COMPUTATION E INFORMATICA

Recibido 18 JUL. 2023 *ReCIBE, Año 12 No.2, NOV. 2023*

Aceptado 28 JUL. 2023

Plug and play (upnp): métodos de ataque y medidas de protección

Plug and play (upnp): attack methods and protection measures

Leticia Chuquiana Casicana
lety.ch06@gmail.com

Galo López Sevilla

Resumen
Universal Plug and Play (UPnP), facilita la conectividad entre dispositivos pertenecientes a una misma red local y la comunicación de programas con servidores de terceros, esta tecnología viene activa por defecto en algunos routers la cual evita la configuración manual para la apertura de puertos en el mismo, ya que se realiza de forma automática. Al ser una tecnología para la comunicación y conectividad ya sea entre dispositivo o programas en internet, puede llegar a ser inseguro, puesto que terceras personas mal intencionadas pueden acceder a la red aprovechando que este protocolo esta activo, poniendo en riesgo tanto la información personal como los dispositivos conectados a la misma red. Por ende, este estudio es importante ya que, ayuda a identificar los métodos de ataque que se realiza al protocolo UPnP y definir las medidas de protección que se pueden aplicar al usar esta tecnología. El objetivo de esta investigación es identificar los métodos de ataque y medidas de protección de UPnP, la cual tendrá una investigación bibliográfica con enfoque cualitativo, además se aplica la metodología RSL para la revisión sistemática de la literatura y desarrollo del artículo. Al finalizar este trabajo de investigación se espera contar con un documento de ayuda para mitigar los ataques informáticos a usuarios que tienen activo el protocolo UPnP.
Palabras clave: UPnP, conexión, protocolos, RSL.

Abstract
Universal Plug and Play (UPnP), facilitates connectivity between devices belonging to the same local network and communication of programs with third-party servers, this technology is activated by default in some routers which avoids the manual configuration for opening ports in the router, as this is done automatically. As it is a technology for communication and connectivity either between devices or programs on the Internet, can become insecure, since illintentioned people can access the network taking advantage of the fact that this protocol is active, putting both personal information and devices connected to the same network at risk. Therefore, this study is important because, helps to identify the attack methods used to attack the UPnP protocol and define the protection measures that can be applied when using this technology. The objective of this research is to identify the methods of attacking and UPnP protection measures, which will have bibliographic research with a qualitative approach, in addition, the SLR methodology is applied for the systematic review of the literature and article development. At the end of this research work, it is expected to have a document that will be of help to mitigate cyber-attacks on users who have UPnP protocol active. **Keywords: UPnP, connection, protocols, RSL.**

1.- INTRODUCCIÓN

A nivel mundial los ataques cibernéticos han crecido a raíz de la pandemia y el teletrabajo, lo cual ha causado una ola de ataques a gran escala, ya sea a nivel empresarial como personal. Los ciberdelincuentes aprovechan cualquier vulnerabilidad para ingresar en los sistemas de las víctimas y realizar operaciones ilícitas. Existen varias formas de atacar un sistema o red, mediante el uso de herramientas, dispositivos y protocolos; como es el caso del protocolo Universal Plug and Play (UPnP).

UPnP es un conjunto de protocolos que permite la comunicación entre dispositivos de una misma red y servidores de terceros mediante la apertura automática de puertos, lo cual facilita la conexión (Maestre, 2015).

Sin duda es una tecnología muy buena ya que, no requiere de configuración manual para la apertura de puertos en los routers del hogar, por otro lado, también es un problema así lo mencionan Rapid7 (2013), en una investigación realizada en el 2012, en donde “se identificaron más de 80 millones de direcciones IP únicas que respondieron a las solicitudes de descubrimiento UPnP de Internet. En algún lugar entre 40 y 50 millones de direcciones IP son vulnerables”.

En este contexto, el problema radica en los inconvenientes que genera la conexión directa de los dispositivos a una red mediante el protocolo UPnP, ya que, este protocolo facilita la conexión y reconocimiento de dispositivos en una misma red local, de igual maneara asigna una IP generada por el Protocolo de Configuración Dinámica de Host (DHCP) a cada dispositivo (Maestre, 2015), este proceso se lleva a cabo sin notificar al usuario. Frente a esta problemática, dentro de la investigación, se pretende dar respuesta a las siguientes preguntas: ¿Cuáles son los aspectos relacionados a la seguridad en UPnP?, ¿Cuáles son los métodos de ataque utilizados en UPnP?, ¿Cuáles son las medidas de protección recomendables para aplicar en UPnP?

De tal manera que, esta investigación es importante pues, se detalla los métodos de ataque a UPnP y sobre todo se especifica medidas de protección. Una vez definido la problemática e importancia del proyecto de investigación propuesto, el objetivo es **Identificar los métodos de ataque y medidas de protección de Plug and Play (UPnP)**, en donde se verifica lo siguiente: Determinación del estado del arte sobre las seguridades de UPnP, revisión de las metodologías para el análisis de las vulnerabilidades y métodos de ataque a UPnP, selección de una metodología para el análisis de las medidas de protección aplicables a UPnP. Para llevar a cabo este proyecto de investigación se utiliza una metodología, que consiste en procedimientos y técnicas para la indagación de un problema que requiere solución (Cohen & Gómez, 2019), es así que, se utiliza una investigación bibliográfica con enfoque cualitativo y se aplica la metodología RSL para la revisión sistemática de la literatura.

2.- ESTADO DEL ARTE

2.1. ¿Qué es un Ciberataque?

En la actualidad, los ciberataques han venido ganando terreno, gracias a los avances tecnológicos que no solo han beneficiado a la población, al contrario, también han desarrollado herramientas para realizar estos delitos informáticos (Izaguirre Olmedo & León Gavilánez, 2018), un ciberataque es un ataque malicioso en donde un ciberdelincuente aprovecha cualquier vulnerabilidad de un sistema informático para introducir virus con la intención de robar información o afectar el funcionamiento de las redes de comunicación y sistemas informáticos. Así mismo, Pons (2017) indica que, para un ciberdelincuente realizar estos delitos informáticos tiene ciertas ventajas, pues no se expone de manera física a la víctima, basta con equipos informáticos, conexión a internet y conocimientos técnicos en informática pueden ejecutar los ataques de manera anónima desde cualquier parte del mundo a cualquier persona u organización.

2.2. Ciberataques a Nivel Mundial

A nivel mundial los ciberataques aumentaron un 29% en el primer trimestre del año 2021, puesto que, los ciberdelincuentes aprovecharon el teletrabajo o trabajo remoto, que fueron restricciones y medidas de seguridad aplicadas por las empresas e instituciones educativas, debido a la pandemia (Check Point, 2021).

Por otra parte, Morales (2022) menciona que, el aumento de los ciberataques también se debe a los avances y desarrollo tecnológicos, que han abierto un camino hacia el mundo digital también conocido como ciberespacio, en donde un sin número de personas intercambian información entre sí por medio de la red, sin embargo, estos avances han sido utilizados por ciberdelincuentes que realizan delitos informáticos con el objetivo de sustraer información personal, de empresas u organizaciones. Los ataques más frecuentes en el año 2022 son: ciberdelincuencia, ciberacoso, ciber espionaje, ciber amenazas entre otros.

2.3. Ciberataques en Ecuador

Según, Alvarado (2020), en Ecuador el 43% de personas tienen acceso a internet, pero la mayoría desconoce los peligros y amenazas de su uso, siendo víctimas de ciberataques; Coello (2021) manifiesta que, en el año 2021 Ecuador se ubicó en el sexto puesto según el análisis de Ciberseguridad a nivel de Latinoamérica “el ministerio de Telecomunicaciones y de la Sociedad de Información (MINTEL), Ecuador tiene carencia de implantaciones políticas y estrategias nacionales en el ámbito de la ciberseguridad que podrían mejorarse y fortalecerse.”

2.4. ¿Qué es Plug and Play (UPnP)?

UPnP es un protocolo de comunicación entre dispositivos conectados en una misma red, se caracteriza por la apertura automática de diferentes puertos del router (Maestre, 2015); a cada dispositivo se asigna una IP de manera dinámica por DHCP, “UPnP permite que se abran y cierren puertos de forma automática por orden o solicitud de un dispositivo o programa” (Fundación Proydesa, 2022).

2.5. Peligros de mantener los puertos abiertos

Novoa & Salazar (2022), Miranda (2019), el router es el encargado de transmitir información entre los dispositivos y programas conectados a una red, por ende permitir la apertura automática resulta beneficiosa para evitar problemas o molestias al usuario, sin embargo, desde el punto de vista de la seguridad informática, es peligroso, ya que la mayoría de atacantes aprovechan esta vulnerabilidad para ingresar a los sistemas informáticos y cometer delitos.

Entre los peligros que conlleva mantener los puertos abiertos son: modificación de la configuración del Sistema de Nombres de Dominio (DNS), *man in the middle* (ataque de intermediario), ataque de denegación de servicio distribuido (DDoS), creación de redes falsas, entre otras (Miranda, 2019).

2.6. Métodos de ataque a (UPnP)

Los métodos de ataque más comunes en este tipo de protocolo son los ataques DoS y DDoS, ya que tienen el objetivo de secuestrar máquinas y usarlas como *bots* para atacar un servidor, enviando una serie de peticiones con el fin de colapsarlo (Microsoft, 2022).

Para ampliar con mayor detalle este tema, se especifica en la fase tres de la Metodología RSL.

3.- METODOLOGÍA DE LA INVESTIGACIÓN

El enfoque de la investigación para este estudio fue el enfoque cualitativo, el cual se orienta a la recolección de datos con la finalidad de analizar y explicar mediante métodos y técnicas de investigación (Sánchez, 2019), así mismo, Iño (2018) define el enfoque cualitativo como: "llevar a cabo la generación de información, descripción, procesamiento, análisis e interpretación y redacción del trabajo". Además, el tipo de investigación que se emplea en ese estudio es la investigación bibliográfica, para Lafuente & Martín (2017) corresponde a la búsqueda bibliográfica o documental de distintas fuentes de información, es la revisión de investigaciones ya existentes y comprobadas por medio de hipótesis, experimentos, entre otros. Esta investigación ayuda a este estudio a buscar información de distintos autores sobre UPnP. Por otra parte, para el desarrollo de esta investigación se utiliza la metodología RSL propuesta por Kitchenham, B. & Charters, S. (2007), consta de tres etapas: planeación, ejecución y reporte de resultados. Esta metodología sigue un proceso de identificación, evaluación y combinación de estudios primarios para realizar estudios secundarios (Carrizo & Moller, 2018).

3.1. Planeación

Es la primera etapa de la metodología RSL en donde se desarrolla la identificación de la necesidad, formulación de las preguntas de investigación, selección de la fuente, definición de la cadena de búsqueda, criterios de inclusión y exclusión.

Identificación de la necesidad

El protocolo UPnP, es una tecnología que facilita la comunicación entre los dispositivos conectados a una misma red, de igual manera facilita la conexión con programas alojados en servidores de terceros, esto se da por la apertura automática de los puertos en el router; de esta manera el usuario no tiene la necesidad de activarlos manualmente para conectar un dispositivo o programa en la red (Maestre, 2015). Por otra parte, este protocolo no tiene la suficiente seguridad y tampoco identifica con exactitud que dispositivos o programas solicita la apertura de un puerto, pueden ser seguros o no, simplemente ante cualquier solicitud de apertura, el router permite la conexión mediante el protocolo UPnP. Es así que surge la necesidad de conocer los métodos de ataques utilizados en UPnP para plantear medidas de protección, mitigar posibles ataques y mantener una conexión segura en la red.

Formulación de las preguntas de investigación

Para este estudio se definen las siguientes preguntas:
P1. ¿Cuáles son los aspectos relacionados a la seguridad en UPnP?
P2. ¿Cuáles son los métodos de ataque utilizados en UPnP?
P3. ¿Cuáles son las medidas de protección recomendables para aplicar en UPnP?

Selección de la fuente

Como fuente de búsqueda se seleccionó a IEEE, por ser una base de datos de investigación académica que proporciona acceso al texto completo de artículos y trabajos sobre Ciencias de la Computación, Ingeniería Eléctrica y Electrónica (IEEE Xplore, 2022). Además, es una de las bases de datos en donde se encontró una cantidad significativa de artículos relacionados al tema de estudio.

Definición de la cadena de búsqueda

La cadena de búsqueda se definió de la siguiente manera:
TITLE-ABS-KEY (universal AND plug AND play) AND PUBYEAR > 2010

Criterios de inclusión y exclusión

Los artículos investigados deben cumplir con los criterios de inclusión: Artículos relacionados con el tema Universal Plug and Play, deben estar escritos en inglés o español, documentos de revistas, conferencias o libros indexados en IEEE; se toma en cuenta artículos desde el año 2010 debido a que se encuentra información que aporta significativamente al tema de investigación. Por otra parte, se ignoran los estudios realizados antes del año 2010 y que no corresponda a fuentes de artículos, revistas o libros.

3.2. Ejecución

En esta etapa se realiza la selección de estudios primarios y extracción de datos encontrados:

Selección de estudios primarios

Se realiza la selección de estudios primarios de la siguiente manera: Se ejecuta la cadena de búsqueda definida en IEEE, en donde se obtuvo 120 resultados. Seguido se selecciona los estudios relacionados al tema, palabras clave y preguntas de investigación en donde se elige 52 estudios. Además, se aplica los criterios de inclusión y exclusión, en el cual se excluye 36 estudios ya que su contenido no era suficiente para responder las preguntas de investigación y los años de publicación eran antes del año 2010. Finalmente se selecciona 16 estudios para esta investigación (ver la Figura 1).

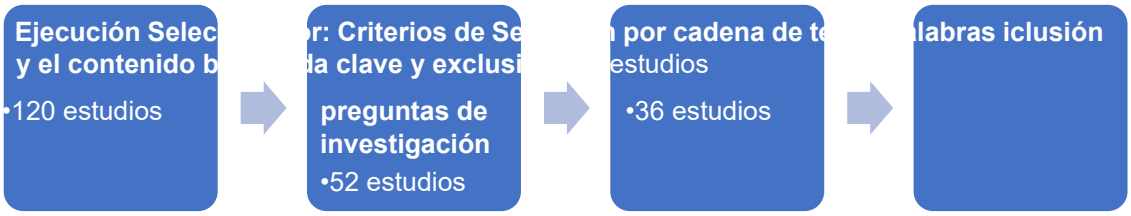

Figura 1. Selección de estudios primarios, elaboración propia.

Extracción de datos encontrados

Una vez seleccionado los estudios de mayor relevancia se procede a la extracción de la información, en donde se utiliza una matriz en Excel que contiene año, autor, título del artículo, URL y posible respuesta a las preguntas planteadas: P1, P2, P3, esto con el fin de llevar una mayor organización de los artículos de acuerdo al año e información obtenida (ver la Figura 2).

A	B	C	D	E
Año	Autor	Título del Artículo	URL	Posible respuestas
2022	Pravin Nair; Kunal N. Chaudhury	Regularización Plug-and-Play usando solucionadores lineales	https://ieeexplore.ieee.org/document/9913822	Convergencia objetiva y de punto fijo
2021	Aristotelis M Tsimtsios; Vassilis C Nikolaidis	PROTECCIÓN PLUG-AND-PLAY: UNA SOLUCIÓN ANTE LA COMPLEJIDAD DE DISEÑO DE ESQUEMAS DE PROTECCIÓN	https://ieeexplore.ieee.org/document/9692104	Para hacer frente a la complejidad de
2021	Xi Fang; Guoqi Sun; Wenjing Li; Liuwang Wang	Diseño de estrategia de identificación automática para módulos funcionales plug-and-play del controlador de	https://ieeexplore.ieee.org/document/9635173	La estrategia de identificación autom
2021	Eudes Rigoberto Apaza Estaño ; Luis Enrique Baca Wiesse ; Christian Augusto Romero Goyzueta	Diseño de firewall empresarial Plug and Play IPv6 basado en Iptables, Nettop y Linux	https://ieeexplore.ieee.org/document/9591064	

Figura 2: Extracción de datos encontrados, elaboración propia.

3.3. Reporte de resultados

En esta etapa se presenta los resultados obtenidos de la RSL.

P1. ¿Cómo funciona UPnP?

UPnP está diseñado para la conexión de dispositivos domésticos y de pequeñas empresas, se usa habitualmente para la conexión de Dispositivos del Internet de las cosas (IoT), Streaming de vídeo, juegos en línea, para la comunicación rápida entre dispositivos (Kayas, Hossain, Payton, & Islam, 2020).

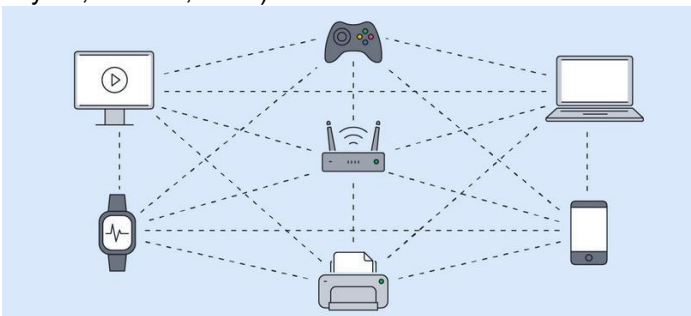

Figura 3. Conexión entre dispositivos UPnP, (Ghimiray, 2022)

En la Figura 3, muestra como es la conexión de los dispositivos UPnP conectados a una misma red, pueden estar conectados dos o más dispositivos entre sí. Además, los dispositivos UPnP se dividen en dos categorías: Dispositivos de Servicio (SD) y Puntos de Control (CP) en donde, SD es el servidor encargado de prestar el servicio; mientras que, CP es un cliente que utiliza los servicios proporcionados por SD (Kayas, Hossain, Payton, & Islam, 2020). Tanto CP como SD, pueden ser dispositivos o programas.
Por otra parte, el funcionamiento de UPnP pasa desapercibido para el usuario, ya que al conectar un dispositivo a la red este se une sin necesidad de alguna configuración manual, todo el proceso de conexión es interno entre los dispositivos, en donde intervienen protocolos como: Protocolo Simple de Descubrimiento de Servicios (SSDP), Protocolo de Transporte de Hipertexto (HTTP), Protocolo de Datagramas de Usuario (UDP), Protocolo de Control de Transmisión (TCP), Protocolo Simple de Acceso a Objetos (SOAP), Seguridad de la Capa de Transporte (TLS), Arquitectura General de Notificación de Eventos (GENA), Protocolo de Internet (IP) y Eventos *Multicast* (Pehkonen & Koivisto, 2010) (Mussi, Barreto, & Cugnasca, 2016).

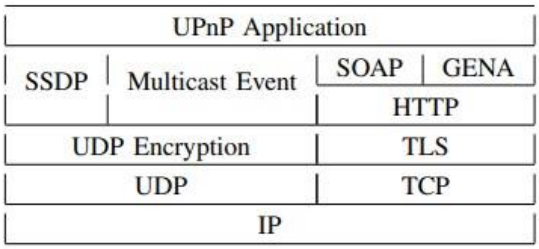

Figura 4. Elementos usados en UPnP, (Pehkonen & Koivisto, 2010)

Como se muestra en la Figura 4, son varios los elementos que intervienen para establecer la conexión entre los dispositivos y una red, cada uno de los protocolos aportan funcionalidades que es aprovechada por UPnP, además, para su correcto funcionamiento UPnP utiliza los puertos 7676 y 1900 del protocolo TCP (Nava-Lopez & otros, 2019). Por otra parte, el proceso que realiza para conectar un dispositivo a la red consta de 6 fases (Grimmett & O'Neill, 2012), (Guo & Li, 2013); en la siguiente tabla se explica el proceso de conexión que utiliza UPnP, en donde hace uso de los elementos mencionados en la Figura 2:

Dirección	Un nuevo dispositivo se une a la red y se le asigna una dirección IP mediante DHCP.
Descubrimiento	El dispositivo anuncia su presencia enviando mensajes mediante protocolo UDP, para la búsqueda y publicidad de los dispositivos interviene el protocolo SSDP.
Descripción	El dispositivo muestra sus servicios a la red.
Control	Otros dispositivos de red comienzan a interactuar con el nuevo dispositivo por medio del protocolo SOAP.
Eventos	Por medio de los eventos, los dispositivos anuncian cambios en sus variables de estado al nuevo dispositivo e informan a este cuando necesitan sus servicios. Los mensajes de notificación de eventos se forman mediante GENA y se envían por HTTP sobre TCP.
Presentación	En algunos casos, el dispositivo contiene una interfaz de usuario a la cual se puede acceder mediante una URL y obtener información o usarla para cambiar la configuración del dispositivo.

Tabla 1. Etapas de conexión UPnP, basado en (Grimmett & O'Neill, 2012) y (Guo & Li, 2013)

Son buenos los beneficios y comodidad que brinda UPnP en la conexión y comunicación de dispositivos en la red; sin embargo, en el tema de seguridad según Zheng, Li & Chen (2011), UPnP no fue diseñado con suficiente seguridad, ya que según estadísticas el 20% de productos habilitados para UPnP están expuestos a amenazas externas e internas que aprovechan cualquier vulnerabilidad para atacar a los dispositivos. Nava-Lopez & otros (2019), también menciona que, un dispositivo se conecta dinámicamente a la red, se asigna una IP con la cual puede comunicarse con los demás dispositivos conectados en la misma red, pero al desconectarse no deja ningún rastro de la actividad realizada en la red, dejando agujeros de seguridad en donde personas mal intencionadas pueden aprovechar para ingresar a la red utilizando distintos métodos de ataque.

P2. ¿Cuáles son los métodos de ataque utilizados en UPnP?

El proceso de conexión de UPnP es automático, pero debe pasar por seis etapas en donde se pueden encontrar vulnerabilidades ya que no proporciona confiabilidad, integridad y autenticidad en los mensajes enviados por la búsqueda y publicidad de dispositivos conectados, además UPnP no detecta si las peticiones enviadas son desde servidores o dispositivos confiables, simplemente las acepta y pasa por el procesos de conexión sin ningún problema (Sales, Sales, Almeida, Perkusich, & Sales, 2013). Las etapas en donde corre el mayor riesgo son: descubrimiento, descripción, control y eventos; ya que, son las etapas en donde tienen mayor interacción los CP y SD (Kayas, Hossain, Payton, & Islam, 2020). En la Tabla 2, se describen los ataques más comunes encontrados en UPnP:

Método de Ataque	**Consecuencia**	**Autor**
Denegación de servicio	Un dispositivo malicioso sobrecarga una red UPnP enviando demasiadas solicitudes de descubrimiento, con el fin de que un dispositivo de servicio no se encuentre disponible para dispositivos legítimos. Como consecuencia de este ataque es el consumo excesivo de memoria, bajo rendimiento y bloqueo temporal del sistema.	(Kayas, Hossain, Payton, & Islam, 2020)
Desbordamiento de búfer	Esta vulnerabilidad sucede porque en la implementación de UPnP contiene un búfer no verificado en uno de sus componentes, el cual es el responsable de procesar los mensajes que anuncian la disponibilidad de dispositivos compatibles con UPnP en una red. Es posible desbordar el búfer mediante una inundación de mensajes desde un dispositivo malicioso, dando como resultado libre acceso al atacante para que obtenga el control del sistema, una vez, comprometido el sistema el atacante puede borrar toda evidencia después del ataque, siendo imposible rastrear al atacante.	(Hasib & Mottalib, 2010)
Consumo de energía	Los dispositivos UPnP funcionan enviando mensajes multicast periódicamente para notificar su presencia, este proceso consume energía a un nivel najo. Si un atacante consigue obligar a los dispositivos enviar anuncios multicast con demasiada frecuencia, hará que el dispositivo consuma energía a un nivel más alto y posiblemente deje de funcionar.	(Hasib & Mottalib, 2010)

Tabla 2. Métodos de ataque UPnP

Los ataques descritos en la Tabla 2, son considerados como principales en UPnP, pero a raíz de estos se derivan los siguientes: suplantación de identidad de dispositivos de servicio, suplantación de puntos de control, agotamiento de recursos al implementar UPnP en redes IoT, falsificación de mensajes de publicidad, falsificación de eventos, inyección de malware (Carron, Wabersich, & Zeilinger, 2021), (Santos, et al., 2020); estos ataques son consecuencias de la poca seguridad que ofrece UPnP, ya que los atacantes se aprovechan de las vulnerabilidades como: ausencia de autenticación en anuncio y publicidad, falta de autenticación en la etapa de control, falta de verificación de integridad en la etapa de eventos, falta de verificación en la etapa de descubrimiento (Kayas, Hossain, Payton, & Islam, 2020).

P3. ¿Cuáles son las medidas de protección recomendables para aplicar en UPnP?

Las medidas de protección de los principales ataques a UPnP son las siguientes:

Ataque	**Medida de Protección**
Denegación de Servicio	Implementar un sistema de detección y prevención de intrusiones (IDS/IPS) que monitorizan las conexiones y alertan si se detecta intentos de acceso no autorizados o mal uso de protocolos. Deshabilitar los servicios UPnP en caso de presentar un fallo en el Sistema Operativo.
Desbordamiento de búfer	Este ataque se puede evitar utilizando la asignación de memoria dinámica en lugar de la asignación estática para la descripción del dispositivo, permitir la descarga de la descripción del dispositivo solo a través del puerto mayor 1024.
Consumo de energía	Instalando un software de medición de energía en el dispositivo UPnP, con el fin de monitorear la curva de consumo de energía; ya que el atacante debe ser alguien dentro de la red, es posible rastrearlo obteniendo la dirección IP de donde provienen los mensajes de búsqueda.

Tabla 2. Medidas de protección, basado en (Guo & Li, 2013) (Hasib & Mottalib, 2010), (Kayas, Hossain, Payton, & Islam, 2021)

Asimismo, como medidas generales de protección, se recomienda: actualizar el firmware del router, uso de contraseñas fuertes, revisar los dispositivos conectados en el router, actualizar los sistemas operativos de los dispositivos con las últimas versiones, reestablecer las configuraciones de fábrica del router, descargar e instalar software de fuentes confiables.

4. CONCLUSIONES

- La funcionalidad de UPnP es compleja, ya que, no solo hace uso de otros protocolos, `al nuevo dispositivo, este envía su IP asignada y otros datos a los demás dispositivos conectados para empezar a interactuar y al mismo tiempo enviar notificación de eventos cuando uno de ellos necesita los servicios de otro dispositivo.
- En cuanto a los ataques, se encontraron tres de mayor impacto, las cuales se filtran por medio de las vulnerabilidades de los protocolos con los que trabaja UPnP.
- Las medidas de protección para los principales ataques constan de la instalación de software específico para evitar dichos ataques que son comunes a nivel de seguridad informática, además se describen medidas generales de protección que dependen del factor humano; con la ausencia de dichas medidas preventivas, una red UPnP pude sufrir de amenazas criticas para la red y los dispositivos.

BIBLIOGRAFÍA

Alvarado, J. E. (2020). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. *Revista Científica Aristas*. Obtenido de https://revistacientificaistjba.edu.ec/images/home/ documentos/Mayo_2020/2.pdf

Carrizo, D., & Moller, C. (2018). Estructuras metodológicas de revisiones sistemáticas de literatura en Ingeniería de Software: un estudio de mapeo sistemático. *Scielo*. Obtenido de Scielo: http://dx.doi.org/10.4067/S0718-33052018000500045

Carron, A., Wabersich, K. P., & Zeilinger, M. N. (abril de 2021). Plug-and-Play Distributed Safety Verification for Linear Control Systems With Bounded Uncertainties. *IEEE Transactions on Control of Network Systems*. Obtenido de https://doi.org/10.1109/TCNS.2021 .3074218

Check Point. (2021). *Ransomware Exploits and Supply Chain Attacks Lead the Cyber Trends in the First Half of 2021*. Obtenido de https://pages.checkpoint.com/cyber-attack-2021trends.html#:~:text=Global%20cyber%20attacks%20increased%20by,attack%20techniq ue%20called%20Triple%20Extortion.

Coello, I. N. (2021). Análisis de ciberataques en organizaciones públicas del Ecuador y sus impactos administrativos. Obtenido de https://dspace.ups.edu.ec/handle/ 123456789/20738

Cohen, N., & Gómez, G. (2019). *Metodología de la investigación, ¿para qué?: la producción de los datos y los diseños.* Buenos Aires: Editorial Teseo. Obtenido de http://biblioteca.clacso.edu.ar/clacso/se/20190823024606/Metodologia_para_que.pdf

Fundación Proydesa. (2022). *¿Qué es UPnP y para qué sirve?* Obtenido de https://www.proydesa.org/portal/index.php/noticias/1746-que-es-upnp-y-para-que-sirve

Ghimiray, D. (2022). *¿Qué es UPnP (Universal Plug and Play)?* Obtenido de https://www.avg.com/es/signal/what-is-unpn

Grimmett, J., & O'Neill, E. (2012). UPnP: Breaking out of the LAN. *IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. Obtenido de https://doi.org/10.1109/WCNCW.2012.6215483

Guo, X., & Li, J. Z. (2013). Secure UPnP services based on group signature algorithm. *Proceedings of 2013 3rd International Conference on Computer Science and Network Technology*. Obtenido de https://doi.org/10.1109/ICCSNT.2013.6967261

Hasib, A. A., & Mottalib, M. (2010). Vulnerability Analysis and Protection Schemes of Universal Plug and Play Protocol. *IEEE International Conference on Computational Science and Engineering*. Obtenido de https://doi.org/10.1109/CSE.2010.37

IEEE Xplore. (2022). *IEEE Xplore Digital Library*. Obtenido de https://biblioguias.uam.es/tutoriales/ieeexplore

Iño, W. G. (2018). Investigación educativa desde un enfoque cualitativo. *Dialnet*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6521971

Izaguirre Olmedo, J., & León Gavilánez, F. (2018). Análisis de los ciberataques realizados en América Latina. *INNOVA Research Journal, 172–181*. Obtenido de https://doi.org/10.33890/innova.v3.n9.2018.837

Kayas, G., Hossain, M., Payton, J., & Islam, S. M. (2020). VSDM: A Virtual Service Device Management Scheme for UPnP-Based IoT Networks. *IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*. Obtenido de https://doi.org/10.1109/UEMCON51285.2020.9298148

Kayas, G., Hossain, M., Payton, J., & Islam, S. M. (2021). SUPnP: Secure Access and Service Registration for UPnP-Enabled Internet of Things. *IEEE Internet of Things Journal*. Obtenido de https://doi.org/10.1109/JIOT.2021.3058699

Kayas, G., Hossain, M., Payton, J., & Islam, S. R. (2020). An Overview of UPnP-based IoT Security: Threats, Vulnerabilities, and Prospective Solutions. *IEEE Annual Information Technology, Electronics and Mobile Communication Conference*. Obtenido de https://doi.org/10.1109/IEMCON51383.2020.9284885

Kitchenham, B., & Charters, S. (2007). *Guidelines for Performing Systematic Literature Reviews in Software Engineering.*

Maestre, J. (2015). *Domótica para Ingenieros.* Madrid: Editorial Paraninfo .

Martín, S. G., & Lafuente, V. (2017). Referencias bibliográficas: indicadores para su evaluación en trabajos científicos. *Scielo*. Obtenido de https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2017000100151

Microsoft. (2022). *Introducción a Plug and Play*. Obtenido de https://learn.microsoft.com/eses/windows-hardware/drivers/kernel/introduction-to-plug-and-play

Miranda, C. K. (2019). Estudio de Riesgos y Vulnerabilidades de la Red LAN y Equipos del Infocentro San Juan. Obtenido de http://dspace.utb.edu.ec/handle/49000/6901

Morales, J. G. (2022). Influencia del covid 19 en el incremento de los ciberataques a nivel mundial. Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/11574

Mussi, G., Barreto, L., & Cugnasca, C. E. (2016). An UPnP architecture for interoperability in Home Area Network. *IEEE International Symposium on Consumer Electronics (ISCE)*. Obtenido de https://doi.org/10.1109/ISCE.2016.7797366

Nava-Lopez, I., Prudente-Tixteco, L., Olivares-Mercado, J., Sanchez-Perez, G., ToscanoMedina, K., & Castro-Madrid, L. C. (2019). Security Tool for UPnP protocol on Smart TV. *IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC)*. Obtenido de https://doi.org/10.1109/ROPEC48299.2019.9057057

Pehkonen, V., & Koivisto, J. (2010). Secure Universal Plug and Play network. *Sixth International Conference on Information Assurance and Security*. Obtenido de https://doi.org/10.1109/ISIAS.2010.5604189

Pons Gamon, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO - Revista Latinoamericana de Estudios de Seguridad, (20), 80–93.* Obtenido de https://doi.org/10.17141/urvio.20.2017.2563

Rapid7. (2013). *Security Flaws in Universal Plug and Play: Unplug, Don't Play*. Obtenido de https://www.rapid7.com/blog/post/2013/01/29/security-flaws-in-universal-plug-and-playunplug-dont-play/

Salazar, J. D., & Novoa, N. U. (2022). Análisis y recomendaciones del estado de seguridad de una empresa de compra de cartera y riesgos de negocios. Obtenido de http://hdl.handle.net/20.500.12495/8124

Sales, T., Sales, L., Almeida, H., Perkusich, A., & Sales, M. (2013). Multilevel security in UPnP networks for pervasive environments. *IEEE Transactions on Consumer Electronics*. Obtenido de https://doi.org/10.1109/TCE.2013.6490253

Sánchez, F. A. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: Consensos y disensos. *Revista Digital De Investigación En Docencia Universitaria, 13(1), 101–122*. Obtenido de https://doi.org/10.19083/ridu.2019.644

Santos, M., Cerdeira, F., Julio, E., Dembogurski, B., Silva, G., & Silva, E. (2020). An IEEE 1451 Standard-based Plug-and-Play Architecture to Empower the Internet of Things. *IEEE Latin America Transactions*. Obtenido de https://doi.org/10.1109/TLA.2020.9400431

Zheng, H., Li, C., & Chen, Z. (2011). Petri Nets Based Modeling and Analysis of UPnP Security Ceremonies. *Third Pacific-Asia Conference on Circuits, Communications and System (PACCS)*. Obtenido de https://doi.org/10.1109/PACCS.2011.5990235