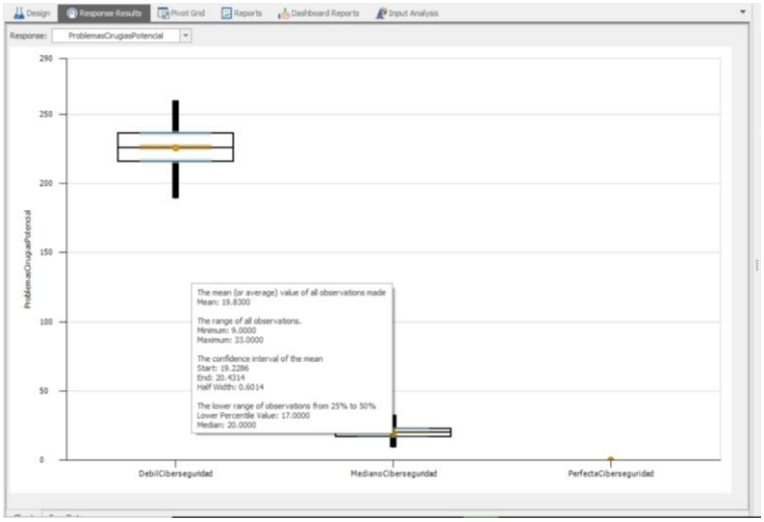


Figura 33. El número potencial de cirugías con problemas para cada escenario de ciberseguridad

Fuente: Elaboración propia usando SIMIO para la simulación.

En la (Figura 33) se utilización 200 réplicas de ejecución de casa escenario. Se utilizaron 60 días de simulación y de esos los primeros 30 días para lograr la estabilización del sistema y la recolección de estadísticas de los últimos 30 días.

7.9. Análisis de Riesgos para la Solución de Gestión de Salas de Cirugía

La evaluación de riesgos generalmente se entiende como el proceso de identificación, estimación y priorización de riesgos para los activos y operaciones de la organización o los diferentes sectores de evaluación. Esta es una actividad crítica dentro de la gestión de riesgos, ya que proporciona la base para los riesgos identificados a tratar. Los enfoques de evaluación de riesgos de ciberseguridad han proporcionado una plataforma a través de la cual las organizaciones y los gobiernos podrían protegerse mejor contra los riesgos pertinentes. Sin embargo, a medida que aumenta la complejidad, la omnipresencia y la automatización de los sistemas tecnológicos, particularmente con el Internet de las Cosas (IoT), existe un fuerte argumento sobre la necesidad de nuevos enfoques para evaluar el riesgo y generar confianza (Nurse et al., 2017).

Para la identificación de los Riesgos se utilizó la técnica de recopilación de información denominada “Tormenta de Ideas”. Por medio de está, se obtuvo una lista inicial de treinta y cinco (35) posibles eventos que impactan positiva o negativamente la solución de gestión de salas de cirugía.

La tormenta de ideas se llevó a cabo entre el director de tesis, algunos consultores de la compañía SAS y el estudiante. Allí se desarrollaron las siguientes actividades:

- Se identificaron los riesgos los cuales fueron nombrados y descritos.
- Se les asigno un identificador de riesgo (R1, R2, …, Rn)
- Se agruparon aquellos que fuesen comunes, a fin de analizarlos como si fuesen un solo riesgo.
- Se les califico el tipo de riesgo (negativo o positivo)
- Se asignó el tipo de acción a seguir según el tipo de riesgo, de acuerdo con la siguiente (Tabla 24).

Tabla 24. Riesgos negativos y positivos

Para Riesgos Negativos	Para Riesgos Positivos
Mitigar	Explotar
Transferir	Compartir
Evitar	Mejorar
Aceptar	Aceptar

Fuente: Adaptado de Norma NTC-5254

7.9.1. Identificación de los riesgos

Los resultados de este ejercicio fueron la asignación de las acciones a los respectivos riegos (Tabla 25).

Tabla 25. Matriz de riesgos por capas de servicio de la solución

ID	Capa	Nombre del riesgo	Descripción del riesgo	Tipo de riesgo	Tipo de acción
R1	IOT INPUT LAYER	Un dispositivo de la clínica u hospital no entrega o recibe información por desconexión u otro problema	Un dispositivo no entrega la información entonces pueden producir fallas en el análisis y diagnóstico del paciente. Pueden producirse procesos adicionales de validación y corrección de la información clínica del paciente y ocasionar retrasos en los ciclos de cirugía.	Negativo	Mitigar
R2	IOT INPUT LAYER	Un dispositivo de la clínica u hospital contiene información errada o alterada del paciente	Registro de información con incongruencias sobre la historia clínica del paciente que puede afectar el diagnostico, injerir negativamente en el suministro de medicinas y conducir a la realización de un procedimiento no adecuado	Negativo	Mitigar
R3	IOT INPUT LAYER	Un dispositivo de la solución no tiene conexión o algún componente esta defectuoso o esta apagado	La información que el dispositivo produce puede impactar la decisión de iniciar la cirugía o reportar que ya ha finalizado causando problemas de facturación	Negativo	Mitigar
R4	IOT INPUT LAYER	La información de los pacientes en el dispositivo de la solución está sin actualizar	La información del paciente y el diagnostico medico no está al día con todos los comentarios y exámenes pudiendo afectar el suministro de algún medicamento	Negativo	Mitigar
R5	IOT INPUT LAYER	Un tercero puede acceder a la información de los pacientes en los dispositivos de la solución	Si alguien no autorizado accede y altera la información clínica del paciente, puede recibir el diagnostico incorrecto y realizársele un procedimiento diferente o suministrársele un medicamento no necesario para su tratamiento	Negativo	Mitigar
R6	IOT INPUT LAYER	Un dispositivo presenta fallas por llegar a la edad de obsolescencia	El dispositivo no recibe actualizaciones y su operación presentada alguna falla que puede afectar las mediciones que realiza al paciente e informar con errores de una condición de salud incorrecta provocando alguna decisión medica sobre la condición del paciente	Negativo	Aceptar
R7	IOT INPUT LAYER	Un dispositivo no permite que accedan a su interfaz de gestión	Un equipo no permite que accedan a su configuración mientras envía información incorrecta a otros dispositivos afectando la integridad de la información clínica del paciente	Negativo	Mitigar

ID	Capa	Nombre del riesgo	Descripción del riesgo	Tipo de riesgo	Tipo de acción
R8	IOT INPUT LAYER	El Wi-Fi de los dispositivos están apagados	La solución desconoce la presencia física del cuerpo médico en las instalaciones de la Clínica u Hospital lo que causaría que la cirugía se retrase e impacte en los costos del procedimiento	Negativo	Aceptar
R9	IOT INPUT LAYER	El sistema operativo y/o los programas de los dispositivos de la solución están sin actualizaciones	Las actualizaciones del dispositivo no están al día entonces podrían permitir que una o varias vulnerabilidades de software sean explotadas y ser usado como medio para alcanzar otros dispositivos y generar indisponibilidad del servicio	Negativo	Mitigar
R10	IOT ELT LAYER	Un dispositivo presenta una falla al recibir la información de otros sistemas de la Clínica u Hospital	El dispositivo no logra recibir la información de otro dispositivo del Hospital o Clínica causando que la información no se puede procesar y reenviar a los demás dispositivos que toman decisiones y podrían causar retrasos en las cirugías y afectación en los costos del procedimiento	Negativo	Mitigar
R11	IOT ELT LAYER	Un tercero puede acceder a la información de los pacientes en los dispositivos de la solución	Si alguien no autorizado accede y altera la información clínica del paciente, este puede recibir el diagnostico inadecuado, realizársele un procedimiento incorrecto o suministrársele un medicamento no necesario	Negativo	Mitigar
R12	IOT ELT LAYER	Se presenta una falla de alguna VM de un equipo de la solución	Si la VM falla en algún momento puede ocasionar que el flujo de servicio se interrumpa, se afecte el agendamiento de las salas de cirugía, incurriendo en sobrecostos y podría afectar la historia clínica de los pacientes	Negativo	Mitigar
R13	IOT ELT LAYER	Un dispositivo tiene uno o varios errores en el código Json	Si el equipo no puede procesar la información a través del Json la información no podría seguir ayudando al servicio y podría interrumpir el ciclo de uso de las salas de cirugía	Negativo	Mitigar
R14	IOT ELT LAYER	Un dispositivo de la solución no tiene conexión o algún componente esta defectuoso o esta apagado	La información que el dispositivo produce puede impactar la decisión de iniciar la cirugía o reportar que ya ha finalizado causando problemas de facturación	Negativo	Mitigar

ID	Capa	Nombre del riesgo	Descripción del riesgo	Tipo de riesgo	Tipo de acción
R15	IOT ELT LAYER	El sistema operativo y/o los programas de los dispositivos de la solución están sin actualizaciones	Las actualizaciones del dispositivo no están al día entonces podrían permitir que una o varias vulnerabilidades de software sean explotadas y ser usado como medio para alcanzar otros dispositivos y generar indisponibilidad del servicio	Negativo	Mitigar
R16	IOT ELT LAYER	Un dispositivo de la solución no entrega la información correctamente a otros dispositivos	Un dispositivo puede producir fallas en el análisis y diagnóstico del paciente al no entregar la información correctamente	Negativo	Mitigar
R17	IOT ELT LAYER	Un dispositivo de la solución contiene información errada o alterada del paciente	Si se registra información con incongruencias sobre la historia clínica del paciente pueden diagnosticarlo con errores, suministrar medicinas equivocadas y/o realizarle un procedimiento no adecuado	Negativo	Mitigar
R18	IOT ELT LAYER	Un dispositivo no permite que accedan a su interfaz de gestión	Un equipo no permite que accedan a su configuración mientras envía información incorrecta a otros dispositivos afectando la integridad de la información clínica del paciente	Negativo	Mitigar
R19	STORAGE LAYER	Un dispositivo presenta una falla al recibir o entregar la información de los otros equipos de la solución	No logra recibir la información de otro dispositivo de la solución causando que la información no se gestione de manera adecuada e impactando el servicio de gestión de las salas con posibles sobrecostos o deterioro del ingreso	Negativo	Mitigar
R20	STORAGE LAYER	Un tercero puede acceder a la información de los pacientes en los dispositivos de la solución	Si alguien no autorizado accede y altera la información clínica del paciente, este puede recibir el diagnostico inadecuado, realizársele un procedimiento incorrecto o suministrársele un medicamento no necesario	Negativo	Mitigar
R21	STORAGE LAYER	Un dispositivo de la solución no tiene conexión o algún componente esta defectuoso o esta apagado	La información que el dispositivo produce puede impactar la decisión de iniciar la cirugía o reportar que ya ha finalizado causando problemas de facturación	Negativo	Mitigar
R22	STORAGE LAYER	Se presenta una falla de alguna VM de un equipo de la solución	Si la VM falla en algún momento puede ocasionar que el fuljo de servicio se interrumpa, se afecte el agendamiento de las salas de cirugía, incurriendo en sobrecostos y podría afectar la	Negativo	Mitigar

ID	Capa	Nombre del riesgo	Descripción del riesgo	Tipo de riesgo	Tipo de acción
			historia clínica de los pacientes		
R23	STORAGE LAYER	El sistema operativo y/o los programas de los dispositivos de la solución están sin actualizaciones	Las actualizaciones del dispositivo no están al día entonces podrían permitir que una o varias vulnerabilidades de software sean explotadas y ser usado como medio para alcanzar otros dispositivos y generar indisponibilidad del servicio	Negativo	Mitigar
R24	STORAGE LAYER	Un dispositivo de la solución contiene información errada o alterada del paciente	Si se registra información con incongruencias sobre la historia clínica del paciente pueden diagnosticarlo con errores, suministrar medicinas equivocadas y/o realizarle un procedimiento no adecuado	Negativo	Mitigar
R25	STORAGE LAYER	Un dispositivo no permite que accedan a su interfaz de gestión	Un equipo no permite que accedan a su configuración mientras envía información incorrecta a otros dispositivos afectando la integridad de la información clínica del paciente	Negativo	Mitigar
R26	STORAGE LAYER	Un dispositivo presenta una falla en la DB	Al existir un problema en la DB, podría alterar el funcionamiento de la solución y su disponibilidad hacia los demás equipos y causar fallas de servicio tanto para los pacientes como para la clínica u hospital	Negativo	Mitigar
R27	RULES LAYER	Un dispositivo presenta una falla al entregar la información a otros sistemas de la Clínica u Hospital	La información no se puede procesar y enviar, lo podría causar retrasos en las cirugías y afectación en los costos del procedimiento	Negativo	Mitigar
R28	RULES LAYER	Un tercero puede acceder a la información de los pacientes en los dispositivos de la solución	Si alguien no autorizado accede y altera la información clínica del paciente, este puede recibir el diagnostico inadecuado, realizársele un procedimiento incorrecto o suministrársele un medicamento no necesario	Negativo	Mitigar
R29	RULES LAYER	Un dispositivo de la solución no tiene conexión o algún componente esta defectuoso o esta apagado	La información que el dispositivo produce puede impactar la decisión de iniciar la cirugía o reportar que ya ha finalizado causando problemas de facturación	Negativo	Mitigar

ID	Capa	Nombre del riesgo	Descripción del riesgo	Tipo de riesgo	Tipo de acción
R30	RULES LAYER	Se presenta una falla de alguna VM de un equipo de la solución	Si la VM falla en algún momento puede ocasionar que el fuljo de servicio se interrumpa, se afecte el agendamiento de las salas de cirugía, incurriendo en sobrecostos y podría afectar la historia clínica de los pacientes	Negativo	Mitigar
R31	RULES LAYER	Un dispositivo tiene uno o varios errores en el código Json	Si el equipo no puede procesar la información a través del Json la información no podría seguir ayudando al servicio y podría interrumpir el ciclo de uso de las salas de cirugía	Negativo	Mitigar
R32	RULES LAYER	El sistema operativo y/o los programas de los dispositivos de la solución están sin actualizaciones	Las actualizaciones del dispositivo no están al día entonces podrían permitir que una o varias vulnerabilidades de software sean explotadas y ser usado como medio para alcanzar otros dispositivos y generar indisponibilidad del servicio	Negativo	Mitigar
R33	RULES LAYER	Un dispositivo de la solución no entrega la información correctamente a otros dispositivos	Un dispositivo no entrega la información correctamente a otras soluciones de terceros podrían producir fallas en la gestión del servicio hacia el paciente	Negativo	Mitigar
R34	RULES LAYER	Un dispositivo de la solución contiene información errada o alterada del paciente	Si se registra información con incongruencias sobre la historia clínica del paciente pueden diagnosticarlo con errores, suministrar medicinas equivocadas y/o realizarle un procedimiento no adecuado	Negativo	Mitigar
R35	RULES LAYER	Un dispositivo no permite que accedan a su interfaz de gestión	Un equipo no permite que accedan a su configuración mientras envía información incorrecta a otros dispositivos afectando la integridad de la información clínica del paciente	Negativo	Mitigar

Fuente: Elaboración propia

Como se puede observar, en esta tabla existen varios riesgos correlacionados, los cuales son (R9,R15,R23,R32); (R12,R22,R30); (R17,R24,R34); (R16,R33); (R3,R14,R21, R29); (R7,R18,R25,R35); (R13, R31) y (R5,R11,R20,R28). Por ello se tratarán de aquí en adelante de R1 a R17 para efectos del presente análisis.

Después de la correlación quedo la siguiente (Tabla 26) para poder continuar con el análisis de riesgos.

Tabla 26. Matriz de riesgos correlacionados por capa de servicio

ID	Capa	Nombre del riesgo	Descripción del riesgo	Tipo de riesgo	Tipo de acción
R1	IOT INPUT LAYER	Un dispositivo de la clínica u hospital no entrega o recibe información por desconexión u otro problema	Un dispositivo no entrega la información entonces pueden producir fallas en el análisis y diagnóstico del paciente. Pueden producirse procesos adicionales de validación y corrección de la información clínica del paciente y ocasionar retrasos en los ciclos de cirugía.	Negativo	Mitigar
R2	IOT INPUT LAYER	Un dispositivo de la clínica u hospital contiene información errada o alterada del paciente	Registro de información con incongruencias sobre la historia clínica del paciente que puede afectar el diagnostico, injerir negativamente en el suministro de medicinas y conducir a la realización de un procedimiento no adecuado	Negativo	Mitigar
R3	IOT INPUT LAYER	Un dispositivo de la solución no tiene conexión o algún componente esta defectuoso o esta apagado	La información que el dispositivo produce puede impactar la decisión de iniciar la cirugía o reportar que ya ha finalizado causando problemas de facturación	Negativo	Mitigar
R4	IOT INPUT LAYER	La información de los pacientes en el dispositivo de la solución está sin actualizar	La información del paciente y el diagnostico medico no está al día con todos los comentarios y exámenes pudiendo afectar el suministro de algún medicamento	Negativo	Mitigar
R5	IOT INPUT LAYER	Un tercero (equipo o persona) puede acceder a la información de los pacientes en los dispositivos de la solución	Si alguien no autorizado accede y altera la información clínica del paciente, puede recibir el diagnostico incorrecto y realizársele un procedimiento diferente o suministrársele un medicamento no necesario para su tratamiento	Negativo	Mitigar
R6	IOT INPUT LAYER	Un dispositivo presenta fallas por llegar a la edad de obsolescencia	El dispositivo no recibe actualizaciones y su operación presentada alguna falla que puede afectar las mediciones que realiza al paciente e informar con errores de una condición de salud incorrecta provocando alguna decisión medica sobre la condición del paciente	Negativo	Aceptar
R7	IOT INPUT LAYER	Un dispositivo no permite que accedan a su interfaz de gestión	Un equipo no permite que accedan a su configuración mientras envía información incorrecta a otros dispositivos afectando la integridad de la información clínica del paciente	Negativo	Mitigar
R8	IOT INPUT LAYER	El Wi-Fi de los dispositivos están apagados	La solución desconoce la presencia física del cuerpo médico en las instalaciones de la Clínica u Hospital lo que causaría que la cirugía se retrase e impacte en los costos del procedimiento	Negativo	Aceptar
R9	IOT INPUT LAYER	El sistema operativo y/o los programas de los dispositivos de la solución están sin actualizaciones	Las actualizaciones del dispositivo no están al día entonces podrían permitir que una o varias vulnerabilidades de software sean explotadas y ser usado como medio para alcanzar otros dispositivos y generar indisponibilidad del servicio	Negativo	Mitigar

ID	Capa	Nombre del riesgo	Descripción del riesgo	Tipo de riesgo	Tipo de acción
R10	IOT ELT LAYER	Un dispositivo de la solución presenta una falla al recibir la información de otros equipos de la Clínica u Hospital	El dispositivo no logra recibir la información de otro dispositivo del Hospital o Clínica causando que la información no se puede procesar y reenviar a los demás dispositivos que toman decisiones y podrían causar retrasos en las cirugías y afectación en los costos del procedimiento	Negativo	Mitigar
R11	IOT ELT LAYER	Se presenta una falla de alguna VM de un equipo de la solución	Si la VM falla en algún momento puede ocasionar que el flujo de servicio se interrumpa, se afecte el agendamiento de las salas de cirugía, incurriendo en sobrecostos y podría afectar la historia clínica de los pacientes	Negativo	Mitigar
R12	IOT ELT LAYER	Un dispositivo tiene uno o varios errores en el código Json	Si el equipo no puede procesar la información a través del Json la información no podría seguir ayudando al servicio y podría interrumpir el ciclo de uso de las salas de cirugía	Negativo	Mitigar
R13	IOT ELT LAYER	Un dispositivo de la solución no entrega la información correctamente a otros dispositivos de 3ros	Un dispositivo puede producir fallas en el análisis y diagnóstico del paciente al no entregar la información correctamente	Negativo	Mitigar
R14	IOT ELT LAYER	Un dispositivo de la solución contiene información errada o alterada del paciente	Si se registra información con incongruencias sobre la historia clínica del paciente pueden diagnosticarlo con errores, suministrar medicinas equivocadas y/o realizarle un procedimiento no adecuado	Negativo	Mitigar
R15	STORAGE LAYER	Un dispositivo presenta una falla al recibir o entregar la información de los otros equipos de la solución	No logra recibir la información de otro dispositivo de la solución causando que la información no se gestione de manera adecuada e impactando el servicio de gestión de las salas con posibles sobrecostos o deterioro del ingreso	Negativo	Mitigar
R16	STORAGE LAYER	Un dispositivo presenta una falla en la DB o alguno de sus componentes	Al existir un problema en la DB, podría alterar el funcionamiento de la solución y su disponibilidad hacia los demás equipos y causar fallas de servicio tanto para los pacientes como para la clínica u hospital	Negativo	Mitigar
R17	RULES LAYER	Un dispositivo presenta una falla al entregar la información a otros equipos de la Clínica u Hospital	La información no se puede procesar y enviar, lo podría causar retrasos en las cirugías y afectación en los costos del procedimiento	Negativo	Mitigar

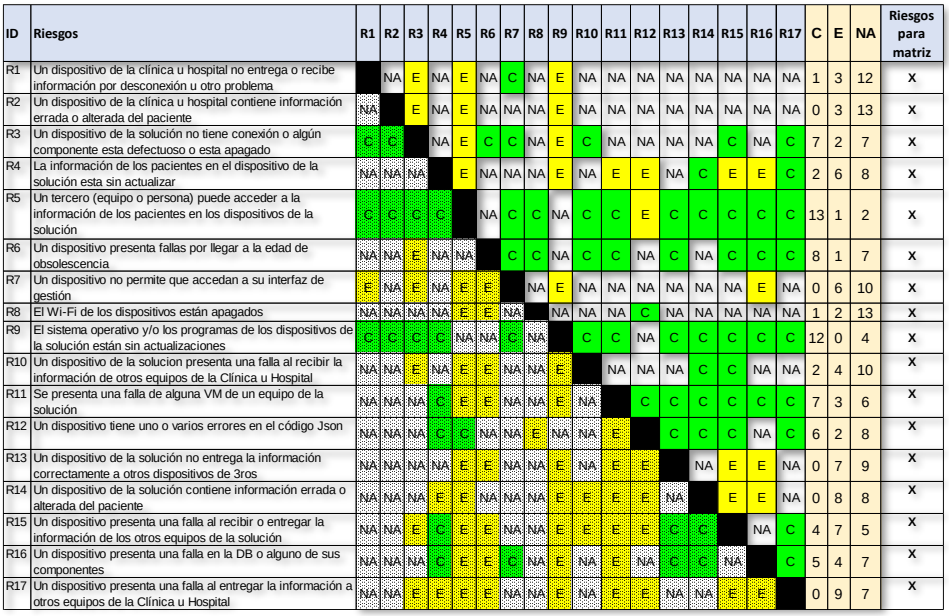
Fuente: Elaboración propia

7.9.2. Priorización de los riesgos

Con el fin de llevar a cabo la priorización de los riegos, se elaboró una matriz causa efecto de cada uno de los riesgos. Los que se intenta determinar a través de esta matriz es la relación causa-efecto que puede existir entre los riesgos mismos.

De esta forma, se atacarían los riesgos que pueden ser causa potencial de la aparición de otros, de manera que se tomarían acciones sobre los riesgos que causan la mayor aparición de riesgos efecto.

De esta manera se generó la siguiente matriz (Figura 34) de priorización de riesgos.



ID	Riesgos	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	C	E	NA	Riesgos para matriz
R1	Un dispositivo de la clínica u hospital no entrega o recibe información por desconexión u otro problema		NA	E	NA	E	NA	C	NA	E	NA	NA	NA	NA	NA	NA	NA	NA	1	3	12	X
R2	Un dispositivo de la clínica u hospital contiene información errada o alterada del paciente	NA		E	NA	E	NA	NA	NA	E	NA	NA	NA	NA	NA	NA	NA	NA	0	3	13	X
R3	Un dispositivo de la solución no tiene conexión o algún componente esta defectuoso o esta apagado	C	C		NA	E	C	C	NA	E	C	NA	NA	NA	NA	C	NA	C	7	2	7	X
R4	La información de los pacientes en el dispositivo de la solución esta sin actualizar	NA	NA	NA		E	NA	NA	NA	E	NA	E	E	NA	C	E	E	C	2	6	8	X
R5	Un tercero (equipo o persona) puede acceder a la información de los pacientes en los dispositivos de la solución	C	C	C	C		NA	C	C	NA	C	C	E	C	C	C	C	C	13	1	2	X
R6	Un dispositivo presenta fallas por llegar a la edad de obsolescencia	NA	NA	E	NA	NA		C	C	NA	C	C	NA	C	NA	C	C	C	8	1	7	X
R7	Un dispositivo no permite que accedan a su interfaz de gestión	E	NA	E	NA	E	E		NA	E	NA	NA	NA	NA	NA	NA	E	NA	0	6	10	X
R8	El Wi-Fi de los dispositivos están apagados	NA	NA	NA	NA	E	E	NA		NA	NA	NA	C	NA	NA	NA	NA	NA	1	2	13	X
R9	El sistema operativo y/o los programas de los dispositivos de la solución están sin actualizaciones	C	C	C	C	NA	NA	C	NA		C	C	NA	C	C	C	C	C	12	0	4	X
R10	Un dispositivo de la solucion presenta una falla al recibir la información de otros equipos de la Clínica u Hospital	NA	NA	E	NA	E	E	NA	NA	E		NA	NA	NA	C	C	NA	NA	2	4	10	X
R11	Se presenta una falla de alguna VM de un equipo de la solución	NA	NA	NA	C	E	E	NA	NA	E	NA		C	C	C	C	C	C	7	3	6	X
R12	Un dispositivo tiene uno o varios errores en el código Json	NA	NA	NA	C	C	NA	NA	E	NA	NA	E		C	C	C	NA	C	6	2	8	X
R13	Un dispositivo de la solución no entrega la información correctamente a otros dispositivos de 3ros	NA	NA	NA	NA	E	E	NA	NA	E	NA	E	E		NA	E	E	NA	0	7	9	X
R14	Un dispositivo de la solución contiene información errada o alterada del paciente	NA	NA	NA	E	E	NA	NA	NA	E	E	E	E	NA		E	E	NA	0	8	8	X
R15	Un dispositivo presenta una falla al recibir o entregar la información de los otros equipos de la solución	NA	NA	E	C	E	E	NA	NA	E	E	E	E	C	C		NA	C	4	7	5	X
R16	Un dispositivo presenta una falla en la DB o alguno de sus componentes	NA	NA	NA	C	E	E	C	NA	E	NA	E	NA	C	C	NA		C	5	4	7	X
R17	Un dispositivo presenta una falla al entregar la información a otros equipos de la Clínica u Hospital	NA	NA	E	E	E	E	NA	NA	E	NA	E	E	NA	NA	E	E		0	9	7	X

Figura 34. Matriz de priorización de riesgos

Fuente: Elaboración propia

Esta matriz muestra la relación entre los riesgos mismos. De esta forma se deberían seleccionar en la columna denominada “Riesgos para matriz” los riesgos que sean los mayores en causa para realizarles el análisis necesario, en nuestro caso no descartaremos ningún riesgo para realizar un análisis más completo.

7.9.3. Clasificación de los riesgos

Con el fin de analizar los riesgos a los que está expuesta la solución, se desarrolló una tabla (Tabla 27) donde se califica el impacto de cada uno de los riesgos respecto a las áreas de posible impacto como Tiempo, Financiera y Personas, teniendo en cuenta las siguientes tablas para la evaluación de riesgos negativos.

Tabla 27. Matriz de escalas de impacto de riesgos negativos.

MATRIZ DE ESCALAS DE IMPACTO DEL RIESGO NEGATIVO SOBRE LAS ÁREAS DE LA SOLUCIÓN				
		ESCALA DE IMPACTO		
		BAJA	MEDIA	ALTA
OBJETIVO	PONDERACIÓN	1	3	5
TIEMPO	20%	$-10\% \leq \Delta \leq 10\%$	$-15\% \leq \Delta < -10\%$ $10\% < \Delta \leq 15\%$	$\Delta < -15\%$ $15\% < \Delta$
FINANCIERA	35%	$-5\% \leq \Delta \leq 5\%$	$-10\% \leq \Delta < -5\%$ $5\% < \Delta \leq 10\%$	$\Delta < -10\%$ $10\% < \Delta$
PERSONAS	45%	$-5\% \leq \Delta \leq 5\%$	$-10\% \leq \Delta < -5\%$ $5\% < \Delta \leq 10\%$	$\Delta < -10\%$ $10\% < \Delta$

Fuente: Elaboración propia basado en NTC-5254

Además, se califica la probabilidad de ocurrencia del riesgo. De acuerdo con la norma NTC-5254 la posibilidad de que ocurra el riesgo o resultado específico se evalúa de acuerdo con los siguientes parámetros (Tabla 28):

Tabla 28. Condición de ocurrencia del riesgo

Condición	Calificación
Nula	0
Raro: puede ocurrir solamente en circunstancias excepcionales	1
Improbable: podría ocurrir pocas veces	2
Posible: puede ocurrir algunas veces	3
Probable: ocurre en la mayoría de las circunstancias	4
Casi cierto: siempre ocurre	5

Fuente: Basado en NTC-5254

De esta forma, los resultados de la calificación para cada uno de los riesgos (Tabla 29) en las diferentes áreas de impacto (Tiempo, Financiera y Personas), ambiente de control a través del Framework COSO – COBIT (Operaciones) y la probabilidad de ocurrencia de este (Probabilidad).

Tabla 29. Matriz de clasificación y nota de riesgo

Variable	Factor	Riesgo	Nota
Impacto	1-Tiempo	1	3.0
Impacto	2-Financiera	1	2.0
Impacto	3-Personas	1	5.0
Probabilidad	4-Operacion	1	4.0
Probabilidad	5-Probabilidad	1	3.0
Impacto	1-Tiempo	2	4.0
Impacto	2-Financiera	2	4.0
Impacto	3-Personas	2	4.0
Probabilidad	4-Operacion	2	2.0
Probabilidad	5-Probabilidad	2	2.0
Impacto	1-Tiempo	3	2.0
Impacto	2-Financiera	3	3.0
Impacto	3-Personas	3	4.0
Probabilidad	4-Operacion	3	3.0
Probabilidad	5-Probabilidad	3	3.0
Impacto	1-Tiempo	4	4.0
Impacto	2-Financiera	4	5.0
Impacto	3-Personas	4	4.0
Probabilidad	4-Operacion	4	1.0
Probabilidad	5-Probabilidad	4	2.0
Impacto	1-Tiempo	5	3.0
Impacto	2-Financiera	5	3.0
Impacto	3-Personas	5	5.0
Probabilidad	4-Operacion	5	2.0
Probabilidad	5-Probabilidad	5	2.0
Impacto	1-Tiempo	6	4.0
Impacto	2-Financiera	6	-
Impacto	3-Personas	6	4.0
Probabilidad	4-Operacion	6	-

Variable	Factor	Riesgo	Nota
Probabilidad	5-Probabilidad	6	-
Impacto	1-Tiempo	7	1.0
Impacto	2-Financiera	7	2.0
Impacto	3-Personas	7	1.0
Probabilidad	4-Operacion	7	2.0
Probabilidad	5-Probabilidad	7	3.0
Impacto	1-Tiempo	8	2.0
Impacto	2-Financiera	8	4.0
Impacto	3-Personas	8	2.0
Probabilidad	4-Operacion	8	4.0
Probabilidad	5-Probabilidad	8	4.0
Impacto	1-Tiempo	9	5.0
Impacto	2-Financiera	9	5.0
Impacto	3-Personas	9	3.0
Probabilidad	4-Operacion	9	4.0
Probabilidad	5-Probabilidad	9	2.0
Impacto	1-Tiempo	10	2.0
Impacto	2-Financiera	10	1.0
Impacto	3-Personas	10	3.0
Probabilidad	4-Operacion	10	4.0
Probabilidad	5-Probabilidad	10	4.0
Impacto	1-Tiempo	11	3.0
Impacto	2-Financiera	11	3.0
Impacto	3-Personas	11	4.0
Probabilidad	4-Operacion	11	2.0
Probabilidad	5-Probabilidad	11	3.0
Impacto	1-Tiempo	12	1.0
Impacto	2-Financiera	12	3.0
Impacto	3-Personas	12	2.0

Variable	Factor	Riesgo	Nota
Probabilidad	4-Operacion	12	4.0
Probabilidad	5-Probabilidad	12	1.0
Impacto	1-Tiempo	13	2.0
Impacto	2-Financiera	13	3.0
Impacto	3-Personas	13	3.0
Probabilidad	4-Operacion	13	1.0
Probabilidad	5-Probabilidad	13	2.0
Impacto	1-Tiempo	14	1.0
Impacto	2-Financiera	14	1.0
Impacto	3-Personas	14	2.0
Probabilidad	4-Operacion	14	2.0
Probabilidad	5-Probabilidad	14	1.0
Impacto	1-Tiempo	15	4.0
Impacto	2-Financiera	15	3.0
Impacto	3-Personas	15	2.0
Probabilidad	4-Operacion	15	3.0
Probabilidad	5-Probabilidad	15	4.0
Impacto	1-Tiempo	16	2.0
Impacto	2-Financiera	16	1.0
Impacto	3-Personas	16	3.0
Probabilidad	4-Operacion	16	2.0
Probabilidad	5-Probabilidad	16	2.0
Impacto	1-Tiempo	17	3.0
Impacto	2-Financiera	17	4.0
Impacto	3-Personas	17	3.0
Probabilidad	4-Operacion	17	2.0
Probabilidad	5-Probabilidad	17	1.0

Fuente: Elaboración propia

7.9.4. Magnitud del Impacto

Impacto y probabilidad son dos componentes principales del análisis de riesgos, observar el impacto versus la probabilidad es común para clasificar y priorizar los riesgos, ya que algunos riesgos pueden tener un impacto severo en los objetivos de los proyectos, pero solo ocurren en raras ocasiones, mientras que otros tienen un impacto moderado, pero ocurren con mayor frecuencia. Un método comúnmente utilizado para la evaluación del riesgo es preparar escalas descriptivas para clasificar el riesgo en términos de probabilidad e impacto. A menudo se les conoce como matriz de impacto y probabilidad y pueden tomar valores tanto cualitativos como numéricos. Este es un método simple y fácil de entender para priorizar riesgos y asignar a futuro recursos necesario para la mitigación (Thorhallsdóttir, 2018).

Respecto a las calificaciones realizadas a los riegos, se llevó a cabo el cálculo de la magnitud de impacto, de manera que se pueda observar cuales son los riesgos que puede llegar a impactar en mayor medida la solución (Tabla 30). Así se obtuvo la siguiente información.

Tabla 30. Matriz de Magnitud de Impacto

		Magnitud del impacto			
RIESGOS		Tiempo	Financiera	Personas	Total Impacto
		20%	35%	45%	100%
R1	Un dispositivo de la clínica u hospital no entrega o recibe información por desconexión u otro problema	3.0	2.0	5.0	3.55
R2	Un dispositivo de la clínica u hospital contiene información errada o alterada del paciente	4.0	4.0	4.0	4.00
R3	Un dispositivo de la solución no tiene conexión o algún componente esta defectuoso o esta apagado	2.0	3.0	4.0	3.25
R4	La información de los pacientes en el dispositivo de la solución está sin actualizar	4.0	5.0	4.0	4.35

RIESGOS		Magnitud del impacto			
		Tiempo	Financiera	Personas	Total Impacto
		20%	35%	45%	100%
R5	Un tercero (equipo o persona) puede acceder a la información de los pacientes en los dispositivos de la solución	3.0	3.0	4.0	3.45
R6	Un dispositivo presenta fallas por llegar a la edad de obsolescencia	4.0	0.0	4.0	2.60
R7	Un dispositivo no permite que accedan a su interfaz de gestión	1.0	2.0	1.0	1.35
R8	El Wi-Fi de los dispositivos están apagados	2.0	4.0	2.0	2.70
R9	El sistema operativo y/o los programas de los dispositivos de la solución están sin actualizaciones	5.0	5.0	3.0	4.10
R10	Un dispositivo de la solución presenta una falla al recibir la información de otros equipos de la Clínica u Hospital	2.0	1.0	3.0	2.10
R11	Se presenta una falla de alguna VM de un equipo de la solución	3.0	3.0	4.0	3.45
R12	Un dispositivo tiene uno o varios errores en el código Json	1.0	3.0	2.0	2.15
R13	Un dispositivo de la solución no entrega la información correctamente a otros dispositivos de 3ros	2.0	3.0	3.0	2.80
R14	Un dispositivo de la solución contiene información errada o alterada del paciente	1.0	1.0	2.0	1.45
R15	Un dispositivo presenta una falla al recibir o entregar la información de los otros equipos de la solución	4.0	3.0	2.0	2.75
R16	Un dispositivo presenta una falla en la DB o alguno de sus componentes	2.0	1.0	3.0	2.10

RIESGOS		Magnitud del impacto			
		Tiempo	Financiera	Personas	Total Impacto
		20%	35%	45%	100%
R17	Un dispositivo presenta una falla al entregar la información a otros equipos de la Clínica u Hospital	3.0	4.0	3.0	3.35

Fuente: Elaboración propia

7.9.5. Probabilidad de ocurrencia

Respecto a las calificaciones realizadas a los riegos, se llevó a cabo el cálculo de la probabilidad de ocurrencia (Tabla 31), de manera que se pueda observar cuales son los riesgos que puede llegar a materializarse en mayor medida en el proyecto.

Tabla 31. Matriz de probabilidad de ocurrencia

RIESGOS		Probabilidad de ocurrencia		
		Operaciones	Probabilidad	Total Probabilidad
		40%	60%	100%
R1	Un dispositivo de la clínica u hospital no entrega o recibe información por desconexión u otro problema	4.0	3.0	3.40
R2	Un dispositivo de la clínica u hospital contiene información errada o alterada del paciente	1.0	3.0	2.20
R3	Un dispositivo de la solución no tiene conexión o algún componente esta defectuoso o esta apagado	2.0	2.0	2.00
R4	La información de los pacientes en el dispositivo de la solución está sin actualizar	3.0	2.0	2.40
R5	Un tercero (equipo o persona) puede acceder a la información de los pacientes en los dispositivos de la solución	2.0	4.0	3.20
R6	Un dispositivo presenta fallas por llegar a la edad de obsolescencia	2.0	3.0	2.60

		Probabilidad de ocurrencia		
RIESGOS		**Operaciones**	**Probabilidad**	**Total Probabilidad**
		40%	**60%**	**100%**
R7	Un dispositivo no permite que accedan a su interfaz de gestión	2.0	4.0	3.20
R8	El Wi-Fi de los dispositivos están apagados	3.0	3.0	3.00
R9	El sistema operativo y/o los programas de los dispositivos de la solución están sin actualizaciones	3.0	4.0	3.60
R10	Un dispositivo de la solución presenta una falla al recibir la información de otros equipos de la Clínica u Hospital	2.0	1.0	1.40
R11	Se presenta una falla de alguna VM de un equipo de la solución	2.0	2.0	2.00
R12	Un dispositivo tiene uno o varios errores en el código Json	4.0	1.0	2.20
R13	Un dispositivo de la solución no entrega la información correctamente a otros dispositivos de 3ros	3.0	1.0	1.80
R14	Un dispositivo de la solución contiene información errada o alterada del paciente	3.0	4.0	3.60
R15	Un dispositivo presenta una falla al recibir o entregar la información de los otros equipos de la solución	1.0	1.0	1.00
R16	Un dispositivo presenta una falla en la DB o alguno de sus componentes	2.0	2.0	2.00
R17	Un dispositivo presenta una falla al entregar la información a otros equipos de la Clínica u Hospital	1.0	4.0	2.80

Fuente: Elaboración propia

7.9.6. Mapa de riesgos

Una vez calculados los impactos y las probabilidades, calculamos el impacto total de cada uno de los riegos (Tabla 32). Con esta información creamos el Mapa de Riesgos, donde de forma visual podremos observar cuales riesgos son los que debemos atacar.

En este punto, cabe destacar, que esta labor se debería hacer con los riesgos seleccionados. Sin embargo, para efectos los realizaremos con todos los riesgos.

Tabla 32. Matriz de Impacto y Probabilidad

		60%	40%	
RIESGOS		**Impacto**	**Probabilidad**	**Impacto total**
R1	Un dispositivo de la clínica u hospital no entrega o recibe información por desconexión u otro problema	3.55	3.40	3.49
R2	Un dispositivo de la clínica u hospital contiene información errada o alterada del paciente	4.00	2.20	3.28
R3	Un dispositivo de la solución no tiene conexión o algún componente esta defectuoso o esta apagado	3.25	2.00	2.75
R4	La información de los pacientes en el dispositivo de la solución está sin actualizar	4.35	2.40	3.57
R5	Un tercero (equipo o persona) puede acceder a la información de los pacientes en los dispositivos de la solución	3.45	3.20	3.35
R6	Un dispositivo presenta fallas por llegar a la edad de obsolescencia	2.60	2.60	2.60
R7	Un dispositivo no permite que accedan a su interfaz de gestión	1.35	3.20	2.09
R8	El Wi-Fi de los dispositivos están apagados	2.70	3.00	2.82
R9	El sistema operativo y/o los programas de los dispositivos de la solución están sin actualizaciones	4.10	3.60	3.90

		60%	40%	
RIESGOS		**Impacto**	**Probabilidad**	**Impacto total**
R10	Un dispositivo de la solución presenta una falla al recibir la información de otros equipos de la Clínica u Hospital	2.10	1.40	1.82
R11	Se presenta una falla de alguna VM de un equipo de la solución	3.45	2.00	2.87
R12	Un dispositivo tiene uno o varios errores en el código Json	2.15	2.20	2.17
R13	Un dispositivo de la solución no entrega la información correctamente a otros dispositivos de 3ros	2.80	1.80	2.40
R14	Un dispositivo de la solución contiene información errada o alterada del paciente	1.45	3.60	2.31
R15	Un dispositivo presenta una falla al recibir o entregar la información de los otros equipos de la solución	2.75	1.00	2.05
R16	Un dispositivo presenta una falla en la DB o alguno de sus componentes	2.10	2.00	2.06
R17	Un dispositivo presenta una falla al entregar la información a otros equipos de la Clínica u Hospital	3.35	2.80	3.13

Fuente: Elaboración propia.

A continuación, se muestra el mapa de riesgos obtenido para los riesgos analizados.

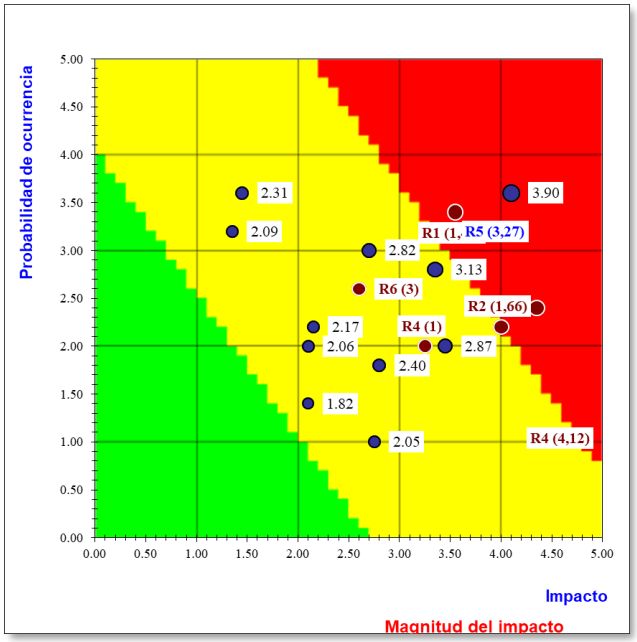


Figura 35. Mapa de criticidad de riesgos

Fuente: Elaboración propia

Del mapa de criticidad riesgos (Figura 35) se puede deducir que 4 representan un riesgo de alto impacto para la solución y que se deben considerar con mayor atención en el plan de mitigación a proponer y se obtuvieron 13 riesgos clasificados en un nivel medio de probabilidad de ocurrencia que también deben tenerse en cuenta en el plan.

7.10. Plan de mitigación de riesgos para la Solución de Gestión de Salas de Cirugía

La Base de Datos de la Gestión de Configuración (CMDB) es una parte esencial en el desarrollo y gestión de software para manejar artefactos dentro de una empresa o institución entre todas las partes relevantes. Su principal objetivo es hacer un seguimiento de los datos relevantes de Elementos de Configuración (CI), que son los artefactos importantes, y sus correspondientes relaciones con otros CI que hagan parte del inventario de la entidad (Berggren, 2020).

Con base en los riegos encontrados y analizados se proponen las siguientes medidas de mitigación (Tabla 33).

Tabla 33. Riesgos y medidas de mitigación

ID	Medidas
R1	1. Fuente redundante de poder 1.1 Circuitos eléctricos diferentes 2. NIC redundante 2.1. Conexiones a switches diferentes 3. Acceso a través de servidores de aplicación en HA o Granja 4. Base de datos en HA
R2	1. Verificación de datos principales con la registraduría (datos, nombres y huellas) 2. Autenticación MFA para los usuarios de la historia clínica. 3. La información de la historia clínica debe estar firmada digitalmente.
R3	Tener dispositivos en inventario, configurados y probados para reemplazo en caso de falla y trámite de RMA del dispositivo dañado
R4	Establecer procedimientos manuales y automatizados de verificación de información de los pacientes comparando con el origen de datos y la información que se encuentra centralizada.
R5	1. Autenticación MFA para los usuarios de la historia clínica. 2. Protección a la base de datos mediante soluciones de DAM o DAP.
R6	Establecer una CMDB mediante un software especializado con el fin de tener el inventario completo de todas las soluciones, los ciclos de EoL y EoS, mantenimientos, actualizaciones y todo lo relacionado.
R7	Establecer un protocolo de pruebas regular que permita establecer el correcto funcionamiento de los dispositivos de la clínica de manera que se garantice el correcto funcionamiento de las soluciones. Esto debe estar en el CMDB.
R8	Definir, documentar, aprobar y socializar una política de uso de los dispositivos la cual debe ser aceptada por los funcionarios médicos para su activación durante las horas de servicio. Incluso una cláusula dentro del contrato.
R9	1. Realizar Análisis de Vulnerabilidades y Pentesting sobre la infraestructura para establecer los planes de mitigación puntual de las soluciones implementadas. 2. Implementar una solución de firewall, IPS y antivirus de perímetro para la inspección de tráfico entre redes de IoT e IT con el fin de proteger los dispositivos de ataques externos. 3. (Operation Guides) Establecer un plan de actualizaciones frecuentes de firmware de los dispositivos de las soluciones de IoT. Esto debe estar en la CMDB
R10	1. Establecer procedimientos de revisión de funcionamiento de los elementos de las soluciones, con protocolos operaciones que permitan garantizar la conectividad y envío y recepción de información dentro del Workflow de la solución. Esto debe estar en la CMDB. 2. Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización de los dispositivos por lo cual se debe incorporar a la CMDB.
R11	Implementar una solución de monitoreo de disponibilidad de hardware y servicios con el fin de generar alarmas y notificaciones de fallas en la solución.
R12	1. Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización de los dispositivos por lo cual se debe incorporar a la CMDB. 2. El fabricante de la solución debe tener procesos establecidos de fábrica de software y desarrollo seguro de software que ayuden a mitigar errores en actualizaciones del producto.

ID	Medidas
R13	1. Establecer procedimientos de revisión de funcionamiento de los elementos de las soluciones, con protocolos operaciones que permitan garantizar la conectividad y envío y recepción de información dentro del Workflow de la solución. Esto debe estar en la CMDB. 2. Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización de los dispositivos por lo cual se debe incorporar a la CMDB.
R14	1. Establecer procedimientos de revisión de funcionamiento de los elementos de las soluciones, con protocolos operaciones que permitan garantizar la conectividad y envío y recepción de información dentro del Workflow de la solución. Esto debe estar en la CMDB. 2. Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización de los dispositivos por lo cual se debe incorporar a la CMDB.
R15	1. Establecer un protocolo de pruebas regular que permita establecer el correcto funcionamiento de los dispositivos de la clínica de manera que se garantice el correcto funcionamiento de las soluciones. Esto debe estar en el CMDB. 2. Establecer procedimientos de revisión de funcionamiento de los elementos de las soluciones, con protocolos operaciones que permitan garantizar la conectividad y envío y recepción de información dentro del Workflow de la solución. Esto debe estar en la CMDB. 3. Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización de los dispositivos por lo cual se debe incorporar a la CMDB. 4. Dentro de lo posible diseñar arquitecturas en HA o redundantes. 5. Establecer procesos robustos de copias de seguridad y configuraciones de acuerdo con las mejores prácticas del fabricante
R16	1. Establecer un protocolo de pruebas regular que permita establecer el correcto funcionamiento de los dispositivos de la clínica de manera que se garantice el correcto funcionamiento de las soluciones. Esto debe estar en el CMDB. 2. Establecer procedimientos de revisión de funcionamiento de los elementos de las soluciones, con protocolos operaciones que permitan garantizar la conectividad y envío y recepción de información dentro del Workflow de la solución. Esto debe estar en la CMDB. 3. Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización de los dispositivos por lo cual se debe incorporar a la CMDB. 4. Dentro de lo posible diseñar arquitecturas en HA o redundantes. 5. Establecer procesos robustos de copias de seguridad y configuraciones de acuerdo con las mejores prácticas del fabricante
R17	1. Establecer protocolos de conexión con terceros de forma segura. 2. Implementar elementos de seguridad que permita tener los accesos controlados. 3. Establecer un protocolo de pruebas regular que permita establecer el correcto funcionamiento de los dispositivos de la clínica de manera que se garantice el correcto funcionamiento de las soluciones. Esto debe estar en el CMDB.

Fuente: Elaboración propia.

De las anteriores medidas es importante mencionar algunas consideraciones comúnmente sugeridas por fabricantes de soluciones de seguridad de la información en bases de datos (McAfee):

- La falta de visibilidad de los datos - no saber exactamente dónde se encuentran los datos sensibles. Es decir, poder identificar en donde y de qué manera se ponen a disposición de otras áreas los datos sensibles de los pacientes.
- El cumplimiento de normativas o nuevas regulaciones, para ofrecer tranquilidad a sus clientes y poder desarrollar nuevos proyectos y programas de infraestructura

De acuerdo con el análisis de riesgos determinamos realizar una correlación de riesgos (Tabla 34) para las medidas de mitigación propuestas.

Tabla 34. Correlación de Medidas de Mitigación

ID	Medidas de mitigación	Riesgos con Medidas Correlacionables
R1	Se requiere que los servidores tengan: 1. Fuente redundante de poder 1.1 Circuitos eléctricos diferentes 2. NIC redundante 2.1. Conexiones a switches diferentes 3. Acceso a través de servidores de aplicación en HA o Granja 4. Base de datos en HA	
R2	1.Verificación de datos principales con la registraduría (datos, nombres y huellas) 2. Autenticación MFA para los usuarios de la historia clínica. 3. La información de la historia clínica debe estar firmada digitalmente.	
R3	1.Tener dispositivos en inventario, configurados y probados para reemplazo en caso de falla y trámite de RMA del dañado	
R4	1. Establecer procedimientos manuales y automatizados de verificación de información de los pacientes comparando con el origen de datos y la información que se encuentra centralizada.	
R5	1.Autenticación MFA para los usuarios de la historia clínica. 2. Protección a la base de datos mediante soluciones de DAM o DAP.	
R6	1. Establecer una CMDB mediante un software especializado con el fin de tener el inventario completo de todas las soluciones, los ciclos de EoL y EoS, mantenimientos, actualizaciones y todo lo relacionado.	
R7	1. Establecer un protocolo de pruebas regular que permita establecer el correcto funcionamiento de los dispositivos de la clínica de manera que se garantice el correcto funcionamiento de las soluciones. Esto debe estar en el CMDB.	

ID	Medidas de mitigación	Riesgos con Medidas Correlacionables
R8	1. Definir, documentar, aprobar y socializar una política de uso de los dispositivos la cual debe ser aceptada por los funcionarios médicos para su activación durante las horas de servicio. Incluso una cláusula dentro del contrato.	
R9	1. Realizar Análisis de Vulnerabilidades y Pentesting sobre la infraestructura para establecer los planes de mitigación puntual de las soluciones implementadas. 2. Implementar una solución de firewall, IPS y antivirus de perímetro para la inspección de tráfico entre redes de IoT e IT con el fin de proteger los dispositivos de ataques externos. 3. (Operation Guides) Establecer un plan de actualizaciones frecuentes de firmware de los dispositivos de las soluciones de IoT. Esto debe estar en la CMDB.	
R10	1. Establecer procedimientos de revisión de funcionamiento de los elementos de las soluciones, con protocolos operaciones que permitan garantizar la conectividad y envío y recepción de información dentro del Workflow de la solución. Esto debe estar en la CMDB. 2. Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización de los dispositivos por lo cual se debe incorporar a la CMDB.	
R11	1. Implementar una solución de monitoreo de disponibilidad de hardware y servicios con el fin de generar alarmas y notificaciones de fallas en la solución. 2. Establecer el protocolo de Gestión de Incidentes con el fin de atender las fallas mencionadas dependiendo del nivel de criticidad de la falla. 3. Dentro de lo posible diseñar arquitecturas en HA o redundantes.	
R12	1. Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización de los dispositivos por lo cual se debe incorporar a la CMDB 2. El fabricante de la solución debe tener procesos establecidos de fábrica de software y desarrollo seguro de software que ayuden a mitigar errores en actualizaciones del producto.	
R13	1. Establecer procedimientos de revisión de funcionamiento de los elementos de las soluciones, con protocolos operaciones que permitan garantizar la conectividad y envío y recepción de información dentro del Workflow de la solución. Esto debe estar en la CMDB. 2. Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización de los dispositivos por lo cual se debe incorporar a la CMDB.	R13 y R14
R14	1. Establecer procedimientos de revisión de funcionamiento de los elementos de las soluciones, con protocolos operaciones que permitan garantizar la conectividad y envío y recepción de información dentro del Workflow de la solución. Esto debe estar en la CMDB. 2. Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización de los dispositivos por lo cual se debe incorporar a la CMDB.	

ID	Medidas de mitigación	Riesgos con Medidas Correlacionables
R15	1. Establecer un protocolo de pruebas regular que permita establecer el correcto funcionamiento de los dispositivos de la clínica de manera que se garantice el correcto funcionamiento de las soluciones. Esto debe estar en el CMDB. 2. Establecer procedimientos de revisión de funcionamiento de los elementos de las soluciones, con protocolos operaciones que permitan garantizar la conectividad y envío y recepción de información dentro del Workflow de la solución. Esto debe estar en la CMDB. 3. Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización de los dispositivos por lo cual se debe incorporar a la CMDB. 4. Dentro de lo posible diseñar arquitecturas en HA o redundantes. 5. Establecer procesos robustos de copias de seguridad y configuraciones de acuerdo con las mejores prácticas del fabricante.	R15 y R16
R16	1. Establecer un protocolo de pruebas regular que permita establecer el correcto funcionamiento de los dispositivos de la clínica de manera que se garantice el correcto funcionamiento de las soluciones. Esto debe estar en el CMDB. 2. Establecer procedimientos de revisión de funcionamiento de los elementos de las soluciones, con protocolos operaciones que permitan garantizar la conectividad y envío y recepción de información dentro del Workflow de la solución. Esto debe estar en la CMDB. 3. Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización de los dispositivos por lo cual se debe incorporar a la CMDB. 4. Dentro de lo posible diseñar arquitecturas en HA o redundantes. 5. Establecer procesos robustos de copias de seguridad y configuraciones de acuerdo con las mejores prácticas del fabricante.	
R17	1. Establecer protocolos de conexión con terceros de forma segura. 2. Implementar elementos de seguridad que permita tener los accesos controlados. 3. Establecer un protocolo de pruebas regular que permita establecer el correcto funcionamiento de los dispositivos de la clínica de manera que se garantice el correcto funcionamiento de las soluciones. Esto debe estar en el CMDB.	

Fuente: Elaboración propia

Hacemos una asociación de riesgos y las categorías en donde pueden impactar la Solución de Gestión de Salas de Cirugía así: Proceso y/o Procedimiento, Política, Tecnología y Recursos Humanos (RRHH). De esta manera relacionamos Riesgos, Aspecto a Mitigar y las Categorías (Tabla 35).

Tabla 35. Asociación de Riesgos, Aspectos y categorías

Categoría	Aspecto de Mitigación	Riesgo Asociado
Proceso y/o procedimiento	Verificación de datos principales de los pacientes con la registraduría (datos, nombres y huellas)	R2

Categoría	Aspecto de Mitigación	Riesgo Asociado
	Autenticación MFA para los usuarios de la historia clínica.	R2, R5
	La información de la historia clínica de cada paciente debe estar firmada digitalmente.	R2
	Establecer procedimientos manuales y automatizados de verificación de información de los pacientes comparando con el origen de datos y la información que se encuentra centralizada.	R4
	Establecer un protocolo de pruebas regular que permita establecer el correcto funcionamiento de los dispositivos de la clínica de manera que se garantice el correcto funcionamiento de las soluciones. Esto debe estar en el CMDB.	R7, R15, R16
	Realizar Análisis de Vulnerabilidades y Pentesting sobre la infraestructura para establecer los planes de mitigación puntual de las soluciones implementadas.	R9
	(Operation Guides) Establecer un plan de actualizaciones frecuentes de firmware de los dispositivos de las soluciones de IoT. Esto debe estar en la CMDB.	R9
	Establecer procedimientos de revisión de funcionamiento de los elementos de las soluciones, con protocolos operaciones que permitan garantizar la conectividad y envío y recepción de información dentro del Workflow de la solución. Esto debe estar en la CMDB.	R10, R13, R14, R15, R16, R17
	El fabricante de la solución debe tener procesos establecidos de fábrica de software y desarrollo seguro de software que ayuden a mitigar errores en actualizaciones del producto.	R12
	Establecer el protocolo de Gestión de Incidentes con el fin de atender las fallas mencionadas dependiendo del nivel de criticidad de la falla.	R11
	Implementar una solución de monitoreo de disponibilidad de hardware y servicios con el fin de generar alarmas y notificaciones de fallas en la solución.	R11
	Establecer protocolos de conexión con terceros de forma segura.	R17
	Implementar elementos de seguridad que permita tener los accesos controlados.	R17
	Establecer procedimientos de Control de Cambios que garanticen la correcta configuración de los dispositivos que componen la solución. Cada cambio debe considerarse como parte de la parametrización y hardenización o robustecimiento de los dispositivos por lo cual se debe incorporar a la CMDB.	R10, R12, R13, R14
Política	Definir, documentar, aprobar y socializar una política de uso de los dispositivos la cual debe ser aceptada por los funcionarios médicos para su activación durante las horas de servicio. Incluso una cláusula dentro del contrato.	R8
Tecnología	Considerar incluir doble fuente de poder en los equipos que lo dispongan	R1
	Conectar los equipos a circuitos eléctricos diferentes	R1
	Incorporar otra NIC a los equipos que lo dispongan	R1
	Conectar a otro equipo de red (switch) redundante disponible	R1
	Equipos configurados en HA	R1
	Protección a la base de datos mediante soluciones de DAM o DAP	R5
	Tener dispositivos en inventario, configurados y probados para reemplazo en caso de falla y trámite de RMA del dañado	R3
	Establecer una CMDB mediante un software especializado con el fin de tener el inventario completo de todas las soluciones, los ciclos de EoL y EoS, mantenimientos, actualizaciones y todo lo relacionado.	R6

Categoría	Aspecto de Mitigación	Riesgo Asociado
	Implementar una solución de firewall, IPS y antivirus de perímetro para la inspección de tráfico entre redes de IoT e IT con el fin de proteger los dispositivos de ataques externos.	R9
	Establecer procesos robustos de copias de seguridad y configuraciones de acuerdo con las mejores prácticas del fabricante.	R15, R16
	Dentro de lo posible diseñar arquitecturas en HA o redundantes.	R11, R15, R16
	Bases de datos configuradas en HA	R1
RRHH	Ninguno	N. A

Fuente: Elaboración propia.

7.11. Soluciones Propuestas

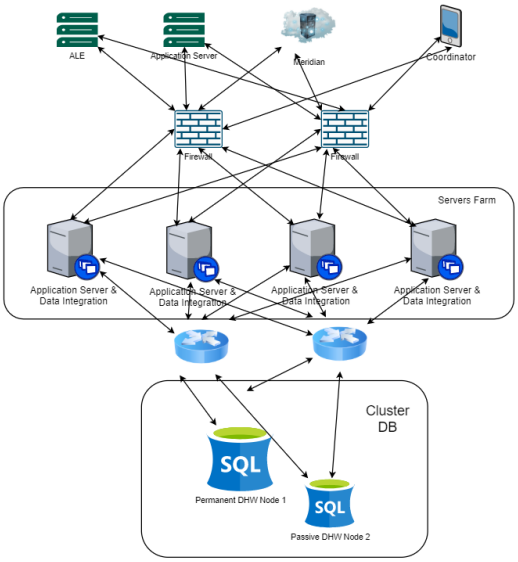
7.11.1. Solución de Sistema de Información Central en HA

Se requiere que los servidores tengan al menos, fuente redundante de poder, las fuentes deben pertenecer a circuitos eléctricos diferentes, cada equipo tener al menos una NIC (Network Interface Controller, por siglas en Ingles) redundante, las NIC deben estar conectadas a diferentes Switches y Firewalls. Se propone implementar el uso de DAM o DSMS (Data Base Secure Manager). Además, incorporar un AntiMalware entre la IOT INPUT LAYER y la IOT ELT LAYER.

Un Switch es un hardware de red que conecta dispositivos en una red de computadoras mediante el uso de conmutación de paquetes para recibir y enviar datos al dispositivo de destino y un Firewall es un es un sistema de seguridad de la red que monitoriza y controla el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas. El AntiMalware es un tipo de programa de software diseñado para prevenir, detectar y eliminar el software malicioso (malware) en los sistemas informáticos, así como en los dispositivos informáticos individuales.

7.11.2. Diagrama de la solución para R1, R11, R15 y R16

Tabla 36. Soluciones para R1, R11, R15 y R16

Propuesta	Componentes	Riesgos que mitiga
	DB, Firewall y Switches	R1, R11, R15 y R16

Fuente: Elaboración propia

Como primera medida, lo que se debe garantizar es la DISPONIBILIDAD de los servicios. Por esta razón se considera importante establecer una arquitectura de alta disponibilidad (HA – High Availability, por sus siglas en Ingles) en la infraestructura que soporta la aplicación de gestión de cirugías. De esta manera se propone implementar dos servidores de Bases de Datos (SQL) en HA (Tabla 36), de manera que la base de datos se encuentre debidamente sincronizada de tal manera que en caso de falla de uno de los servidores que componen el clúster, será el otro servidor quien tomara todas las operaciones de transacción, mientras se recupera el servidor que falló.

Así mismo, para la aplicación, la cual es la porción de software que maneja la inteligencia del proceso de negocio, se propone implementar una granja de servidores. La diferencia con la solución en HA es que permite crecer en la medida que los usuarios requieran acceso a la aplicación, por lo cual permite agregar más servidores a la granja de acuerdo con las necesidades de la organización. De esta forma, cuando un usuario

se conecte a la granja, existirá un servidor principal que indicará al usuario en que servidor de la granja se alojara la sesión solicitada, manteniendo el balanceo de cargas entre los servidores que componen dicha granja.

Al tener una granja de servidores nos permite sincronizar productos y componentes de las plataformas y valores de configuración en varios servidores con equilibrio de carga. En escenarios en los que se necesita más de un servidor, como entornos de ensayo y producción, esto puede simplificar enormemente las pruebas y los procesos de configuración.

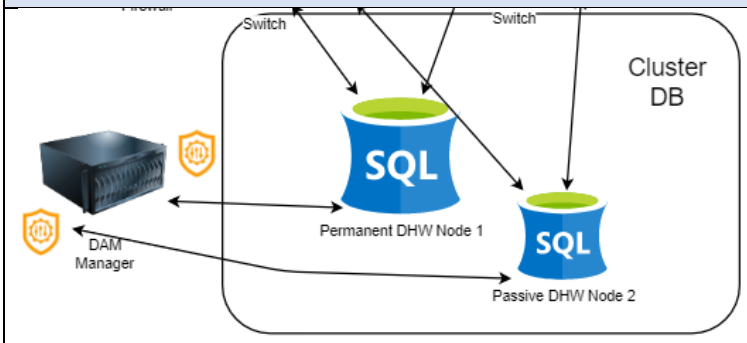
Es de anotar que esta infraestructura puede ser empleada por otras aplicaciones críticas de la organización, reduciendo sustancialmente el TCO (Total Cost on Ownership, por sus siglas en ingles) y manejando un mejor ROI (Return Of Investment, por sus siglas en Ingles) de las mismas

Ahora bien, también es necesario mantener la SEGURIDAD en el acceso a la información. Por esta razón se propone la implementación de un cluster de Firewalls que permitan filtrar los accesos desde los diferentes dispositivos hacia la infraestructura de servidores que contiene las aplicaciones críticas de la organización. Es importante entender que esto permitirá el acceso exclusivamente aquellos dispositivos que realmente requieren acceder a la información de la aplicación evitando que dispositivos no autorizados puedan acceder a la información y poner en riesgo la integridad y confidencialidad de la información, exponiendo a la organización a demandas y multas por incumplimiento a estas condiciones amparadas por la ley.

La idea de que sea en HA, al igual que los Switches de red, esta soportada bajo la necesidad de mantener la disponibilidad de los servicios y esta arquitectura apoya la disponibilidad integral que debe tener la aplicación en general.

7.11.3. Diagrama de la solución para R5

Tabla 37. Soluciones para R5

Propuesta	Componentes	Riesgos que mitiga
	DAM o DSMS Manager	R5

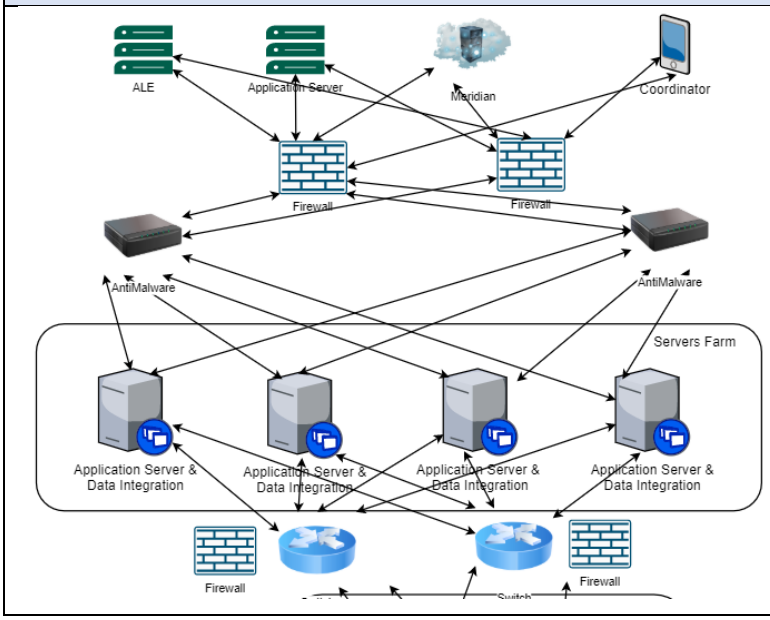
Fuente: Elaboración propia

Además de garantizar el acceso hacia las bases de datos, es importante proteger el acceso de las actividades que se realizan sobre las mismas (Tabla 37). A pesar de que, desde la conexión de los dispositivos, se trata de garantizar la seguridad de la conexión, existen diferentes tipos de ataques, como ARP spoofing que permiten realizar a suplantación de dispositivos en la red que pueden poner en riesgo la data de las bases de datos, por cuanto autorizan la conexión de dispositivos no autorizados que pueden modificar datos en las BD. De esta forma la solución de Database Activity Monitoring (DAM) , permite monitorear y proteger de forma permanente las actividades que se realizan sobre las bases de datos, incluyendo consultas, modificaciones y eliminaciones de los registros contenidas en estas por agentes externos o no autorizados, poniendo en riesgo la disponibilidad, confidencialidad e integridad de los datos.

El DAM ofrece protección en tiempo real para las bases de datos críticas para el negocio contra todo tipo de amenazas: externas, internas, e incluso contra exploits de intra-bases de datos. Esta solución basada en software proporciona una seguridad robusta y un cumplimiento continuo sin necesidad de cambios de arquitectura, hardware costoso o tiempo de inactividad.

7.11.4. Diagrama de la solución para R9

Tabla 38. Soluciones para R9

Propuesta	Componentes	Riesgos que mitiga
	Antimalware	R9

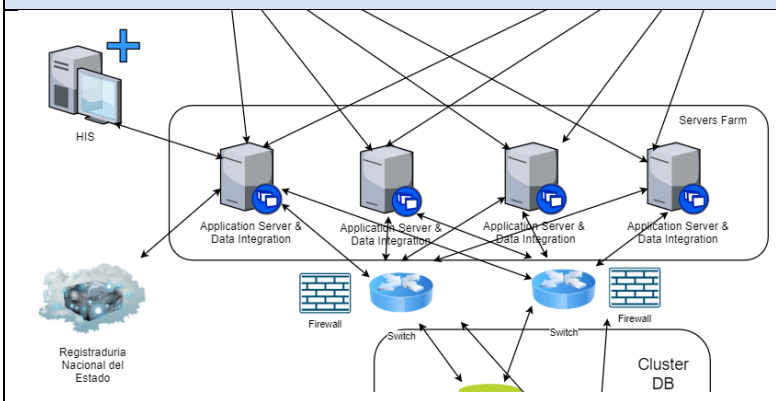
Fuente: Elaboración propia

Uno de los inconvenientes más frecuentes en los dispositivos IoT es la incapacidad que éstos presentan para poder instalar software de seguridad como lo es una solución de protección contra amenazas. Esto, debido a que cuentan con componentes de hardware que únicamente permiten la actualización de firmware de sistema operativo, el cual normalmente no incluye actualizaciones o inclusión de características de protección al dispositivo para protección contra amenazas.

Para solventar este inconveniente y evitar que los dispositivos puedan ser abusados por malware, botnets, virus, gusanos o cualquier otro tipo de amenazas, se hace necesaria la implementación de un antimalware externo (Tabla 38) que permita proteger todas las actividades ejecutadas por estos dispositivos, manteniendo el nivel de seguridad requerido dentro de la organización.

7.11.5. Diagrama de la solución para R2

Tabla 39. Soluciones para R2

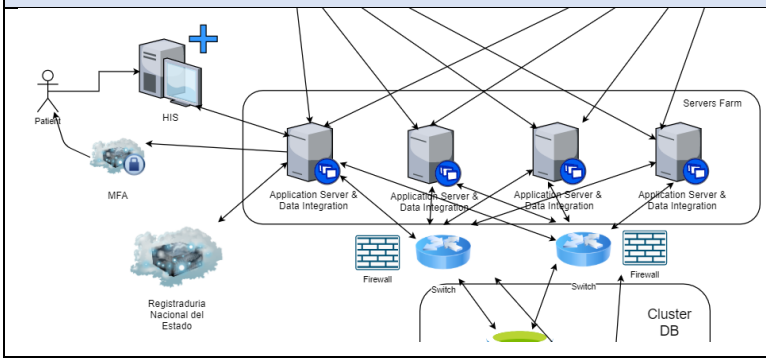
Propuesta	Componentes	Riesgos que mitiga
	Conexión a la Registraduría Nacional del Estado	R2

Fuente: Elaboración propia.

Apoyándose en servicios de cruces de información y consulta de su base de datos biométrica (Tabla 39), que ofrece la registraduría nacional del estado civil de Colombia a entes públicos y empresas del sector privado, se pretende evitar fraudes por suplantación. En este sentido, el servicio permite acceder a la información biométrica del código bidimensional, la validación de la firma digital del documento de identidad y el acceso a consulta de la información del servicio web del registro civil, con lo que podemos verificar la identidad del paciente.

7.11.6. Diagrama de la solución para R2 y R5

Tabla 40. Soluciones para R2 y R5

Propuesta	Componentes	Riesgos que mitiga
	MFA	R2 y R5

Fuente: Elaboración propia

Un certificado digital en formato token físico corresponde a un documento digital contenido en un dispositivo, que se otorga a una persona natural, el cual contiene información de identificación de dicha persona y un par de llaves criptográficas, las cuales permiten la generación de la firma.

Las firmas digitales, generadas mediante el uso de certificados digitales emitidos por algún ente autorizado, cuentan con el mismo valor probatorio y fuerza obligatoria de una firma manuscrita, que aporta atributos de seguridad jurídica, como la integridad de la información, autenticidad de la identidad del firmante y el No Repudio de la transacción.

Se propone implementar la firma digital (Tabla 40) de los funcionarios que ingresan información a la base de datos de las historias clínicas de los pacientes. Además, implementar autenticación de doble factor a los funcionarios que ingresan información a la base de datos de las historias clínicas de los pacientes, con el fin que cada actividad en los registros (adición, modificación y eliminación) de los pacientes, se pueda identificar quien realizó el ajuste bajo la premisa de No Repudio. Esto se puede realizar

mediante el uso de firmas digitales, localizadas en tokens físicos o de software de obligatorio uso para funcionarios que acceden a información de los pacientes.

7.11.7. Descripción de la solución para R6

En cuanto a R6, la intención de estas acciones es mantener una base de datos activa, viva, con información al punto y que ésta sea el centro de coordinación de las modificaciones y el punto de unión del proceso de mejora continua del servicio (con respecto a cambios). Toda esta información, tanto de entrada como de salida, y la evaluación de resultados debe quedar reflejada en la base de datos, adquiriendo está cada vez más valor, de cara a que esta CMDB permita la gestión del conocimiento con respecto a cambios de la entidad; es decir, que sea el referente, el modelo de comparación, el lugar de búsqueda, el lugar donde se contraste y donde se estime si cualquier cambio que vaya a producirse se ha realizado con anterioridad y qué resultados puede ofrecer (Ríos, 2014).

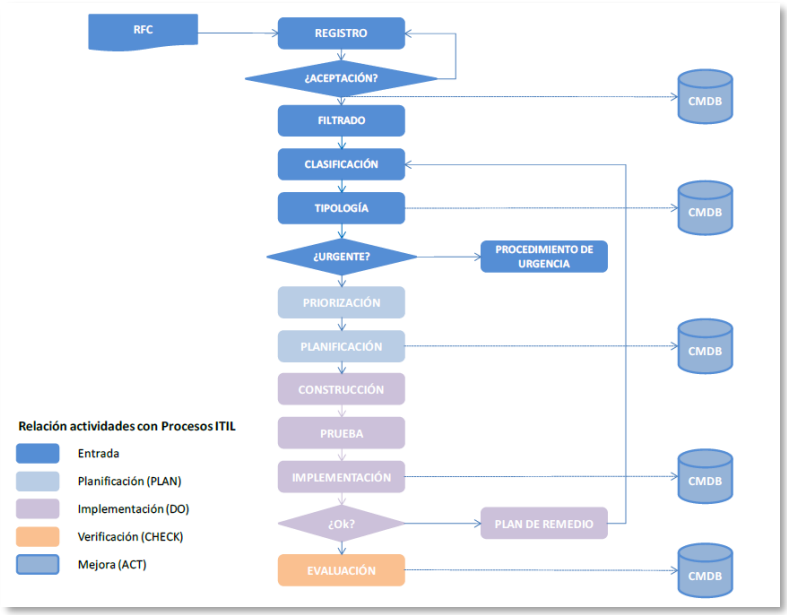


Figura 36. Proceso de gestión del cambio.

Fuente: Tomado de (Ríos, 2014)

Para evaluar las vulnerabilidades de los equipos de la solución se propone realizar un análisis de vulnerabilidades y unas pruebas de penetración. La gestión de vulnerabilidades consistirá en identificar, remediar y verificar que las diferentes vulnerabilidades de los sistemas de información se hayan mitigado. Se pueden realizar escaneos constantes por medio de un appliance (elemento de red, por sus siglas en inglés) a todos los dispositivos, aplicaciones, servicios, estaciones y servidores de la red de la organización. Las pruebas no destructivas deberán apoyarse en estándares como OWASP, OSSTMM, LPT y PCI-DSS.

7.11.8. Descripción de la solución para R9

En R9, ITIL recomienda que la entidad o institución realice y disponga de una CMDB (Change Management Data Base) o base de datos para la gestión del cambio, donde se recojan los datos provenientes de las RFC (Request for Change - peticiones de cambio), de la que se obtendrán para su posterior análisis, evaluación y se planifique un posible cambio (Ríos, 2014).

7.11.9. Descripción de la solución para R10, R13, R14, R15, R16 y R17

Para R10, R13, R14, R15, R16 y R17 propones un manejo de checklist manuales. Las listas de control, listas de chequeo, checklist u hojas de verificación, son formatos generados para realizar actividades repetitivas, controlar el cumplimiento de un listado de requisitos o recolectar datos ordenadamente y de manera sistemática. Se utilizan para hacer comprobaciones sistemáticas de actividades o productos asegurándose de que el funcionario no se olvida de nada importante.

Con las listas buscamos si se han seguido los procedimientos, si el servicio ofrecido cumple con las especificaciones, se han completado todos los registros de los pacientes, si se ha presentado una anomalía o incidencia, los equipos están en correcto estado de mantenimiento, calibrados / verificados, etc.

7.11.10. Consideramos para R10, R13, R14, R15, R16, R17 las 2 siguientes estrategias:

En el corto plazo es posible gestionar la demanda para evitar que ocurran incidencias. En este sentido es necesario disponer de un equipo bien integrado que conozca perfectamente cuáles son las prioridades de la entidad en cuestiones estratégicas, de acuerdo con evitar que las incidencias ocurran sobre procesos críticos que mermen su capacidad de reacción. Las incidencias más comunes pueden venir por fallos en la integridad del servicio por aumentos no previstos de la demanda, o bien por interrupciones del servicio por errores (o actualizaciones, o modificaciones, etc.) de hardware o software.

En el medio/largo plazo la Gestión de la Demanda ha de ser capaz de mantener un perfecto equilibrio para optimizar las TI de manera que las inversiones se realicen racionalmente. En ocasiones en las que parece necesitarse realizar un aumento de la capacidad, quizá sea posible una redistribución de la carga de trabajo de la infraestructura, de acuerdo con el mantenimiento de la calidad del servicio ofrecido. En estos casos es esencial estar realizando una gestión de la demanda, ya que si se está realizando correctamente, la monitorización de la infraestructura se estará llevando a cabo, permitiendo rentabilizar adecuadamente su servicio evitando una inversión innecesaria (Ríos, 2014).

Con respecto a R3, proponemos que se implementen checklist de los equipos que están en inventario y almacenamiento (preferiblemente al menos un dispositivo de la misma referencia, dependiendo de la criticidad) con previas pruebas de funcionamiento y ciclos de rotación con equipos en producción y revisión cada 3 y/o 6 meses. Todo esto para mantener el nivel de servicio y evitar indisponibilidad hacia los pacientes. Incluyendo los respectivos procesos de actualización de firmware y/o software del dispositivo.

7.11.11. Descripción de la solución para R8

Política de activación del radio Wi-Fi de los dispositivos de los médicos y anestesiólogos, que nos permita mitigar el R8, que este claramente definida, socializada y documentada.

Los aspectos para tener en cuente en el establecimiento de la política consideramos:

- La política debe ser comunicada en términos cumplibles.
- Debe tener reglas de juego claras para médicos y anestesiólogos.
- La directriz debe ser clara en que se espera que haga el personal médico.
- Al ser documentada debe ser clasificada como especifica.

8. Conclusiones, limitaciones, futuras investigaciones y contribuciones

8.1. Conclusiones

Los programas malignos y las respectivas vulnerabilidades que pueden explotar, ya sea a niveles de hardware o software, siguen siendo una debilidad en la implementación y gestión de sistemas modernos, en cualquier sector económico. Dado que la continua evolución y generación de malware como la intención de los atacantes no pueden eliminarse, es deber de la gerencia o tomador de decisiones en materia de tecnología invertir en avances relacionados con entornos de IT seguros para minimizar las amenazas y tomar medidas correctivas con respecto a potenciales ataques de software malicioso.

Existen en la literatura encontrada dos principales fuentes de información: la comercial suministrada principalmente por compañías de ciberseguridad que realizan investigaciones con el fin de informar y generar necesidades referentes a las amenazas en la web en los lectores e interesados y, por otra parte, la académica, en el que se pretende desde la investigación entender y modelar los comportamientos de los malware dañinos para poder realizar distintas acciones de propuestas de mitigación. Este trabajo involucró la consulta de ambas fuentes con el fin de poder generar un insumo de conocimiento consolidado acerca del impacto de los malware en los nuevos ecosistemas de IoT, hecho que se ve registrado durante la documentación del estado del arte y el marco teórico.

La consulta a expertos fue una decisión clave en la caracterización de los malware estudiados, los resultados de la Metodología Delphi permitieron eliminar el concepto de asociar la complejidad de los malware, en particular de los enfocados a dispositivos IoT, con su nivel de propagación. Ejemplos como Stuxnet demostraron que las consecuencias en caso de un ataque a un solo dispositivo como las turbinas de una planta nuclear pueden ser a escala mundiales y generar implicaciones para generaciones

posteriores. Siendo dicho ataque, aunque de proporciones muy elevadas, de carácter muy particular.

La caracterización de los tipos de malware permitió entender de manera técnica los modelos de propagación, para los gerentes de tecnología y tomadores de decisiones comprender el funcionamiento de una amenaza es importante para saber cómo afecta su sector de negocio, identificar sus activos de riesgo y poder tomar decisiones de mitigación de manera efectiva. Adicionalmente, este documento presenta una identificar vulnerabilidades de alto riesgo presentes en dispositivos IoT para industria, salud y hogares inteligentes con el propósito que fabricantes y usuarios pueden probar y quizás someter a pruebas si sus sectores tienen debilidades frente a las vulnerabilidades más comunes que se explotan en los ataques cibernéticos.

En este trabajo se introduce un modelo matemático SEIR para simular la propagación del Mirai Botnet a través de una red informática. También, el modelo SEIR se redujo a un modelo SIR para simular en forma bien precisa el ataque del Sartori Botnet (2018). En este modelo, se consideran varios parámetros relacionados con el ciclo de vida del malware, con las contramedidas implementadas en los dispositivos y con el comportamiento de los usuarios. Los resultados obtenidos parecen estar de acuerdo con el comportamiento razonable. Las simulaciones numéricas obtenidas de este modelo corroboran que las estrategias de mitigación de riesgos y control de seguridad eficientes conducen a tasas más bajas de dispositivos infectados.

La capacidad de monitorear una red e identificar dispositivos no autorizados requiere la capacidad de identificar cada dispositivo en la red como lo que trata de hacer Akamai y evaluar los cambios en tiempo real. Esto puede ser más factible incluyendo métodos estandarizados para generar identificadores a la hora de fabricar el dispositivo (y algo más fuerte que el MAC Address, por sus siglas en ingles).

Las fallas de software son comunes y casi inevitables, haciendo posible actualizar el software y el firmware necesario. Verificación de los procesos de actualización propios

de la seguridad cibernética puede requerir un análisis más profundo que la verificación y actualización de la configurabilidad. Hay que tratar de proporcionar un mecanismo de actualización más automático y periódico.

Las organizaciones deben concentrarse en construir respuestas como un todo a lo largo de su estructura que integre sus capacidades cibernéticas con sus procesos internos para lograr una interacción segura y exitosa.

Los informes usados de referencia como los resultados obtenidos denotan que la incursión de un malware y su explotación de una brecha de seguridad demuestran que a corto plazo afectan el servicio, a mediano plazo los costos y al final la reputación de una organización.

Herramientas como la simulación de amplio uso en la gerencia de ingeniería se convierten en un elemento muy importante para evaluar otras condiciones de riesgo en soluciones industriales con adopción continua de nuevas tecnologías. Gracias a sistemas como Vensim o SIMIO es posible recrear nuevos escenarios donde las condiciones no sean de eficiencia humana u operativa si no de potenciales riesgos inherentes a la solución.

No obstante, aunque los desarrollos tecnológicos traen grandes avances en términos de medidas de seguridad e implementación de estándares de control, como lo hemos identificado, estos ciclos necesitan de mucha atención de las áreas que participan en la implementación y operación de la infraestructura tanto en empresas como en entidades que prestan servicios de carácter terciario como las de salud.

Cabe mencionar que el potencial impacto en costo humano, económico y de reputación debe ser evaluado con mucho rigor de acuerdo con los hallazgos en los modelos de propagación de Botnet como Sartori.

Nos atrevemos a sugerir que dentro las diferentes prácticas y metodologías para la evaluación e implementación de proyectos de ingeniería con nuevos elementos tecnológicos como los IoT se considere los análisis rigurosos de riesgos de seguridad de estos dispositivos cohabitando con otros elementos tradicionales presentes.

Finalmente, la definición de los niveles de riesgo fue la herramienta para contextualizar las amenazas y vulnerabilidades con su respectiva probabilidad e impacto. El análisis de los riesgos de seguridad de IoT contribuye a una mejor comprensión de la necesidad de un enfoque de estandarización más alineado. Es importante que entidades, organizaciones y personas busquen una coordinación más amplia entre los comités de ingeniería con el fin de contrarrestar el vacío de estándares formales de seguridad existente en los dispositivos y articular que sus actividades cubran todos los aspectos de la seguridad del ecosistema del IoT.

8.2. Limitaciones de la investigación

Existen diferentes tipos malware circulantes en la red, de diferentes tipologías, fuentes y objetivos de ataque. Dado el alcance del documento y con el propósito de profundizar en la aplicación de las herramientas y metodologías, la principal limitación provino en el tamaño de la muestra seleccionada de tipologías de malware y su respectiva subclasificación. Si bien en la red existen muchos más tipos de malware que los aquí caracterizados, el documento se encargó de desarrollar los seleccionados por el panel de expertos debido a su criticidad.

Uno de los factores mas complejos en la dinámica para la evaluación de riesgos informáticos es la documentación existente y de fuentes confiables. Las posibilidades de correlacionar eventos pasados en tecnologías actuales o pasadas con eventos futuros y con tecnologías futuras no son medianamente posibles, la extrapolación de eventos con determinadas tecnológicas nos sirve de marco de referencia para la creación de nuevos escenarios en donde el riesgo informático puede tener desarrollo e

implicaciones inciertas. La simulación es una herramienta fundamental para ayudar a entender al malware y las implicaciones correspondientes.

Simulación de dinámica de sistemas es uno de los enfoques para la evaluación y estudio de los esquemas de la seguridad de los sistemas de información. El modelaje del Sartori Botnet fue único y nos dio la tasa de propagación. En estos experimentos se emplearon métodos de Investigación de Operaciones y se pudo obtener mapeos confiables. Lo interesante fue extrapolar esa tasa de propagación a un sistema de simulación de eventos discretos y así ver un ataque similar y el impacto en los procesos de negocio de un hospital. Este análisis fue importante ya que ayuda a determinar la viabilidad de los ataques y su impacto en la información y también la prevención requerida por parte de la organización.

El trabajo actual fue un intento enfocado a identificar un malware, sus implicaciones e impactos desde una perspectiva gerencial. Esto deja un espacio para profundizar los análisis tanto cualitativos como cuantitativos desde una perspectiva técnica con mayores métodos y simulaciones. Debido a la naturaleza exploratoria de este documento, los hallazgos deben interpretarse de manera mesurada y son necesarios estudios adicionales. En particular, se recomienda realizar estudios con un tamaño de tipologías mayor. Finalmente, es probable que la clasificación de malware en este documento esté sujeta a cambios dependiendo de la evolución de estas.

8.3. Futuras investigaciones

Los dispositivos IoT están surgiendo cada vez más en entornos comerciales y personales. A menudo pasan desapercibidos, simplemente aparecen dentro de las infraestructuras de red, utilizando conexiones por cable o inalámbricas y expandiendo la potencial superficie de ataque de la empresa. Las investigaciones orientadas en ciberseguridad, en especial, enfocado a los IoT deben ser una prioridad urgente debido a que este sector cuenta con una de las oportunidades más atractivas de la industria y

desaprovecharla debido a desafíos de seguridad sería un gran error, especialmente porque esos desafíos son superables.

Desde la perspectiva propia de este documento se recomienda en futuras investigaciones ampliar el alcance de tipología de malware a estudiar, si bien este trabajo involucro los gusanos y los botnet como tipología de estudio, es recomendable incluir tipologías adicionales para analizar los comportamientos particulares en cada sector de estudio.

Por otra parte, uno de los aspectos que se recomienda profundizar en futuras investigaciones es la implementación de nuevas herramientas de mitigación de riesgos cibernéticos como los honeypots o los sandbox, estos sistemas tienen como objetivo detectar y obtener información de los ataques informáticos, y, sobre todo, su procedencia, con el fin de tomar las medidas de seguridad necesarias en la organización.

Un desarrollo muy importante para el futuro es la de incluir la de Ciberseguridad Conductual. Los atacantes a la empresa siempre intentarán penetrar todos los niveles de defensa. Por lo tanto, la empresa debería analizar la seguridad utilizando herramientas para descubrir vulnerabilidades. Las empresas deben tener en cuenta la posibilidad de vulnerabilidades, incluido el error humano, en el diseño de los sistemas. Esta es una de las lecciones aprendidas de este estudio y para así hacer del modelado y la simulación un componente esencial. Las partes interesadas (ejemplo: usuarios, gerentes y desarrolladores) deben participar en la construcción de esos modelos y determinar simulaciones que evalúan cargas cognitivas. Las partes interesadas también pueden usar la simulación para ejercitar escenarios de la vida real de ataques de ingeniería social. La ciberseguridad conductual debe incluirse en un estudio futuro. Esta ciberseguridad abordará los perfiles y métodos de los piratas informáticos tanto como también las teorías de conducta, sociales y delictivas. La Inteligencia Artificial será un componente importante de la inclusión de la ciberseguridad conductual y, potencialmente, la utilización de la simulación basados en agentes y nuevos esquemas como Blockchain.

En la continuación de esta investigación, esperamos que otras personas puedan explorar formas de mejorar la precisión de los modelos de propagación y alinear mejor otros modelos de propagación con la evolución que se presentara de otros malware. Así mismo poder usar las bases del análisis de riesgos para poder evaluar otras soluciones de tecnológicas que tienen otras condiciones por su naturaleza como por su servicio, tanto al interior como hacia los clientes de muchas entidades.

8.4. Contribuciones a la gerencia de ingeniería

El rol de gerente de ingeniería pertenece a un campo multidisciplinario que busca abordar problemas asociados con operaciones o sistemas de ingeniería complejos. Adicionalmente, proporciona habilidades y conocimientos para liderar iniciativas y programas de gestión tecnológica e innovación y contribuir a la competitividad empresarial e industrial. Es importante decir que un gerente de ingeniería lleva conceptos de ingeniería tanto como de administración.

Las amenazas cibernéticas de infraestructura se están expandiendo a un ritmo rápido y plantean nuevos desafíos para el rol del gerente de ingeniería ya que son los responsables de garantizar la operación segura, eficiente y confiable de los sistemas, procesos y recursos a cargo de los departamentos de TI a nivel corporativo y gubernamental. Estos sistemas están sujetos a riesgos crecientes basados en vulnerabilidades tecnológicas, amenazas cibernéticas e impactos a los sistemas, los gerentes de ingeniería deben asegurarse de que están reduciendo adecuadamente su riesgo cibernético para satisfacer las necesidades de la organización.

Este trabajo tiene la intención de contribuir desde una perspectiva académica a presentar herramientas y metodologías para la categorización de malware y sus respectivos riesgos, por lo cual, un gerente de ingeniería puede intentar minimizar las amenazas internas y externas a través de detección, análisis de riesgos y modelos de mitigación, a su vez, también puede incluir el fortalecimiento de políticas,

procedimientos y controles de calidad en términos de ciber seguridad. También es un ejemplo de cómo utilizar herramientas de simulación para guiarnos en la toma de decisiones y el entendimiento de la complejidad de ciertos procesos.

Una importante contribución fue como poner juntos los que nos enseñaron en Gerencia Estratégica y una de sus herramientas que es el Delphi. También, como utilizar la simulación desde dos puntos de vistas: el de dinámica de sistemas enseñado en la clase de Análisis de Decisiones Económicas junto con el punto de vista de la simulación de eventos discretos enseñado en la clase de Métodos Estadísticos y Simulación. Todas estas herramientas, marcos conceptuales, y formas de pensar aprendidas en el curso de Gerencia de Ingeniería junto con nuestra experiencia profesional de varios años en ciberseguridad en compañías reconocidas a nivel mundial (Intel (www.intel.com), McAfee (www.mcafee.com)) y la red profesional cultivada fueron esenciales. Este proceso es una contribución que no hemos visto en la literatura actual y que va más allá de una contribución a la Gerencia de Ingeniería.

9. Bibliografía

• *Internet of Things units installed base by category 2014-2020 | Statista*. (n.d.). Retrieved August 4, 2020, from https://www.statista.com/statistics/370350/internet-of-things-installed-base-by-category/

Acarali, D., Rajarajan, M., Komninos, N., & Zarpelão, B. B. (2019). Modelling the Spread of Botnet Malware in IoT-Based Wireless Sensor Networks. *Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/3745619

Akamai. (2020). *Use routed map*. https://learn.akamai.com/en-us/webhelp/security-center/kona-security-solutions-security-center-user-guide/GUID-066058C0-5D3F-417A-98D1-04AA6472BA45.html

Alenezi, A., Atlam, H. F., Alsagri, R., Alassafi, M. O., & Wills, G. B. (2019). IoT forensics: A state-of-the-art review, challenges and future directions. *COMPLEXIS 2019 - Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk*, 106–115. https://doi.org/10.5220/0007905401060115

Angrishi, K. (2017). *Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets*. http://arxiv.org/abs/1702.03681

Armiñana Gorriz, J. (2018). *Seguridad en Internet de las Cosas Honeypot to capture IoT-attack methods*. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/82136/6/parriagaTFM0618memoria.pdf

Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Internet of Things: State-of-the-art, Challenges, Applications, and Open Issues. *International Journal of Intelligent Computing Research*, *9*(3), 928–938. https://doi.org/10.20533/ijicr.2042.4655.2018.0112

Avella, J. R. (2016). Delphi panels: Research design, procedures, advantages, and challenges. *International Journal of Doctoral Studies*, *11*, 305–321. https://doi.org/10.28945/3561

Bauer, H., Burkacky, O., & Knochenhauer, C. (2017). *Security in the Internet of Things*.

Bechtsoudis, A., & Sklavos, N. (2010). Side channel attacks cryptanalysis against block ciphers based on FPGA devices. *Proceedings - IEEE Annual Symposium on VLSI, ISVLSI 2010*, 460–461. https://doi.org/10.1109/ISVLSI.2010.104

Berggren, R. (2020). *Benchmarking and comparison of a relational and a graph database in a CMDB context*.

Brian Krebs. (2016). Who makes the IoT things under attack? In *Krebs on Security*. https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

Cha, S., Ruiz, M. P., Wachowicz, M., Tran, L. H., Cao, H., & Maduako, I. (2017). The role of an IoT platform in the design of real-time recommender systems. *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016*, 448–453. https://doi.org/10.1109/WF-IoT.2016.7845469

Chang, Z. (2019). *Inside the Smart Home: IoT Device Threats and Attack Scenarios - Security News - Trend Micro USA*. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios

Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer*, *44*(4), 91–93. https://doi.org/10.1109/MC.2011.115

Chib, S., & Greenberg, E. (1996). Markov Chain Monte Carlo Simulation Methods in Econometrics. *Econometric Theory*, *12*(3), 409–431. https://doi.org/10.1017/s0266466600006794

Cloudflare. (2019). What is the Mirai Botnet? *Cloudflare*, 1–4. https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

Coss, R. (2005). *Simulacion un enfoque practico*. 158.

Costa, L., Barros, J. P., & Tavares, M. (2019). Vulnerabilities in IoT devices for smart home environment. *ICISSP 2019 - Proceedings of the 5th International Conference on Information Systems Security and Privacy*, 615–622. https://doi.org/10.5220/0007583306150622

De Donno, M., Dragoni, N., Giaretta, A., & Spognardi, A. (2018). DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/7178164

Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT: A survey. *Proceedings of*

the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017, 32–37. https://doi.org/10.1109/I-SMAC.2017.8058363

ENISA. (2017). *Baseline Security Recommendations for IoT*. *November*, 1–103. https://doi.org/10.2824/03228

Estrada, D., Tawalbeh, L., & Vinaja, R. (2020). How Secure Having IoT Devices in Our Homes? *Journal of Information Security*, *11*(02), 81–91. https://doi.org/10.4236/jis.2020.112005

Eustis, A. G. (2019). *The Mirai Botnet and the Importance of IoT Device Security*. 85–89. https://doi.org/10.1007/978-3-030-14070-0_13

Fagade, T., Spyridopoulos, T., Albishry, N., & Tryfonas, T. (2017). System dynamics approach to malicious insider cyber-threat modelling and analysis. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10292 LNCS*, 309–321. https://doi.org/10.1007/978-3-319-58460-7_21

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32.Stuxnet Dossier. *Symantec-Security Response*, *Version 1.*(February 2011), 1–69. https://doi.org/20 September 2015

Feily, M., Shahrestani, A., & Ramadass, S. (2009). A survey of botnet and botnet detection. *Proceedings - 2009 3rd International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2009*, 268–273. https://doi.org/10.1109/SECURWARE.2009.48

Ficco, M. (2019). Detecting IoT malware by markov chain behavioral models. *Proceedings - 2019 IEEE International Conference on Cloud Engineering, IC2E 2019*, 229–234. https://doi.org/10.1109/IC2E.2019.00037

FortiGuard SE Team. (2017). Reaper: The Next Evolution of IoT Botnets. *Fortinet*. https://www.fortinet.com/blog/threat-research/reaper-the-next-evolution-of-iot-botnets.html

Frank, C., Nance, C., Jarocki, S., Pauli, W. E., & Madison, S. D. (2017). Protecting IoT from Mirai botnets; IoT device hardening. *Proceedings of the Conference on Information Systems Applied Research ISSN*, *2167*, 1508. http://iscap.info

Fuster, A., del Rey, M., & Rodriguez, G. (2014). Simulación de la propagación del

malware : Modelos continuos vs . modelos discretos. *Resci 2014*, 2–5.

Gardner, M. T., Beard, C., & Medhi, D. (2017). Using SEIRS epidemic models for IoT botnets attacks. *DRCN 2017 - 13th International Conference on Design of Reliable Communication Networks*.

Gemalto. (2019). Gemalto: State of IoT Security. *Network Security*, *2019*(2), 4. https://doi.org/10.1016/s1353-4858(19)30018-2

Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection*, *10*, 3–17. https://doi.org/10.1016/j.ijcip.2015.04.001

Healthcare Modeling and Decision Making During Pandemics: A Case Study. (n.d.). Retrieved October 12, 2020, from https://www.simio.com/blog/2020/04/10/healthcare-modeling-and-decision-making-during-pandemics-a-case-study/

Homeland Security. (2003). Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. *National Security Presidential Directives*, *104*(1), 1822–1826. https://www.dhs.gov/sites/default/files/publications/Homeland

Hosseini, S., Abdollahi Azgomi, M., & Rahmani Torkaman, A. (2016). Agent-based simulation of the dynamics of malware propagation in scale-free networks. *Simulation*, *92*(7), 709–722. https://doi.org/10.1177/0037549716656060

Hsu, A. P. T., Lee, W. T., Trappey, A. J. C., Trappey, C. V, & Chang, A. C. (2016). Using System Dynamics Analysis for Performance Evaluation of IoT Enabled One-Stop Logistic Services. *Proceedings - 2015 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2015*, 1291–1296. https://doi.org/10.1109/SMC.2015.230

Hu, S., Hu, B., & Cao, Y. (2018). The wider, the better? The interaction between the IoT diffusion and online retailers' decisions. *Physica A: Statistical Mechanics and Its Applications*, *509*, 196–209. https://doi.org/10.1016/j.physa.2018.06.008

Huang, C. Y., & Chen, H. N. (2010). Global digital divide: A dynamic analysis based on the Bass model. *Journal of Public Policy and Marketing*, *29*(2), 248–264. https://doi.org/10.1509/jppm.29.2.248

Hughes, D. (2016). Silent risk: new incarnations of longstanding threats. *Network Security*, *2016*(8), 17–20. https://doi.org/10.1016/S1353-4858(16)30079-4

Hugo Hernando, A. S., Emiliano de Jesús, L. M., Hernandez Cuadrado, A. E., & Monsalve Quintero, A. J. (2010). Evolución: Herramienta software para modelado y simulación con Dinámica de Sistemas. *Dinámica de Sistemas*, *5*(1), 1–27.

Humphrey, D. (2018). *HARTING Deploys Edge Computing in Its Own Production*.

Hung, M. (2017). Leading the IoT. In *Journal of Telecommunication, Electronic and Computer Engineering* (Vol. 7, Issue 1). https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

IBM. (2019). Cost of a Data Breach Report. *IBM Security*. https://www.ibm.com/security/data-breach

Idika, N., & A.P.Mathur. (2007). A survey of {M}alware {D}etection {T}echniques, Purdue University. *Profsandhu.Com*. http://profsandhu.com/cs5323_s17/im_2007.pdf

IEEE. (2013). IEEE Spectrum - March 2013. *IEEE Spectrum*, *43*(3), 1. https://doi.org/10.1109/mspec.2006.1604826

Imperva. (2020). *Honeypot*.

Institute for Disease Modeling. (2020). *SEIR and SEIRS models*. http://idmod.org/docs/tuberculosis/model-seir.html

IoT-Analytics. (2019). The Top 10 IoT Segments in 2018 – based on 1,600 real IoT projects. *IoT-Analytics*. https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/

Ipropertymanagement.com. (2020). *Smart Home Statistics [2020]: Growth of Connected Devices*. https://ipropertymanagement.com/research/iot-statistics

ITU. (2012). Overview of the Internet of things. *Series Y: Global Information Infrastructure, Internet Protocol Aspects and next-Generation Networks - Frameworks and Functional Architecture Models*, 22.

Izquierdo, L. R., Galán Ordax, J. M., Santos, J. I., & Del Olmo Martínez, R. (2008). Modelado de sistemas complejos mediante simulación basada en agentes y mediante dinámica de sistemas. *Empiria. Revista de Metodología de Ciencias Sociales*, *0*(16), 85. https://doi.org/10.5944/empiria.16.2008.1391

Jankowski, S. (2014). The Sectors Where the Internet of Things Really Matters. *Harvard Business Review - Internet*.

Jerkins, J. A. (2017). Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code. *2017 IEEE 7th Annual Computing and Communication Workshop and Conference, CCWC 2017*. https://doi.org/10.1109/CCWC.2017.7868464

Kaspersky Lab. (2016). *Daños Causados por el Malware*. https://encyclopedia.kaspersky.es/knowledge/damage-caused-by-malware/

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. *Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012*, 257–260. https://doi.org/10.1109/FIT.2012.53

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80–84. https://doi.org/10.1109/MC.2017.201

Lan, L. (2012). Study on security architecture in the internet of things. *Proceedings of 2012 International Conference on Measurement, Information and Control, MIC 2012*, *1*, 374–377. https://doi.org/10.1109/MIC.2012.6273274

Limaye, A., & Adegbija, T. (2017). A Workload Characterization for the Internet of Medical Things (IoMT). *Proceedings of IEEE Computer Society Annual Symposium on VLSI, ISVLSI*, *2017-July*, 302–307. https://doi.org/10.1109/ISVLSI.2017.60

Loras R, E. (2000). What is a Honeypot? *Sans*. https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2016). Internet of things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, 336–341. https://doi.org/10.1109/ICITST.2015.7412116

Maidstone, R. (2012). Discrete Event Simulation, System Dynamics and Agent Based

Simulation: Discussion and Comparison. *System*, 1–6.

Makalesi, A., Atac, C., & Akleylek, S. (2019). A Survey on Security Threats and Solutions in the Age of IoT. *European Journal of Science and Technology*, *15*(15), 36–42. https://doi.org/10.31590/ejosat.494066

Martinov, G. M., Pushkov, R. L., & Evstafieva, S. V. (2020). Collecting diagnostic operational data from CNC machines during operation process. *IOP Conference Series: Materials Science and Engineering*, *709*(3). https://doi.org/10.1088/1757-899X/709/3/033051

Masood, R., Ghazia, U. E., & Anwar, Z. (2011). SWAM: Stuxnet worm analysis in Metasploit. *Proceedings - 2011 9th International Conference on Frontiers of Information Technology, FIT 2011*, 142–147. https://doi.org/10.1109/FIT.2011.34

McAfee. (n.d.). *SOLUTION BRIEF 1 Respond Faster to Security Threats with ServiceNow and McAfee Respond Faster to Security Threats with ServiceNow and McAfee*.

McDermott, C. D., Petrovski, A. V, & Majdani, F. (2018). Towards situational awareness of botnet activity in the internet of things. *2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2018*. https://doi.org/10.1109/CyberSA.2018.8551408

Milosevic, J., Regazzoni, F., & Malek, M. (2017). Malware threats and solutions for trustworthy mobile systems design. *Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment*, 149–167. https://doi.org/10.1007/978-3-319-44318-8_8

Mishra, B. K., & Jha, N. (2010). SEIQRS model for the transmission of malicious objects in computer network. *Applied Mathematical Modelling*, *34*(3), 710–715. https://doi.org/10.1016/j.apm.2009.06.011

Molina García, J. A. (2019). *La importancia de la gestión de riesgos y seguridad en el internet de las cosas (IOT)*. http://repository.unipiloto.edu.co/handle/20.500.12277/6754

Muñoz, C. (2017). Reaper IoT, la botnet que tiene secuestrados a miles de dispositivos y mantiene en alerta a investigadores. *FayerWayer*. https://www.fayerwayer.com/2017/10/reaper-iot-la-botnet-que-tiene-

secuestrados-miles-de-dispositivos-y-mantiene-en-alerta-investigadores/

Nausheen, F., & Begum, S. H. (2018). Healthcare IoT: Benefits, vulnerabilities and solutions. *Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018*, 517–522. https://doi.org/10.1109/ICISC.2018.8399126

Nebbione, G., & Calzarossa, M. C. (2020). Security of IoT Application Layer Protocols: Challenges and Findings. *Future Internet*, *12*(3), 55. https://doi.org/10.3390/fi12030055

Newman, L. H. (2016). The botnet that broke the Internet isn't going away. *Wired*.

Newsweek. (2020). *Weathering the Perfect Storm*. https://www.newsweek.com/vantage-weathering-perfect-storm-1493513

Nurse, J. R. C., Creese, S., & De Roure, D. (2017). Security Risk Assessment in Internet of Things Systems. *IT Professional*, *19*(5), 20–26. https://doi.org/10.1109/MITP.2017.3680959

Palo Alto. (2020). 2020 Unit 42 IoT Threat Report. In *Palo Alto*. https://start.paloaltonetworks.com/unit-42-iot-threat-report

Paul, M., & Yadegari, B. (2013). The Stuxnet Worm. *Chemical Engineering Vol, New York*, *5*(Jun), 44–46. https://www2.cs.arizona.edu/%7B~%7Dcollberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf%0Ahttp://danlev.deviantart.com/journal/More-Like-This-A-New-Way-To-Explore-deviantART-331552297

Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys*, *39*(1). https://doi.org/10.1145/1216370.1216373

Perez, C. (2017). Reaper IoT botnet. *Tenable*, 1–2. https://es-la.tenable.com/blog/reaper-iot-botnet

Radware. (2017). *ERT Threat Alert Reaper Botnet*. 1–4.

Radware. (2018). *Satori IoT Botnet Variant*. https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/satori-iot-botnet/

Rambus. (2020). *Industrial IoT: Threats and Countermeasures*. https://www.rambus.com/iot/industrial-iot/

Rao, A. R., & Clarke, D. (2020). Perspectives on emerging directions in using IoT devices in blockchain applications. *Internet of Things*, *10*(xxxx), 100079. https://doi.org/10.1016/j.iot.2019.100079

Renzi, A. B., & Freitas, S. (2015). The Delphi Method for Future Scenarios Construction. *Procedia Manufacturing*, *3*, 5785–5791. https://doi.org/10.1016/j.promfg.2015.07.826

Rhebo. (2019). *Glossary | IoT Reaper Malware explained*. https://rhebo.com/en/service/glossar/iot-reaper-25113/

Ríos, S. (2014). ITIL v3 Manual íntegro. *B-Able*, 101. https://doi.org/10.1080/08820130500496811

S, S., & L, M. (2015). A Survey on Malware Propagation Analysis and Prevention Model. *International Journal of Advancements in Technology*, *06*(02). https://doi.org/10.4172/0976-4860.1000148

Sarmiento-Vásquez, A. T. (2016). *Análisis comparativo de los paradigmas de simulación*. http://repositorio.ulima.edu.pe/handle/ulima/3296

Schneier, B. (2016). Lessons From the Dyn DDoS Attack. *Schneier on Security*. https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html

SCmagazine. (2016). *DDoS attack Friday hits Twitter, Reddit, Spotify and others*.

Shanbhag, R., & Shankarmani, R. (2015). Architecture for Internet of Things to minimize human intervention. *2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2015*, 2348–2353. https://doi.org/10.1109/ICACCI.2015.7275969

Sharma, N., Shamkuwar, M., & Singh, I. (2019). The history, present and future with iot. *Intelligent Systems Reference Library*, *154*, 27–51. https://doi.org/10.1007/978-3-030-04203-5_3

Sharmeen, S., Huda, S., Abawajy, J. H., Ismail, W. N., & Hassan, M. M. (2018). Malware Threats and Detection for Industrial Mobile-IoT Networks. *IEEE Access*, *6*, 15941–15957. https://doi.org/10.1109/ACCESS.2018.2815660

Sinanovic, H., & Mrdovic, S. (2017). Analysis of Mirai malicious software. *2017 25th International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2017*. https://doi.org/10.23919/SOFTCOM.2017.8115504

Sklavos, N. (2017). *Malware in IoT Software and Hardware*. *May*, 8–11.

Souri, A., & Hosseini, R. (2018). A state-of-the-art survey of malware detection approaches using data mining techniques. *Human-Centric Computing and Information Sciences*, *8*(1). https://doi.org/10.1186/s13673-018-0125-x

Stallings, W. (2015). The Internet of Things: Network and Security Architecture. *The Internet Protocol Journal*, *18*(4), 1–32. https://doi.org/10.1525/jsah.2015.74.4.406

Suresh, P., Daniel, J. V., & V.Parthasarathy. (2014). A state of the art review on the Internet of Things (IoT). *International Conference on Science Engineering and Management Research (ICSEMR)*, 4–5.

Thorhallsdóttir, K. (2018). *Impact and probability in risk assessment* . 2–9. http://apppm.man.dtu.dk/index.php/Impact_and_Probability_in_Risk_Assessme nt

Vyas, K. K., & Shrimali, D. T. (2017). Congestion Control and Protected Broadcast of Data Using FTP and TELNET in a Cloud Network. *An International Journal of Engineering Sciences*, *6913*(63019), 112–125.

Wang, A., Liang, R., Liu, X., Zhang, Y., Chen, K., & Li, J. (2017). An inside look at IoT malware. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *202*, 176–186. https://doi.org/10.1007/978-3-319-60753-5_19

What are the Differences Between M2M and IoT? | Electronics For You. (n.d.). Retrieved August 4, 2020, from https://www.electronicsforu.com/resources/learn-electronics/difference-between-m2m-and-iot

Zawoad, S., & Hasan, R. (2015). FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*, 279–284. https://doi.org/10.1109/SCC.2015.46

Zhang, Z.-K., Cho, M. C. Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., & Shieh, S. (2014). IoT Security: Ongoing Challenges and Research Opportunities. *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, 230–234. https://doi.org/10.1109/SOCA.2014.58

Zhaosheng, Z., Zhi, J. F., Guohan, L., Phil, R., Yan, C., & Keesook, H. (2008). Botnet research survey. *Proceedings - International Computer Software and Applications Conference*, 967–972. https://doi.org/10.1109/COMPSAC.2008.205