CIBERSEGURIDAD EN HOGARES INTELIGENTES

Sergio Andres Mazo Otalvaro

Yamil Alberto Mosquera Solano

Javier Alejandro Jaimes Pimentel

Asesora de Trabajo de Grado

Silvia Elena Vanegas Pérez

INSTITUCIÓN UNIVERSITARIA DE ENVIGADO (IUE)
FACULTAD DE INGENIERÍA
INGENIERÍA EN SISTEMAS Y ELECTRÓNICA
ENVIGADO
2019

Contenido

LISTA DE FIGURAS

Pág.

1. INTRODUCCIÓN

El presente informe contiene la idea de proyecto que surge de una necesidad latente en el ámbito de la ciberseguridad en hogares, aunque este tipo de sistema de seguridad es común verlo implementado en empresas, el nicho de negocio de este proyecto radica en que hay actualmente hogares vulnerables a los ataques informáticos, sin tener presentes los grandes riesgos que esto conlleva a la seguridad de los usuarios del internet de las cosas Internet of Things (IoT).

En el documento podrá leer los antecedentes explicando la revolución en el mundo de la informática y de las telecomunicaciones, la evolución que ha tenido el internet de las cosas en el mercado por regiones y segmentos, verá consultas sobre el crecimiento de dicho mercado durante los últimos 5 años, lo cual demostrará que los hogares cuentan con al menos un dispositivo (IoT) que está transmitiendo información a la nube (red) sin algún tipo de protección, explicando esto con datos estadísticos de los ataques cibernéticos por sectores desde el año 2017.

En consecuencia encontrará la recopilación de dispositivos y las políticas de prevención, defensa y recomendaciones generales para los usuarios con la respectiva documentación, siendo este el objetivo del proyecto ciberseguridad en hogares inteligentes debido a la formación académica y experiencia laboral del equipo de trabajo lo cual permite disminuir las vulnerabilidades o los riesgos que se presentan en los dispositivos (IoT), las conclusiones y las recomendaciones para el manejo de la seguridad de la información en estos dispositivos estarán implícitas en el informe.

2. OBJETIVOS

2.1 Objetivo General

Proponer políticas de prevención y defensa con la respectiva documentación para la infraestructura del internet de las cosas (IoT) ante ciberataques en proyectos de hogares inteligentes, mediante la experiencia del grupo de trabajo en la constructora especializada en proyectos (IoT) HIGH CLASS Technology .

2.2 Objetivos Específicos

- Contrastar las estadísticas del mercado de las (IoT) sobre los riesgos derivados de la tendencia de ciberseguridad.
- Evaluar vulnerabilidades de una infraestructura IoT en un hogar inteligente seleccionando dispositivos de proyectos usados por una constructora especializada en IoT.
- Exponer las políticas que reduzcan las amenazas, fallos de seguridad, malware, virus entre otros tipos de ciberataques presentados en los IoT de un proyecto de hogar inteligente.

3. JUSTIFICACIÓN

El proyecto ciberseguridad en hogares inteligentes, se plantea al evaluar nueve tecnologías que conforman las industrias 4.0, asociando ciberseguridad e internet de las cosas (IoT), y basándose en estudios que demuestran fallas de seguridad, un ejemplo es el siguiente:

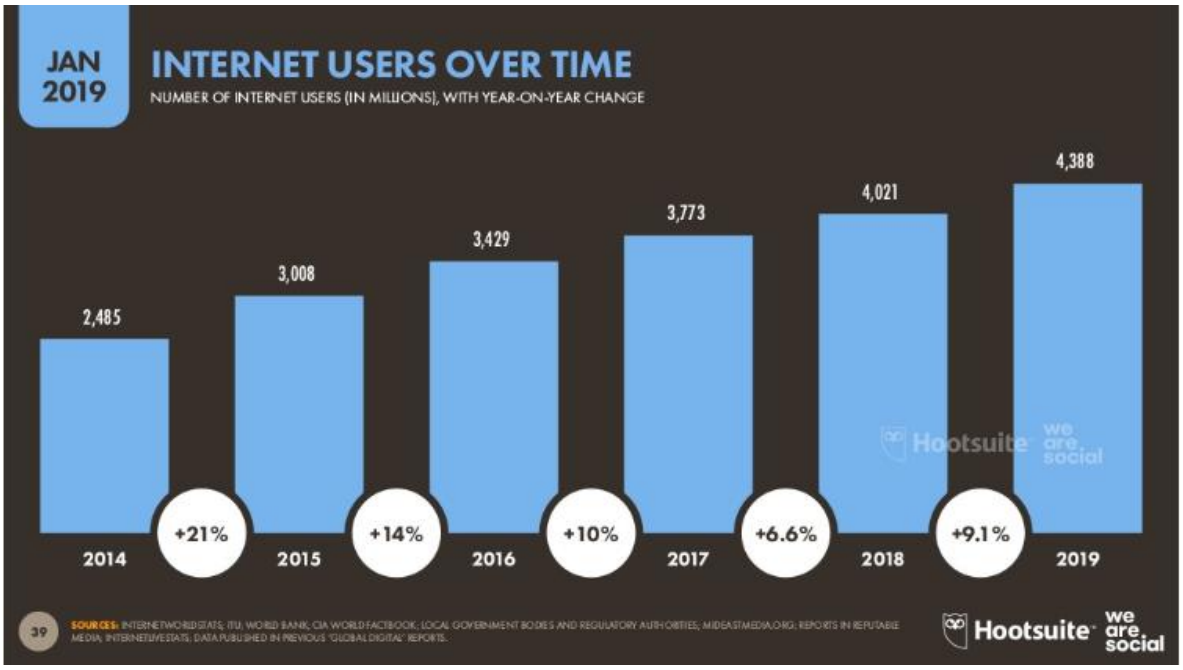
*"Según el informe de **Kaspersky Lab** sobre IoT, durante la primera mitad de 2018 los dispositivos IoT fueron atacados con más de 120.000 modificaciones de malware. Eso es más del triple de la cantidad de malware de IoT observada en durante 2017. Kaspersky Lab advierte que el crecimiento vertiginoso de las familias de malware que tienen como objetivo los dispositivos inteligentes es una continuación de una tendencia peligrosa, dado a que en 2017, el número de modificaciones de malware para dispositivos inteligentes aumentó 10 veces con respecto al monto visto en 2016"* (ebizLatam.com, 2019)

Teniendo en cuenta la formación académica y experiencia laboral del grupo de trabajo, se analiza la idea de generar políticas, técnicas y configuraciones de seguridad informática incluyendo electrónica, sobre el desarrollo, implementación e instalación de este tipo de dispositivos (IoT), disminuyendo el riesgo o las vulnerabilidades que se presentan, para lo cual se puede transformar como proyecto de negocio.

Realizando consultas sobre el crecimiento del mercado durante los últimos 5 años y observando a la fecha actual, los hogares cuentan con algún dispositivo catalogado como IoT, los cuales ponen en muestra la información a internet sin ningún tipo de protección debido al diseño de los fabricantes, porque estos dispositivos son creados para funcionar, pero no para ser seguros. Teniendo en cuenta la información presentada de las empresas enfocadas a la seguridad informática, en donde indican que tienen un mercado basado en

protección de infraestructura y networking empresarial, abre una oportunidad de negocio para el proyecto de Ciberseguridad en hogares inteligentes con (IoT).

Figura 1 Usuarios de Internet a lo largo del tiempo



[Figura](The Next Web, 2019)

4. DESARROLLO DEL CONTENIDO

4.1 Antecedentes

Internet es la revolución en el mundo de la informática y de las comunicaciones. Antes de Internet se produjo inventos como el telégrafo, teléfono, radio y el computador generando así bases para el éxito que ha tenido Internet, el cual genera ventajas frente a los diferentes sistemas de comunicaciones creados, posicionándose como un sistema de transmisión potencial y que logra la interacción de información a nivel mundial.

"Actualmente, somos parte de un mundo tecnológico que está modificando sustancialmente la forma en que vivimos, pensamos, trabajamos y nos relacionamos. El despliegue de los avances tecnológicos, la permeabilidad de la tecnología en los distintos sectores de la sociedad; y su profunda capacidad de transformar complejos escenarios de producción y gobernanza han coadyuvado a que el mundo esté bajo una constante y rápida transformación" (CEPAL, 2015).

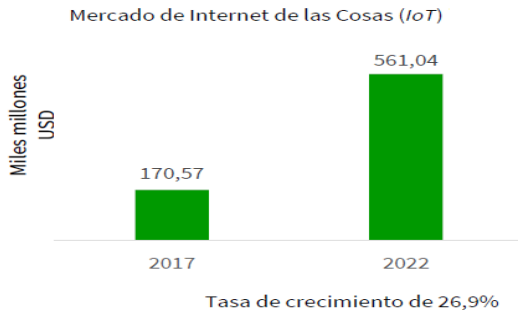
Esta transformación tan grande en el mundo de las comunicaciones por medio del internet, ha llevado a pensar ya desde este milenio como se puede hacer que el internet mejore nuestra vida, dando como origen a lo que denominan el internet de las cosas.

"*Internet de las cosas (IdC), algunas veces denominado "Internet de los objetos", lo cambiará todo, incluso a nosotros mismos. Si bien puede parecer una declaración arriesgada, hay que tener en cuenta el impacto que Internet ha tenido sobre la educación, la comunicación, las empresas, la ciencia, el gobierno y la humanidad. Claramente Internet es una de las creaciones más importantes y poderosas de toda la historia de la humanidad. Ahora debemos tener en cuenta que IdC representa la próxima evolución de Internet, que será un enorme salto en su capacidad para reunir, analizar y distribuir datos que podemos convertir en información, conocimiento y en última instancia, sabiduría."* Dave Evans (2011)

Todo esta evolución que tiene el internet de las cosas es debido a los sensores electrónicos que obtienen todo tipo de información del ambiente, desde la temperatura, la humedad, iluminación y la envían a equipos que la procesan para resolver posibles problemas y para adaptar los servicios a las necesidades, además, en relación con la Internet debe ser capaz de modificar los servicios para que estos se adapten, sin intervención directa de las personas. *"En el Internet de las cosas se busca que millones de equipos están interconectados transmitiendo su estado actual e información que puede ser de interés para el usuario o para algún operador de servicios y siempre de una manera dinámica cambiando su posición continuamente o en algunos casos con elementos estáticos como lo son electrodomésticos en el hogar que su rango de movimiento no es demasiado amplio ni es recurrente su desplazamiento"* Luis Carlos Luis García (2014)

Con lo planteado anteriormente se aprecia que el internet de las cosas es un sistema de dispositivos interrelacionados entre mecánicos y digitales, que tienen identificador únicos y la capacidad de transferir datos a través de una red, sin requerir de interacciones persona a persona o persona a computadora. Con la transformación tan acelerada de la tecnología se ha accedido al internet de las cosas en el mundo y el mercado lo demuestra con el predictivo generado por MarketsandMarkets ™ el cual proporciona investigación B2B cuantificada sobre 30,000 oportunidades / amenazas emergentes de alto crecimiento.

Figura 2 Mercado de Internet de las Cosas

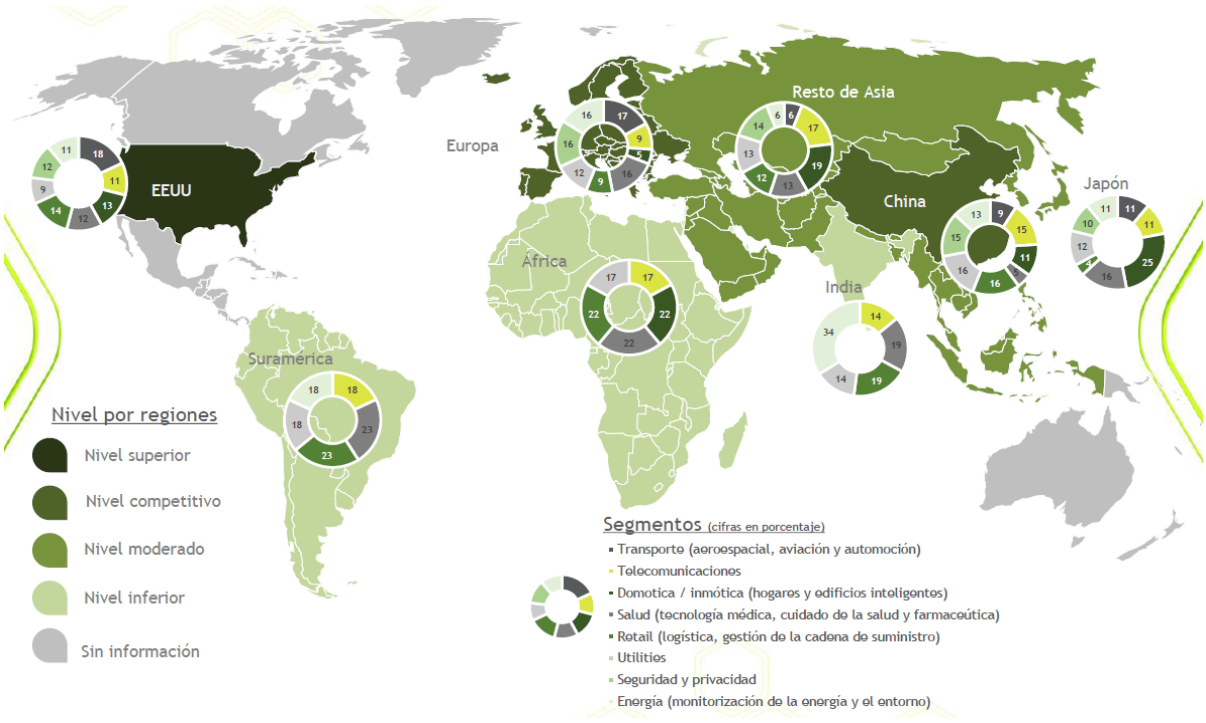


[Figura] (MARKETSANDMARKETS, 2017)

"con el incremento de los dispositivos interconectados, muchos analistas comenzaron a hacer predicciones sobre cómo sería el futuro: 50 mil millones para 2020

fue el número que citó en una presentación en 2017 el ex CEO de Ericsson Hans Vestberg. Ocho años después, la expectativa inicial en torno al sector industrial ha disminuido y los números citados son más conservadores. En la actualidad, Ericsson ofrece una visión más matizada: estima que para 2022 se pronostican alrededor de 29 mil millones de dispositivos conectados, de los cuales alrededor de 18 mil millones estarán relacionados con la IoT." Tony Anscombe (2018)

Figura 3 PENETRACIÓN DEL INTERNET DE LAS COSAS POR REGIONES Y SEGMENTOS



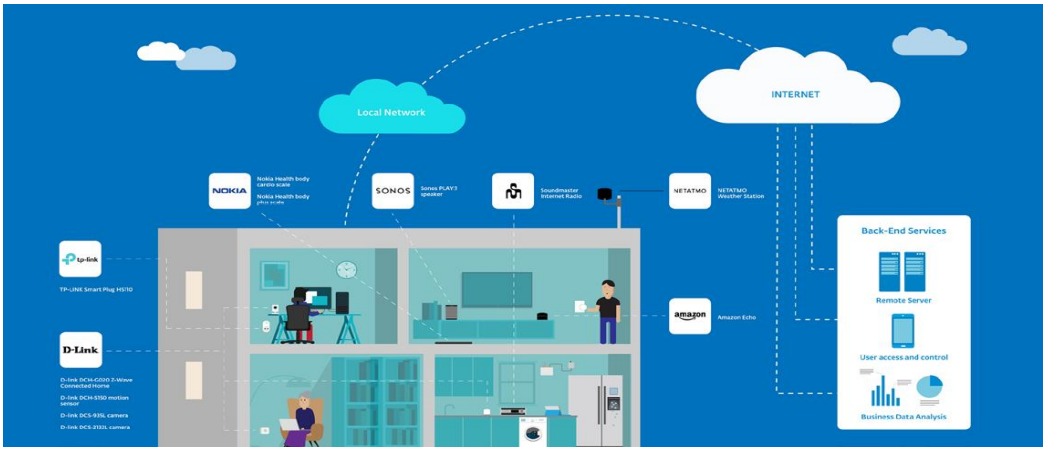
[Figura](Corporación Ruta N, 2015).

Por este crecimiento excesivo, comienza a generar la inquietud sobre los riesgos que surgen de compartir datos de manera inadvertida o inapropiada acerca de sus hábitos o su estilo de vida, captados por estos dispositivos con sensores. Y en la actualidad los datos compartidos son de extremo cuidado ya que justifica plenamente preocupaciones frente a la tendencia actual de ciberataques o delito informático.

"Un delito Informático o ciberdelincuencia, es toda aquella acción ilegal que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet. Muchos de estos delitos, al no estar tipificados en la ley, se definen como abusos informáticos." Centeno, F. J. U. (2015)

Por lo cual cada fabricante debe tener una política de privacidad o documento que explique cómo se recopilan y utilizan los datos por un dispositivo, definiendo los límites de la responsabilidad que como fabricante tiene al entregar el producto. Los hogares inteligentes, denominados así por la participación del internet de las cosas dentro de todo su funcionamiento por medio de dispositivos, deben tener en cuenta que ningún dispositivo o software está exento de tener vulnerabilidades potenciales. Sin embargo, se puede juzgar a las empresas en función de cómo reaccionan ante la divulgación de una falla en sus productos y cómo se han solucionado rápidamente con un nuevo software y firmware.

Figura 4 Ejemplo Hogar inteligente modo de conexión de dispositivos



[Figura] (Tony Anscombe,2018)

Con los ejemplos de estudio de seguridad para IOT, como es el caso de Eset el cual realiza a 12 productos de 8 proveedores donde se toma un panel de control de automatización del hogar capaz de administrar sensores de movimiento, controles de calefacción, motores de persianas, sensores de ambiente y enchufes inteligentes enuncia las vulnerabilidades así:

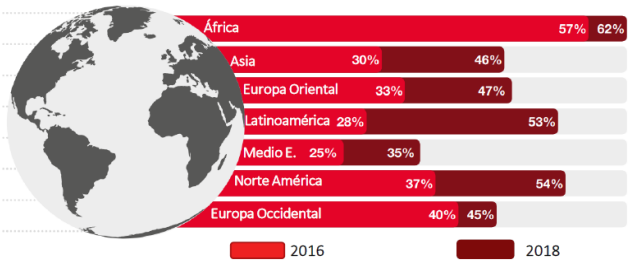
“

- *El proceso de inicio de sesión desde la red local no está completamente autenticado. La opción predeterminada es permitir el inicio de sesión automático, lo que evita la necesidad de usar credenciales estándar como ID de usuario y contraseña. El fabricante menciona este problema en una alerta de seguridad y recomienda deshabilitar la opción predeterminada.*
- *Como ocurre con casi todos los sistemas de hogares inteligentes, un servicio en la nube brinda la funcionalidad para administrar los dispositivos conectados desde un solo lugar. Pero en este caso, las comunicaciones enviadas al servicio en la nube no están cifradas.*
- *El servicio en la nube del fabricante tiene la capacidad de establecer una conexión de red privada virtual (VPN) con los dispositivos remotos. Una vez que se establece este túnel, podría ser posible cambiar la configuración de la red remota. Esto podría otorgarle acceso a la red local a usuarios no autorizados.*
- *El acceso al servicio en la nube requiere el registro del usuario, pero si los detalles del usuario fueron comprometidos, el acceso de la VPN a la red remota podría presentar un riesgo considerable.* ”Tony Anscombe (2018)

Se denota entonces la necesidad de proteger los dispositivos mucho más por medio de equipos y políticas que disminuyan las amenazas presentes a nivel mundial que afecten los datos o información vital de las personas que los usan.

Sobre latinoamérica se presenta que hay mayor crecimiento de la tasa de fraude a nivel global según reporte de Pulling fraud out of the shadows de Global Economic Crime and Fraud Survey 2018 y Fraude al descubierto de Encuesta Global de Crimen Económico en Colombia PWC 2018

Figura 5 Tasa de fraude o crimen económico a nivel regional



[Figura] (Castaño Gutiérrez, 2018)

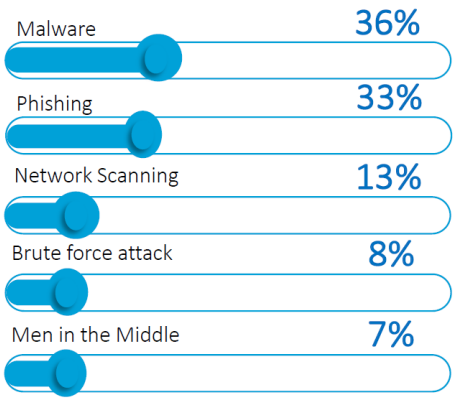
Implicando que el control de organizaciones dado por sistemas es afectado por ciberataques teniendo en cuenta las estadísticas reportadas por el centro cibernético policial en qué; *"El cibercrimen en el país aumentó 28,3% en 2017 frente a los resultados de 2016 y 446 empresas reportaron haber sido víctimas de ciberataques"* (Centro cibernético policial, 2017)

Los ataques tienden a ser dirigidos a diferentes clases de interés por lo que estos atacantes se dividen en tipos como lo son;

- Hacktivistas, decididos a hacer actividades dañinas o a favor por diferentes causas de tendencia, como algo ambiental.
- Insiders, buscan solo conseguir dinero sobre cualquier información.
- Crimen organizado, se especializan en ocultar sus operaciones y rastrear información que los afecte.
- Naciones, algunas naciones hacen rastreos y tendencias de información.
- Terroristas, estos solo buscan el caos de un país.

Se valida el 97% de los fraudes o ciberataques, provienen de fuentes conocidas o distinguidas de la siguiente manera.

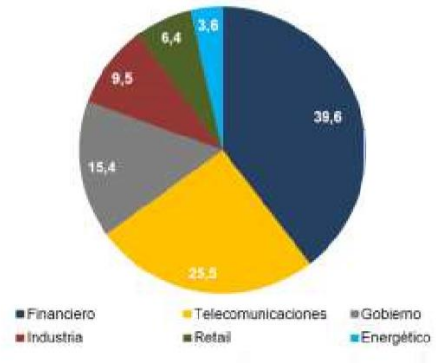
Figura 6 Fuentes de Ciberataque



[Figura] (Castaño Gutiérrez, 2018)

Para el país la distribución de los ataques cibernéticos por sector de empresas en 2017 dio como resultado la siguiente estadística.

Figura 7 Distribución de los ataques cibernéticos por sector en 2017



[Figura](Valencia Duque, 2019)

En consecuencia, los ataques hechos a empresas, pueden ser reflejados en el sector de hogares inteligentes que está creciendo a pasos agigantados y dejando a los usuarios con la inquietud de cómo deben proteger su información.

4.2 Elementos Conceptuales

¿Cómo podemos protegernos?

"Lo primero de todo, el usuario debe ser consciente de que muchos dispositivos IoT son pequeños ordenadores compatibles con la web que se pueden controlar desde el exterior" afirma Michael Veit, IT Security Expert at Sophos. (Iberia & Iberia, 2019)

Dispositivos IoT que conforman un proyecto de Automatización (Domótica)

Dentro de la automatización de un hogar inteligente se encuentra varios grupos de sistemas, conformados de la siguiente manera:

- Control de iluminación
- Integración
- Control de temperatura
- Seguridad electrónica
- Audio
- Video
- Redes de datos

Mencionar todos los dispositivos que conforman integralmente cada uno de estos sistemas, es extenso, por lo que el estudio centrará su selección bajo la experiencia del grupo de trabajo en los proyectos implementados por la constructora IoT de nombre HIGH CLASS Technology.

Dispositivos seleccionados para auditar y proteger

Se describen brevemente los dispositivos usados en los diferentes sistemas de un hogar inteligente teniendo en cuenta sus características o funcionamiento con términos coloquiales, para un lenguaje técnico y preciso se debe recurrir a las fichas técnicas de las referencias mencionadas.

Control de iluminación

- Procesador
  - **Referencia:** Pyng Hub
  - **Marca:** Crestron
  - **Descripción:** Se encarga de controlar a través de radiofrecuencia los elementos que conforman el control de iluminación, switches, dimmers, antenas, sensores, permitiendo centralizar la información recolectada y generar un entorno gráfico para la interacción con el usuario desde una aplicación o pantallas distribuidas en el hogar.

Integración

- Procesador:
  - **Referencia:** MC3
  - **Marca:** Crestron
  - **Descripción:** Integra los diferentes dispositivos que conforman el sistema domótico de un hogar, permitiendo unificar en un solo control un grupo de acciones, nombrado las escenas o configuraciones predeterminadas, ejemplo de esto será, al presionar un botón en el control de iluminación nombrado romántico, encenderá la chimenea, bajara las cortinas, atenuara la iluminación del área a un porcentaje bajo, encenderá los dispositivos de música ambiental bajo sonidos románticos preestablecidos.

Control de temperatura

- Termostato:
  - **Referencia:** Next.
  - **Marca:** Google
  - **Descripción:** Controla dispositivos de enfriamiento y calefacción dentro del hogar, permitiendo adecuar la temperatura deseada por el usuario de forma autónoma, genera reportes de consumo, se conecta a una app en la cual informa consumos de energía, temperatura promedio, permite agendamiento para encendido y apagado o cambios de temperatura por horarios, centraliza todos los aires o calefactores en una sola aplicación o interfaz gráfica.

Seguridad electrónica

- Alarma de intrusión:
  - **Referencia:** Power Neo
  - **Marca:** DSC
  - **Descripción:** Integra y controla dispositivos de seguridad perimetral en el hogar, sensores de apertura, temperatura, movimiento, inundación, rotura de vidrio, Co2 entre otros.
- Video vigilancia:
  - **Referencia:** M1011
  - **Marca:** Axis
  - **Descripción:** Cámara de video ip, conexión a la red cableada o inalámbrica, almacenamiento en almacenamiento de vídeo en red NVR (Network video recorder), visualización en vivo a través de streaming.
- Control de acceso biométrico:
  - **Referencia:** Biostation 2.
  - **Marca:** Bosch

- **Descripción:** Lectora de control de acceso biométrico e identificación por radiofrecuencia Radio Frequency Identification (RFID), permite almacenamiento interno de usuarios, huellas, puertas, salidas de relevos para aperturas de puertas, genera reportes de control de horario y aperturas.

Audio

- Audio Multizona:
  - **Referencia:** Play One
  - **Marca:** Sonos
  - **Descripción:** Parlante con control de voz por dispositivo alexa de amazon incorporado, control por app, integración con app de terceros, funcionamiento por wifi, conexión a la nube de sonos, sistema escalable e integrable con más referencias de la marca sonos, play 3, play 5, play bar, sonos amp, sonos bean, play 1, connect amp.

Video

- Televisión o proyección smart:
  - **Referencia:** Por definir
  - **Marca:** LG
  - **Descripción:** Smart TV, 50” conexión a internet LG webOS sistema operativo

Redes de datos

- Switch Capa 2:
  - **Referencia:** GS950/24
  - **Marca:** Allied telesis
  - **Descripción:** Switch administrable de 24 puertos 10/100/1000

- Router
    - **Referencia:** RB750GL
    - **Marca:** Mikrotik
    - **Descripción:** Dispositivo de enrutamiento dentro de la red, 5 puertos de 1 GB.

Dispositivos y equipos de seguridad a implementar

Según los sistemas indicados anteriormente de un hogar inteligente, se presenta la idea de implementar las soluciones de seguridad para reducir las amenazas a través de dispositivos core con indicaciones y configuraciones guiadas a la tendencia actual.

Endpoint protection

- **Referencia:** Intercept
    - **Marca:** Sophos
- **Descripción:** *"Para detener la más amplia variedad de amenazas, Sophos Intercept X utiliza un completo enfoque de defensa exhaustiva a la protección para endpoints, en lugar de simplemente depender de una técnica de seguridad principal. Este es "el poder del más", una combinación de técnicas base (tradicionales) y modernas (next-gen) líderes. Intercept X combina la protección contra malware y exploits mejor valorada del mercado con la detección y respuesta para endpoints (EDR) integradas."* ("Endpoint Protection: Sophos Intercept X Advanced Endpoint Security", 2019)

Firewall

- **Referencia:** Next-Gen
- **Marca:** Sophos

- **Descripción:** *"Sophos XG Firewall proporciona una visibilidad sin precedentes sobre su red, usuarios y aplicaciones directamente desde el centro de control. También ofrece una generación de informes detallados integrada y la opción de añadir Sophos iView para la generación de informes centralizada para múltiples firewalls.*

  XG Firewall ofrece la mejor protección contra las últimas amenazas avanzadas como el ransomware, la criptominería, bots, gusanos, hackers, filtraciones y amenazas avanzadas recurrentes.

  - *Potente tecnología de espacio seguro de Sandstorm*
  - *Deep Learning con inteligencia artificial*
  - *IPS de máximo rendimiento*
  - *Protección avanzada contra amenazas y redes de bots*
  - *Protección web con AV dual, emulación de JavaScript e inspección SSL*

  XG Firewall, toda una novedad en el sector, integra la tecnología del Deep Learning en los espacios seguros de nuestro Sophos Sandstorm. Ha sido desarrollada por científicos de datos de SophosLabs para proporcionar las mejores tasas de detección sin utilizar firmas. Detecta el malware desconocido que se esconde en las cargas sospechosas de forma rápida y efectiva. Es solo una de las formas en que XG Firewall frena las amenazas desconocidas en seco.

  XG Firewall integra parte de la mejor tecnología de nuestra protección líder de última generación Intercept X para endpoints, como la prevención de exploits y la protección CryptoGuard para identificar exploits de malware y ransomware antes de que puedan acceder a su red. En combinación con nuestro sistema de prevención de intrusiones (IPS) de máximo rendimiento, da igual que los hackers intentan aprovechar una vulnerabilidad de la red o de un endpoint, XG

Firewall los frena en seco."("Firewall de última generación de Sophos: Protección empresarial con Security Heartbeat | Firewall centralizado e integración de endpoints", 2019)

Plataforma centralizada

- **Referencia:** Sophos Central
- **Marca:** Sophos
- **Descripción:** *"Sophos Central le permite administrar nuestra plataforma galardonada de Synchronized Security. Los ataques avanzados están más coordinados que nunca. Ahora, sus defensas también lo están. Nuestro revolucionario Security Heartbeat™ garantiza la comunicación entre su protección de endpoints y su firewall. Es una idea sencilla pero eficaz que le proporciona una mayor protección contra amenazas avanzadas y le permite responder a incidentes de forma más rápida. Es tan sencilla que se preguntará por qué nadie antes lo había hecho."*("Plataforma de gestión de seguridad sincronizada para redes: Sophos Central", 2019)

Políticas de seguridad

El objetivo principal de una política de seguridad es:

- Informar a los usuarios de la red o dispositivos IoT sus obligaciones para proteger a los recursos dentro del sistema, como hardware, software, documentos o cualquier tipo de información que pertenezca a un hogar o empresa.
- Especificar los mecanismos a través de los cuales estos requerimientos pueden ser logrados.
- Proveer una guía que permitirá implementar, configurar y controlar los sistemas de la red y dispositivos IoT para determinar su conformidad con la política.
- Una política de seguridad debe asegurar cuatro aspectos fundamentales en una solución de seguridad: autenticación, control de acceso, integridad y confidencialidad, a partir de estos, surgen los principales componentes de una política de seguridad.

Recomendaciones generales para el usuario

- *Mi hogar (red) es mi castillo: nunca comparta su red doméstica con otros.*
- *En general, haga una simple búsqueda en Internet para descubrir cómo evaluar el nivel de seguridad de los dispositivos de IoT de su hogar inteligente.*
- *Reemplace inmediatamente las contraseñas que vienen de fábrica con contraseñas seguras cuando el dispositivo esté instalado.*
- *Si hay actualizaciones disponibles (y este es un requisito previo para la seguridad), siempre actualice el firmware.*
- *Elimine los dispositivos IoT de su red doméstica tanto como sea posible. Un ejemplo: si su señal de televisión se recibe principalmente por cable o antena, su televisor también se puede administrar sin acceso inalámbrico a Internet.*

- *En su red doméstica, haga una distinción entre los componentes importantes y los que no lo son. Deben configurarse para estar en diferentes redes para asegurarse de que los posibles dispositivos no seguros no tengan acceso a datos confidenciales.*
- *Lo que es aún más seguro es crear áreas de red "selladas" para su oficina de casa, electrodomésticos, sistemas de construcción y seguridad y la red de invitados con diferentes redes inalámbricas. Esto se puede lograr por medio de un firewall que solo permite la comunicación necesaria para usar los dispositivos, evitando que una infección se propague de un dispositivo IoT a otro.*
- *Utilice la tecnología VPN: en lugar de habilitar el acceso remoto desde Internet a los dispositivos IoT configurando el reenvío de puertos no seguros en el router, es mejor usar tecnología segura VPN en su teléfono inteligente o Mac / PC.*
- *Y es evidente que los dispositivos "tradicionales" como PC, teléfonos inteligentes y computadoras portátiles también deben protegerse con un programa antivirus. Hay versiones gratuitas disponibles.*

" (Iberia & Iberia, 2019)

Servicios ofrecidos por el sistema:

La razón de ser del sistema de información es ofrecer servicios a los usuarios, cada uno de los servicios que presenta el sistema incurre en riesgo propio que deben ser valorados y analizados profundamente, como parte de una definición amplia de políticas de seguridad, y posterior generación de un plan de contingencias que permite regenerar el sistema completo, o parte del caso de un evento catastrófico, bien sea natural vandálico o fortuito, y el cual puede afectar el hardware, el software o el entorno físico del sistema de información.

Estos servicios generan cada uno de los diferentes requisitos para acceder a ellos, por lo que cada uno se describirá brevemente y de manera independiente.

- **Almacenamiento en la red:** la totalidad de usuarios de un sistema tienen el atributo técnico, así como están obligados por protección de la información, a guardar toda la información, producto de su diario laboral en la red de acuerdo a una distribución de grupos de usuarios, tipos de archivos, entre otros, la cual está clasificada normalmente por departamentos o áreas del sistema, todos los espacios de la red son utilizados por todos los usuarios y dispositivos IoT que tienen acceso a ella, en la cual se restringirá el envío de la información detectada con código malicioso (malware, sniffer, keyloguer, virus), entre otras.
- **Acceso a internet:** La totalidad de dispositivos IoT tendrán acceso a internet para permitir su comunicación en la nube por protocolos como de control de transmisión Transmission Control Protocol (TCP) punto a punto (point to point, (P2P)), protocolo de transferencia de archivos seguro (Secure Simple File Transfer Protocol (SFTP)), los cuales serán monitoreados y restringidos por el firewall como reglas de entrada y salida, redirección de puertos, traducción de puertos de red Network Address Translation (NAT), realizando filtro por contenido de acuerdo con las políticas de acceso de datos especificado por cada fabricante.
- **Comunicación con el servidor:** la mayoría de dispositivos IoT establecen comunicación con un servidor o controladora, para la cual se restringirá los permisos suministrados a esta, los horarios de conexión, envío de información no aprobada por el usuario, cambio de usuarios y contraseñas de fábrica del sistema, bloqueo de los protocolos sin uso, bloqueo de puertos sin uso, cambio de puertos de fábrica.

Tipos de personas que acceden al sistema:

Existen varios grupos de personas que interactúan con el sistema Iot los cuales por sus funciones dentro del sistema tienen diferentes responsabilidades y permisos frente a

este, estas personas se pueden diferenciar en tres (3) grupos: usuarios, administradores de la información y administradores del sistema.

- **Usuarios:** se llama usuario del sistema a toda persona, que interactúe con los aplicativos de un dispositivo IOT, los usuarios que hagan uso de los dispositivos IoT que conforman un sistema de automatización o domótica.
- **Administradores de la información:** se llama administradores de la información a quien es el responsable de las aplicaciones y de velar por la calidad de los datos que hacen parte del sistema o dispositivos IoT. Esta responsabilidad está fraccionada por aplicaciones y generalmente el responsable corresponde a las políticas o funciones de cada host.
- **Administradores del sistema:** se le llama administradores de información al personal del departamento de informática o electrónica responsable por velar que la información esté disponible para que los usuarios puedan acceder a ella desde un aplicativo o sistema conectado a la red

Políticas normas y procedimientos

Las responsabilidades de los diferentes actores del sistema (usuarios, administradores de la información y administradores del sistema) y en la plataforma tecnológica existente se definen unas políticas normas y procedimientos, las cuales han sido aprobadas por el usuario (cliente) y son de obligatorio cumplimiento para todas las personas que tienen acceso al sistema.

Manejo de la información:

- Toda la información contenida en los dispositivos de la red es propiedad de la compañía y/o cliente, esta se reserva sus diferentes usos a no ser que contractualmente se especifique algo diferente.

- Los usuarios son los responsables de la calidad, confiabilidad, oportunidad y del buen uso de la información.
- Toda la información que se maneja en la compañía y/o hogar es confidencial y de uso restringido dentro y fuera del hogar y compañía, la información resultante de las actividades normales como (planos de clientes, presupuestos, fotos del proyecto, entre otras) se constituye en el conocimiento que le da ventaja competitiva y por lo tanto debe considerarse como un activo empresarial y material incluido dentro de la protección de la información contemplada en las pólizas de confidencialidad.
- La información confidencial impresa en papel deben ser destruida en lo posible con máquinas picadoras de papel, por ningún motivo estos informes deben ir a la basura. Cada persona responsable debe identificar este tipo de información y garantizar su destrucción.
- Los usuarios son los responsables de clasificar la información suministrada a los aplicativos y dispositivos IoT y de colocar contraseñas seguras alfanuméricas con caracteres especiales y de mínimos 8 dígitos a los archivos, aplicativos o dispositivos que contengan y accedan a información confidencial.
- Toda la información que reposa en las computadoras de la compañía y/o hogar, software y de mas, debe ser copiada realizando backups personales o en dispositivos de almacenamientos personales, ajenos a los dispositivos Iot que conforman el sistema, ya que esta información es susceptible de ser usada en beneficio particular o de terceros, y es considerada esta actividad una violación a las políticas, pólizas y acuerdos de confidencialidad.

5. CONCLUSIONES Y RECOMENDACIONES

- Las políticas de prevención y defensa, buscan satisfacer la necesidad del mercado emergente IOT de la ciberseguridad, que pertenece a las 8 industrias que hacen parte de la industrias 4.0.

- Los integrantes que conforman este equipo de trabajo pertenecen a diferentes disciplinas académicas lo cual permite dar más respaldo de las políticas propuestas.

- Los ataques hechos a empresas en el año 2017, donde se reportaron 400 empresas de diferentes sectores económicos, pueden verse reflejados o replicados en los hogares que cuenten con dispositivos IoT.

- Los dispositivos IoT al cumplir su función para la cual son diseñados, son equipos que recopilan información conectados a la nube (red) para lo cual se le da un valor comercial.

- Las recomendaciones para el manejo de la seguridad de la información están implícitas en el desarrollo del informe.

6. BIBLIOGRAFÍA

ebizLatam.com. (2019). Malware para dispositivos IoT triplicó su crecimiento durante el primer semestre de 2018 - ebizLatam.com. [online] Recuperado de: http://www.ebizlatam.com/malware-para-dispositivos-iot-triplico-su-crecimiento-durante-el-primer-semestre-de-2018/ [Accessed 21 Aug. 2019].

The Next Web. (2019). Digital trends 2019: Every single stat you need to know about the internet. [online] Usuarios de Internet a lo largo del tiempo [Figura] Recuperado de : https://thenextweb.com/contributors/2019/01/30/digital-trends-2019-every-single-stat-you-need-to-know-about-the-internet/ [Accessed 21 Aug. 2019].

CEPAL (2015) Comisión Económica para América Latina y el Caribe (CEPAL) . La nueva revolución digital: De la Internet del consumo a la Internet de la producción. Chile. [En línea] Recuperado de: https://www.cepal.org/es/publicaciones/38604-la-nueva-revolucion-digital-la-internetconsumo-la-internet-la-produccion.

Dave Evans (2011) Internet de las cosas, Como la próxima evolución de Internet lo cambia todo Recuperado de: Cisco Cisco Internet Business Solutions Group (IBSG) © 2011

Luis Carlos Luis García (2014) ESTUDIO DEL IMPACTO TÉCNICO Y ECONÓMICO DE LA TRANSICIÓN DE INTERNET AL INTERNET DE LAS COSAS (IoT) PARA EL CASO COLOMBIANO. Recuperado de: Tesis de investigación de la Universidad Nacional de Colombia, Facultad de Ingeniería, Departamento de Ingeniería de Sistemas e Industrial.
MARKETSANDMARKETS. (2017). marketsandmarkets.com. Atractivo del mercado IOT [Figura] Recuperado de: https://www.marketsandmarkets.com/MarketReports/internet of things market 573.html

Tony Anscombe (2018) PROTECCIÓN COMPLETA PARA UN HOGAR INTELIGENTE Recuperado de: ESET, spol. s r.o. Aupark Tower, 16th Floor Einsteinova 24, 851 01 Bratislava Slovak Republic

Tony Anscombe (2018) PROTECCIÓN COMPLETA PARA UN HOGAR INTELIGENTE Ejemplo Hogar inteligente modo de conexión de dispositivos [Figura] Recuperado de: ESET, spol. s r.o. Aupark Tower, 16th Floor Einsteinova 24, 851 01 Bratislava Slovak Republic

Centeno, F. J. U. (2015). Ciberataques, la mayor amenaza actual. Documento de Opinión, (09).

Corporación Ruta N (2015). Observatorio CT+i: Informe No. 1 Área de oportunidad en Internet of Things. Recuperado de: www.brainbookn.com

Iberia, S., & Iberia, S. (2019). Día de la Seguridad Informática: ¿Es el IoT una amenaza para tu casa?. Recuperado de: https://news.sophos.com/es-es/2017/11/30/dia-de-la-seguridad-informatica-es-el-iot-una-amenaza-para-tu-casa/

Endpoint Protection: Sophos Intercept X Advanced Endpoint Security. (2019). Retrieved 22 August 2019, from https://www.sophos.com/es-es/products/intercept-x.aspx
Firewall de última generación de Sophos: Protección empresarial con Security Heartbeat | Firewall centralizado e integración de endpoints. (2019). Recuperado de: https://www.sophos.com/es-es/products/next-gen-firewall.aspx

Castaño Gutiérrez, J. (2018). [Figura] Hacia una gestión multidimensional de la ciberseguridad 12º Congreso de prevención del fraude y seguridad -Asobancaria. 1st ed. Bogota: Jorge Castaño Gutiérrez.

Valencia Duque, F. (2019). Ciberseguridad. 1st ed. [ebook] Bogota: Francisco Javier Valencia Duque. Recuperado de: http://pensamiento.unal.edu.co/fileadmin/recursos/focos/desarrollo-sostenible/Simposio_4a_Revolucion/8_Francisco_javier_valencia/9_Francisco_Javier_Valencia.pdf

7. ANEXOS

- All-in-one NAS Server TS-101 Ficha Técnica
- ARD-FPBEPxx-OC Ficha Técnica
- Clw-delvex Ficha Técnica
- Clw-dimswex Ficha Técnica
- Control Wifi mc3 Ficha Técnica
- Fire TV Ficha Técnica
- Fire+TV+Stick+4K_Quick+Start+Guide_US Ficha Técnica
- intercept-x-edr Ficha Técnica
- manual-amazon-echo-guia-uso-alexa Ficha Técnica
- Nest-thermostat-3rd-Ficha Técnica
- PowerSeries_Neo_Controlador_de_alarma_Manual_de_usuario_V1.0_Ficha Técnica
- Pyng-hub_Ficha Técnica
- RouterBOARD 750GL Ficha Técnica
- Sonos One Ficha Técnica
- sophos-intercept-x-deep-learning-dsna Ficha Técnica
- sophos-sandstorm-dsna Ficha Técnica
- Switch-gs950series-ds Ficha Técnica