



**UNIVERSIDAD TECNOLÓGICA ISRAEL**

**MEMORIA DEL PROYECTO DE FIN DE CARRERA**

**INGENIERÍA EN SISTEMAS DE INFORMACIÓN**

**TEMA:**

**AUTOMATIZACIÓN CON SELENIUM PARA LA ACTUALIZACIÓN DE  
FIRMWARE DE SWITCHES ARUBA 1930 EN LOS ESTABLECIMIENTOS DE  
MULTINACIONAL DE COMIDA RÁPIDA.**

**AUTOR:**

**CÁCERES CASTRO PABLO DAVID**

**TUTOR:**

**Mg. HENRY RECALDE ARAUJO**

**QUITO, ECUADOR  
2024**

## UNIVERSIDAD TECNOLÓGICA ISRAEL

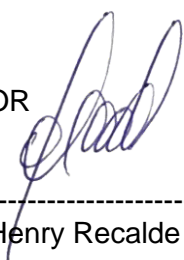
### APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación certifico:

Que el trabajo de titulación **“AUTOMATIZACIÓN CON SELENIUM PARA LA ACTUALIZACIÓN DE FIRMWARE DE SWITCHES ARUBA 1930 EN LOS ESTABLECIMIENTOS DE MULTINACIONAL DE COMIDA RÁPIDA.** presentado por Pablo David Cáceres Castro, estudiante de la Carrera Ingeniería en Sistemas de Información, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D.M., agosto 2024

TUTOR



-----  
Mg. Henry Recalde Araujo

## TABLA DE CONTENIDOS

Antecedentes de la situación objeto de estudio.....	1
Planteamiento del problema .....	1
Justificación.....	2
Objetivos .....	3
General.....	3
Objetivos específicos .....	3
Alcance.....	3
Vinculación con la sociedad y beneficiarios directos .....	4
CAPÍTULO 1. PROPUESTA.....	5
1.1    Diagramas de procesos.....	5
1.2    Recopilación de información .....	8
1.3    Factibilidad técnica.....	9
1.4    Factibilidad operacional.....	9
1.5    Factibilidad financiera económica .....	10
1.6    Modelo o estándar por aplicar para infraestructura .....	11
CAPÍTULO 2. RESULTADOS .....	14
2.1    Desarrollo.....	14
2.2    Aplicación del modelo, estándar o metodología .....	16
2.3    Resultados.....	17
2.4    Pruebas .....	18
2.5    Implementación.....	31
2.6    Requerimientos de hardware y software.....	31
CONCLUSIONES.....	33

RECOMENDACIONES.....	34
REFERENCIAS BIBLIOGRÁFICAS .....	35
ANEXOS .....	37

## LISTA DE FIGURAS

<i>Figura 1 Proceso actual, no automatizado .....</i>	<i>6</i>
<i>Figura 2 Diagrama del proceso para la autorización de ejecución. ....</i>	<i>7</i>
<i>Figura 3 Diagrama del proceso de automatización.....</i>	<i>7</i>
<i>Figura 4 Gráfico de encuesta #1.....</i>	<i>8</i>
<i>Figura 5 Gráfico de encuesta #2.....</i>	<i>8</i>
<i>Figura 6 Gráfico de encuesta #3.....</i>	<i>9</i>
<i>Figura 7 Modelo PPDIOO.....</i>	<i>12</i>
<i>Figura 8 Modelo OSI.....</i>	<i>13</i>
<i>Figura 9 Diagrama de red promedio locales KFC.....</i>	<i>14</i>
<i>Figura 10 Cálculo de tiempo de transferencia. ....</i>	<i>15</i>
<i>Figura 11 Código en Jupyter Notebook. – Introducción.....</i>	<i>16</i>
<i>Figura 12 Código en Jupyter Notebook – Vista inicial .....</i>	<i>18</i>
<i>Figura 13 Código en Jupyter Notebook – Dependencias .....</i>	<i>18</i>
<i>Figura 14 Script para encriptar la clave de switch .....</i>	<i>19</i>
<i>Figura 15 Archivos para encriptar contraseña .....</i>	<i>19</i>
<i>Figura 16 Script para desencriptar la clave de switch.....</i>	<i>20</i>
<i>Figura 17 Script para cargar el firmware en switch Aruba .....</i>	<i>21</i>
<i>Figura 18 Servidor TFTP .....</i>	<i>23</i>
<i>Figura 19 Resultado del Script de carga Firmware.....</i>	<i>24</i>
<i>Figura 20 Correo de notificación carga de IOS.....</i>	<i>25</i>
<i>Figura 21 Filtrar los switches que tienen el estado 'OK' .....</i>	<i>25</i>
<i>Figura 22 Script para reiniciar los switches Aruba 1930.....</i>	<i>26</i>
<i>Figura 23 Resultados de Script en pantalla .....</i>	<i>28</i>
<i>Figura 24 Pantalla de espera reinicio .....</i>	<i>29</i>
<i>Figura 25 Pantalla instalar actualización firmware.....</i>	<i>29</i>
<i>Figura 26 Correo de notificación reinicio de switches Aruba 1930 .....</i>	<i>30</i>

## LISTA DE TABLAS

<i>Tabla 1 Comparativa de plataformas con capacidad de automatización...</i>	<i>9</i>
<i>Tabla 2 Análisis de equipos en red.....</i>	<i>10</i>
<i>Tabla 3 Análisis de costos de licenciamiento con otras soluciones. ....</i>	<i>10</i>
<i>Tabla 4 Tiempos ejecución Scripts.....</i>	<i>30</i>
<i>Tabla 5 Inventario Switches Aruba 1930 KFC Ecuador.....</i>	<i>39</i>

# **INTRODUCCIÓN**

## **Antecedentes de la situación objeto de estudio**

Con el crecimiento en tamaño y complejidad de la infraestructura y las redes, la gestión manual de la seguridad y el cumplimiento se vuelve cada vez más desafiante. En este entorno complejo, las operaciones manuales ralentizan la detección y resolución de problemas, aumentan los errores en la configuración de recursos y crean inconsistencias en la aplicación de políticas. Como resultado, los sistemas quedan vulnerables a problemas de cumplimiento y ataques, lo que puede llevar a tiempos de inactividad inesperados y costosos, así como a una disminución general en el rendimiento.. (“¿Qué es la automatización de la seguridad? - Red Hat”)

La protección de la red integra un conjunto de políticas, procedimientos, prácticas, herramientas y conocimientos especializados destinados a salvaguardar las redes de TI. Esto asegura la defensa de todos los elementos dentro de la red, como servidores, aplicaciones y datos, frente a diversas ciberamenazas.

Para las empresas de consumo alimenticio masivo, la seguridad informática es un punto importante en la continuidad en el negocio, el mantener actualizados a las últimas versiones estables sus dispositivos informáticos y de red, puede ser un determinante que evite brechas de seguridad que podrían afectar el correcto funcionamiento o inclusive causar una para total de las funciones críticas en uno o varios locales, lo que afectarían las ventas como la buena imagen de la empresa.

## **Planteamiento del problema**

Para la multinacional de comida rápida KFC considerando la sede ubicada en el Ecuador, la gestión de actualizaciones de firmware de equipos de red marca Aruba actualmente se realizan por parte del área de Infraestructura IT, la misma que por el momento cuenta con 1 delegado de Networking para cubrir la demanda de actualización de los 157 locales, lo que ha causado una demora en la realización de estos parches de seguridad necesarios para poder mantener actualizada la infraestructura y libre de vulnerabilidades.

Actualmente cuando se identifica una posible brecha de seguridad ““Common Vulnerabilities and Exposures” (CVE) que son una lista de vulnerabilidades y exposiciones de seguridad de la información divulgadas públicamente,” (Red Hat, 2021), la multinacional de comida rápida mediante el servicio contratado de un CSOC con un proveedor ISP local, de primera mano informa de las vulnerabilidades en fabricantes como por ejemplo Aruba, permitiendo que se pueden tomar acciones inmediatas. Una vez validado el alcance de la vulnerabilidad en base al CVE se procede con un parchado manual de firmware de cada equipo switches Aruba de los locales de la multinacional, trabajo realizado por un recurso humano asignado en el área de Networking.

Al disponer de los modelos de switches Aruba 1930 los cuales únicamente tienen administración Web y carecen de gestión CLI por SSH, Telnet o de opciones de actualización de firmware con un sólo clic, ha surgido la necesidad de disponer de una solución o automatización que permita reducir los tiempos operativos de actualización de firmware manuales al mínimo.

### **Justificación**

Mediante la automatización del proceso de actualización del firmware en los switches de la marca Aruba, modelo 1930, instalados en los locales de una reconocida multinacional de comida rápida en Ecuador, mediante el uso de la herramienta Selenium y Python. Se busca mejorar la eficiencia y precisión de este procedimiento crítico, garantizando un entorno de red seguro y actualizado para optimizar el rendimiento de las operaciones en los establecimientos de comida rápida.

Esta automatización permitirá gestionar de manera centralizada y controlada las actualizaciones de firmware en los switches, eliminando posibles errores humanos y reduciendo el tiempo necesario para llevar a cabo estas tareas de mantenimiento. La implementación de la automatización con Selenium garantizará una interacción efectiva con la interfaz web de los switches Aruba 1930, facilitando la ejecución de comandos y la supervisión del proceso de actualización. La iniciativa no solo simplificará el proceso de gestión de actualizaciones, sino que también contribuirá a la seguridad de la red, asegurando que todos los switches operen con la versión más reciente del firmware, lo que a su vez fortalece la protección contra posibles vulnerabilidades de seguridad.



## **Objetivos**

### **General**

Diseñar un proceso de automatización con Selenium para la actualización de firmware en Switches Aruba 1930 en los establecimientos de multinacional de comida rápida con el fin de que se reduzca la brecha de seguridad debido a la falta de actualización en el firmware de los equipos de red.

### **Objetivos específicos**

- Analizar el estado situacional actual de la multinacional de comida rápida con respecto a la gestión de actualizaciones de firmware de los equipos de red marca Aruba modelo 1930.
- Diseñar el prototipo de la automatización de actualizaciones de firmware para los equipos switches Aruba modelo 1930.
- Implementar un escenario de pruebas controlado para el despliegue del diseño de automatización elaborado.
- Evaluar el comportamiento de la automatización mediante pruebas de actualizaciones de firmware controladas.

### **Alcance**

Para la elaboración de la automatización se plantearon los siguientes puntos a desarrollar:

- Levantamiento inventario switches: Levantamiento del inventario de los switches de la reconocida marca de comida rápida en el Ecuador para el dimensionamiento y análisis de únicamente los modelos Aruba 1930.
- Esquema de red actual: Levantamiento de diagrama general de conexión de red y diagrama de red de un local demo en Ecuador, para visualización del escenario general actual de red.

- Revisión de AB: AB (Ancho de Banda) del enlace de datos general que disponen los locales de la reconocida marca de comida rápida, tomando 2 locales de ejemplo, para validación del medio guiado por el cual se transferirán las actualizaciones con la automatización.
- Desarrollo del proceso: Elaboración del proceso con Selenium y Python para el análisis y despliegue necesario para las actualizaciones de firmware.
- Generación de Reporte de automatización: El proceso contará con:  
Un reporte de la gestión del despliegue realizado. el mismo que informará si la tarea fue realizada con éxito o si existe algún error, este reporte incluirá la IP del equipo de red validado y el estado de la automatización, indicando “ok” o “error en actualización” de tal manera que se pueda tener un control y revisión.

### **Vinculación con la sociedad y beneficiarios directos**

La meta del ODS 9 es desarrollar infraestructuras que sean sostenibles, resilientes y de alta calidad para toda la población, al mismo tiempo que se promueve una industria moderna que adopte tecnologías y procesos respetuosos con el medio ambiente. También se enfatiza la importancia de fomentar la tecnología, la innovación y la investigación, asegurando que todos tengan acceso equitativo a la información y el conocimiento, especialmente a través de internet (Pactomundial.org, s.f.).

El beneficio directo que se obtendrá con la automatización planteada será para los equipos de red de marca Aruba de la marca reconocida de comida rápida en el Ecuador, el beneficio indirecto se da debido a que con el mismo principio se puede automatizar para las otras marcas que disponen de switches de Core, acceso o distribución para las otras marcas del Grupo.

## **CAPÍTULO 1. PROPUESTA**

### **1.1 Diagramas de procesos**

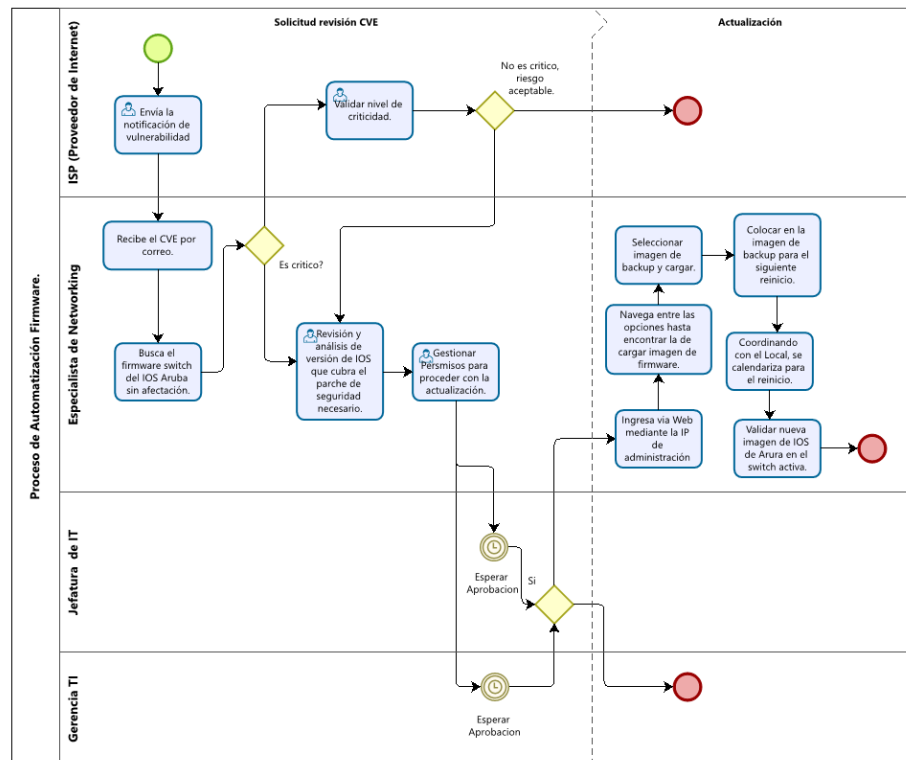
En la actualidad el proceso que se genera es manual en donde se recibe la notificación del CVE y se procede con la validación uno a uno de los switches que deben ser actualizados, para lo que:

Se ingresa 1 a 1 mediante acceso web con un usuario y contraseña en los switches Aruba de KFC, se navega por los menús hasta la opción de actualización en donde se selecciona la opción para cargar la imagen IOS sin vulnerabilidad en la ubicación correspondiente.

Una vez cargada la imagen del IOS se selecciona la opción de carga de nueva versión de imagen en el siguiente reinicio del equipo.

Se planifica el reinicio del equipo con una ventana de mantenimiento fuera de horario de alta demanda, para poder ejecutar el reinicio remoto del switch sin afectar el funcionamiento y las ventas en el local. Las ventanas de mantenimiento están habilitadas en el rango de tiempo de 2 am a 7 am en GMT -5

**Figura 1**  
Proceso actual, no automatizado



Nota: Propio del autor.

Se propone la automatización del proceso mediante el desarrollo de una automatización que permita eliminar la interacción humana en el proceso, para lo que se plantea es:

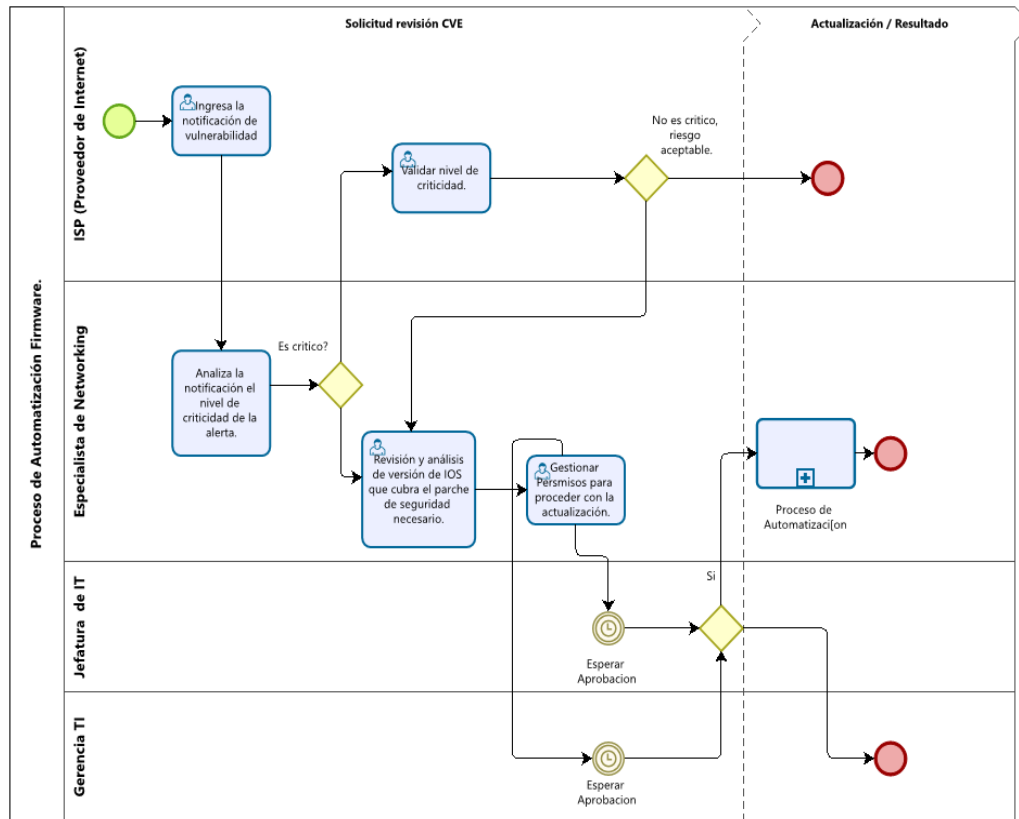
Levantamiento del listado de Switch que dispone del IOS con vulnerabilidad a ser actualizado.

Generación de la automatización mediante el uso de Selenium, donde se va a especificar qué movimientos y acciones se requieren.

La navegación con la automatización debe ser controlada con espacios de tiempo, en caso de que exista retardos en la comunicación, considerando que la conexión se realiza mediante MPLS hacia los diferentes locales alrededor del país.

**Figura 2**

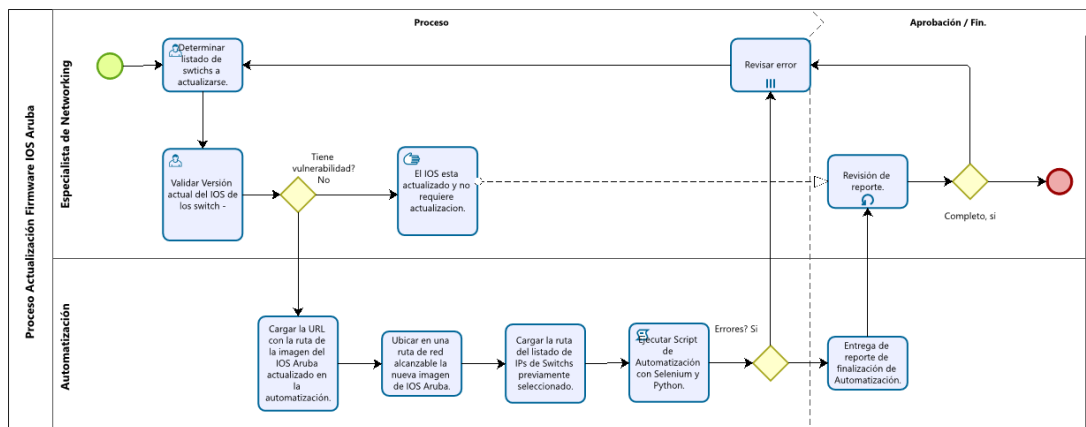
Diagrama del proceso para la autorización de ejecución.



*Nota.* La figura representa la interacción previa a la ejecución de la automatización. Propio del autor

**Figura 3**

Diagrama del proceso de automatización



*Nota.* La figura representa el proceso de la automatización en el entorno de red empresarial. Propio del autor

## 1.2 Recopilación de información

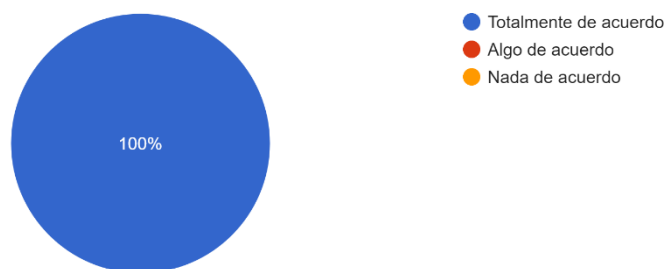
Para el presente caso práctico se utilizará el método de encuesta no probabilística, en donde se toma en cuenta la necesidad de la automatización expuesto a la Gerencia y Jefatura de Infraestructura para la viabilidad del proyecto, utilizando la técnica de encuesta mediante 3 preguntas referentes a la necesidad de automatización de actualizaciones de firmware identificado, de igual manera se utilizará el muestreo experimental de los equipos de red seleccionados.

**Figura 4**

*Gráfico de encuesta #1.*

¿Esta de acuerdo en utilizar una solución de automatización para actualizar el IOS de los Switchs Aruba de la marca KFC en EC?

2 respuestas



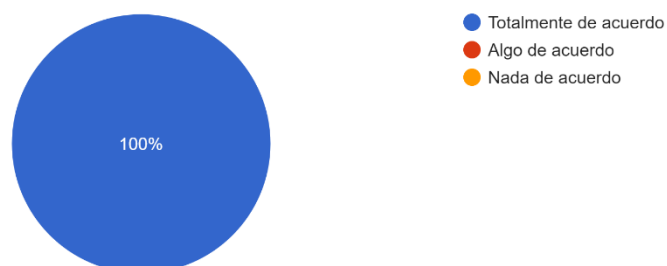
*Nota:* Representa el porcentaje de aceptación.

**Figura 5**

*Gráfico de encuesta #2.*

¿Esta de acuerdo en que se implemente una solución de automatización de upgrade de IOS para Switchs Aruba con costo cero?

2 respuestas

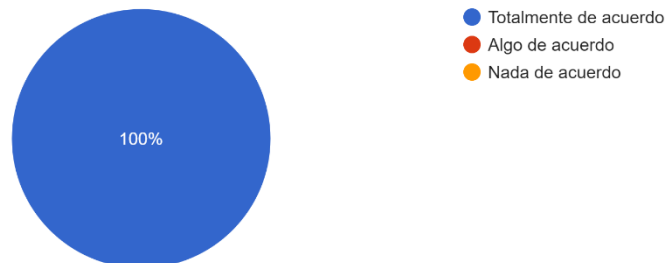


*Nota:* Representa el porcentaje de aceptación.

**Figura 6***Gráfico de encuesta #3.*

¿Está de acuerdo en que se corrija vulnerabilidades de ciberseguridad con actualización de IOS de networking en los switchs Aruba de los locales de KFC EC?

2 respuestas



*Nota:* Representa el porcentaje de aceptación.

### 1.3 Factibilidad técnica

A continuación, se muestra una tabla comparativa de los recursos evaluados.

**Tabla 1**

*Comparativa de plataformas con capacidad de automatización.*

Sistema	Tipo	Características – Requerimientos
Ansible	Pago	Requiere de SSH habilitado
Selenium	free / open-source	Es amigable y nativo para WEB.
Aruba Manager	Pago	Requiere de licenciamiento por equipo.
Manage Engine	Pago	Requiere de licenciamiento.

*Nota:* Tabla comparativa de características soluciones de automatización. Propio del autor.

### 1.4 Factibilidad operacional

Para el presente proyecto la investigación experimental permitió determinar la cantidad de equipos de red que serán intervenidos a base de muestreo de los equipos de red en los locales de la reconocida marca de comida rápida que disponen de los switches marca Aruba y modelo 1930 en Ecuador, los datos obtenidos se observan en la tabla:

**Tabla 2***Análisis de equipos en red.*

MODELOS	CANTIDAD	PORCENTAJE
Aruba 1930	59	37.58%
Switch no administrables	3	1.91%
Switch otro modelo	95	60.51%
<b>TOTAL</b>	<b>157</b>	<b>100.00%</b>

*Nota:* Tabla de cantidades de equipos de red en los locales KFC en Ecuador. Propio del autor.

El universo seleccionado de los locales de la reconocida marca de comida rápida consta de 157 locales distribuidos alrededor del Ecuador, en los cuales se ha considerado como objeto de muestra 59 que disponen de un switch Aruba modelo 1930 y los otros 2 muestreos cuantitativos correspondientes a los switches no administrables y a los que disponen de otro tipo de marca y modelo, los mismos que a futuro se migrarán a la marca Aruba.

### 1.5 Factibilidad financiera económica

**Tabla 3***Análisis de costos de licenciamiento con otras soluciones.*

Sistema	Tipo	Características – Requerimientos	Costo aproximado
Ansible	Pago	Requiere de SSH habilitado	\$14000 /Anuales
Selenium	free / open-source	Es amigable y nativo para WEB.	\$ 0.00
Aruba Central	Pago	Licenciamiento por equipo.	\$100000 /Anuales
Manage Engine	Pago	Requiere de licenciamiento.	\$120000 /Anuales

*Nota:* Desarrollo del autor, obtenido de internet. *Ansible pricing 2024(s/f)*, *Selenium (Open Source)(s/f)*, *Aruba Central Subscription (S/f)*, *ManageEngine Network Configuration Management (NCM) pricing 2024*.

En base al cuadro anterior considerando que la inversión en licenciamiento sería \$0,00 se optó por Selenium como solución para ser implementado.



## 1.6 Modelo o estándar por aplicar para infraestructura

La metodología por utilizar en el presente proyecto es el Ciclo de Vida que propone Cisco, llamado PPDIOO; es uno de los más completos que parten desde la planificación de un proyecto y diseñando un esquema de optimizaciones para volver a comenzar el ciclo. Las siglas de PPDIOO hace referencia a las fases de Preparación, Planificación, Diseño, Implementación, Operación y Optimización. Cada fase tiene un papel fundamental y se encuentra estrictamente relacionada con su antecesora y predecesora, no se puede saltar ninguna fase si se desea un proyecto satisfactorio.

PPDIOO sus fases son:

**Preparar:** Consiste en establecer los requerimientos organizacionales, elaborar una estrategia de red, y diseñar una arquitectura de alto nivel que permita establecer las tecnologías más adecuadas para respaldar dicha arquitectura. Durante esta fase, también se puede justificar financieramente la estrategia de red al analizar el asunto de negocio para la arquitectura ofertada.

**Planificar:** Consiste en definir los requisitos iniciales de la red teniendo en cuenta objetivos, instalaciones y necesidades de los usuarios, entre otros factores. Durante la fase de planificación, se realiza una caracterización de los sitios y una evaluación de la red existente, además de un análisis de seguridades para verificar si la infraestructura actual, sitios y la operación pueden soportar la solución propuesta. Un plan de proyecto es esencial para organizar tareas, compromisos, hitos que pueden llegar a ser críticos al igual que los recursos necesarios para desplegar los cambios en la red. Esta solución debe estar encaminada con los lineamientos de alcance, costo y recursos definidos en los requisitos de negocio originales.

**Diseñar:** Los requisitos preliminares establecidos durante la fase de planificación orientan el trabajo de los expertos en diseño de redes. La especificación del diseño de la red es un esquema detallado y exhaustivo que satisface tanto las necesidades empresariales como técnicas actuales, e integra especificaciones que garanticen la disponibilidad, confiabilidad, seguridad, escalabilidad y rendimiento. Esta especificación constituye el fundamento sobre el cual se basan las actividades de implementación.

**Implementar:** La red se construye o se añaden componentes adicionales siguiendo las especificaciones del diseño, con el propósito de integrar los dispositivos sin causar interrupciones en la red actual ni generar puntos de vulnerabilidad.

**Operar:** La fase operativa sirve como la prueba final para verificar la adecuación del diseño. En esta etapa, se busca mantener la salud de la red mediante la gestión de operaciones diarias, asegurando una alta disponibilidad y controlando los costos. La identificación y corrección de fallos, así como el monitoreo del rendimiento durante estas operaciones, generan los datos necesarios para la fase de optimización.

**Optimizar:** Involucra la gestión proactiva de la red, cuyo propósito es identificar y resolver problemas antes de que afecten a la organización. Cuando la gestión proactiva no logra prever y mitigar fallos, es necesario abordar la detección y corrección de errores de manera reactiva. En PPDIOO, la fase de optimización puede conllevar un rediseño de la red si surgen varios inconvenientes o errores, si el rendimiento no proporciona las expectativas o si se presentan nuevas aplicaciones para cubrir los requerimientos de la organización. (Richard Froom et al., 2010)

**Figura 7**  
*Modelo PPDIOO*

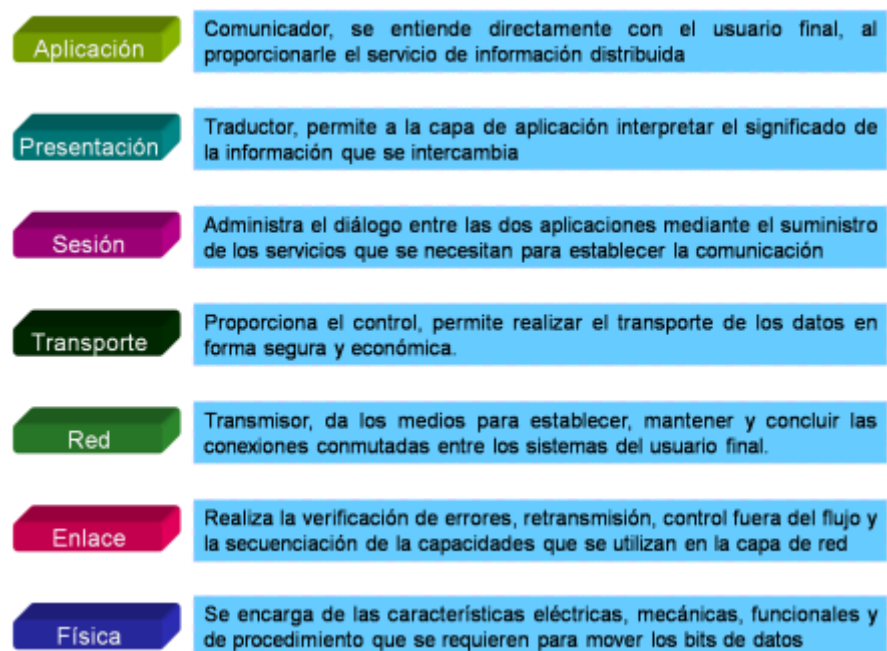


*Nota: Detalle el ciclo de vida del Modelo PPDIOO. (Pozo, 2017, pág. 23)*

Según Pozo (2017), el propósito central es optimizar costos en la infraestructura de red mediante la definición clara de los requisitos para la implementación de nuevas tecnologías y un enfoque adaptable en el ciclo de vida.

Desde el punto de vista de la administración de redes, el modelo OSI es el que prevalece y es referente de los diseños a nivel mundial, por lo tanto, se tomará como eje central del proyecto. En donde se va a utilizar las 7 capas del modelo.

**Figura 8**  
*Modelo OSI.*



*Nota:* Detalle de cada una de las 7 capas del modelo OSI.

## CAPÍTULO 2. RESULTADOS

### 2.1 Desarrollo

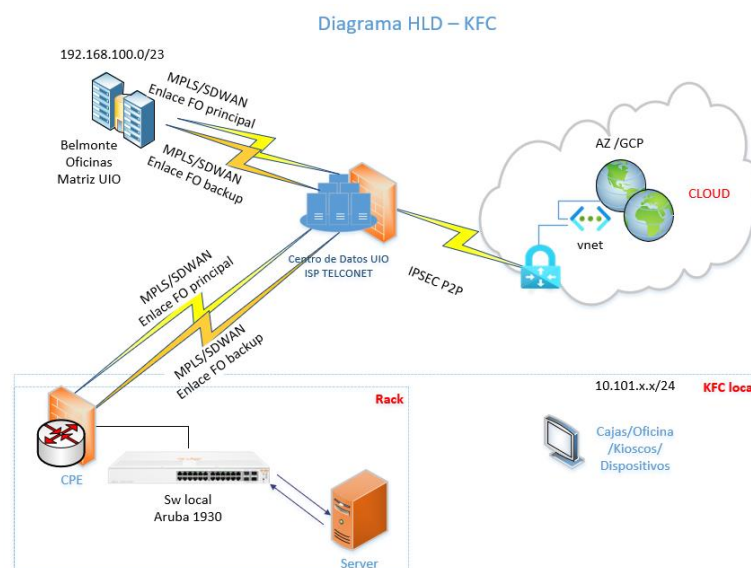
Para el desarrollo del presente componente práctico se ha considerado la necesidad de tener un proceso automatizado que permita el realizar la actualización del firmware de los switches de marca Aruba con el propósito de reducir las brechas de seguridad y los tiempos actuales al tratarse de un proceso manual.

Con el objetivo de tener acceso a todos los dispositivos de red switches Aruba 1930 del grupo, procedemos a realizar una revisión de la infraestructura de red y conexión, para determinar la mejor ubicación para el despliegue de la automatización.

Como factor importante para la automatización la cadena KFC en Ecuador utiliza MPLS Datos con el ISP Telconet para la interconexión de sedes, Data Center y con los diferentes locales de KFC en Ecuador.

A continuación, se visualiza en la siguiente figura el esquema actual de conexión de red de ejemplo de un local promedio.

**Figura 9**  
*Diagrama de red promedio locales KFC.*



*Nota. El diagrama presenta una vista en HLD (High Level Diagram) Diagrama de Alto Nivel.*

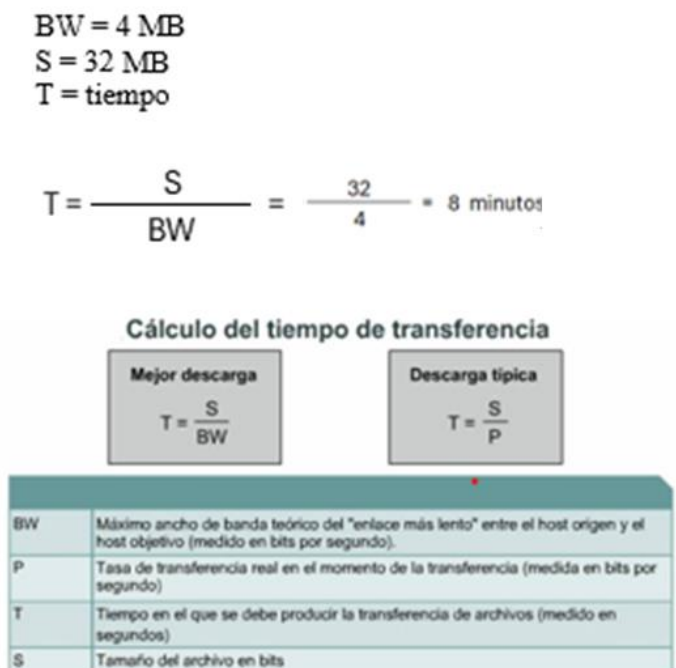
Una vez establecido que existe comunicación entre la sede principal, ubicación en donde se propone desplegar la automatización, y los locales se realiza la revisión de los requerimientos para poder realizar la automatización.

El AB (Ancho de banda) proporcionado por el proveedor Telconet con el que cuentan los locales es de 4 MB de datos tanto de carga como descarga. Un archivo de configuración del IOS de los switches Aruba 1930 tiene un peso aproximado de 32 MB, dato que se requiere para poder calcular el tiempo del envío del firmware a través de la red hacia el switch final.

El cálculo utilizado para determinar el tiempo que tardará en llegar el IOS hacia el switch en el local es el siguiente:

**Figura 10**

*Cálculo de tiempo de transferencia.*



*Nota:* Fórmula para calcular la descargada y ejemplo. (LLagua, 2012)

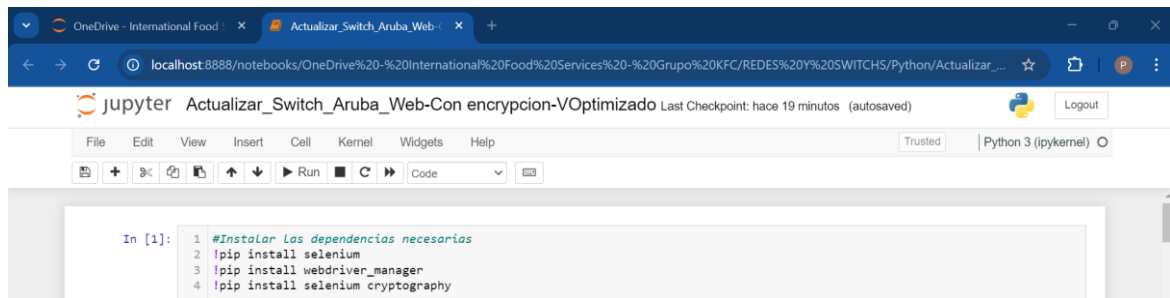
Con el cálculo previamente realizado, se debe considerar 8 minutos aproximadamente de transferencia de la imagen del IOS al switch, a través del enlace de datos existente entre las oficinas matriz y el switch en el local.

La automatización debe ser ejecutada desde un dispositivo o servidor que tenga interconexión y disponga de alcance a todas las redes de los locales, para lo que necesitará disponer de Python y Selenium para su correcto funcionamiento.

Para motivos de este componente práctico se elaborará la automatización en Jupyter de Notebook, siendo el código es el siguiente:

**Figura 11**

*Código en Jupyter Notebook - Introducción.*



*Nota:* Plataforma instalada en el cliente con Core Kernel Python para funcionamiento.

## 2.2 Aplicación del modelo, estándar o metodología

Se utilizará la metodología de Cisco con 6 fases cíclicas, las cuales se detallan:

En la fase de Preparación se va a determinar lo necesario para cubrir los objetivos de la actualización del firmware para los switches Aruba 1930 la cadena de comida rápida, la manera como se plantea la comunicación entre el equipo que ejecute la automatización y el switch en los locales. Toda la información se va a obtener mediante las entrevistas a la Jefatura y Gerencia de Infraestructura IT.

La segunda fase es la Planificación y se va a analizar la situación actual de la red. El análisis se realizará de la arquitectura, dispositivos switches Aruba 1930 de las sucursales, al igual del conocimiento técnico del personal encargado de redes.

La tercera fase es el Diseño y se hará en base a lo obtenido en las anteriores fases. Los diagramas y equipos por usar van a ser plasmados en este documento en los siguientes ítems.

La cuarta fase es la Implementación donde se va a plasmar el diseño de la automatización en unos equipos de prueba para validar que todo está funcionando correctamente.

La quinta fase es la Operación, en este punto se va depurando las líneas de conexión, ajustando los tiempos de respuesta en la automatización, y demás configuraciones. Se realizará un monitoreo del comportamiento de la red y posibles correcciones que puedan surgir.

La sexta y última fase es la Optimización, donde en base al reporte de ejecución identificamos problemas y sus posibles causas y poderlas corregir antes de que vuelvan a suceder. En esta fase también se van a proponer modificaciones en el diseño para mejorar el desempeño de la automatización de ser necesarias.

### **2.3 Resultados**

Se desarrolló un estándar de pasos a seguir ordenados a ser utilizados en la automatización de Python, el mismo que podrá ser utilizado por otras marcas que utilicen el mismo modelo de equipo de red Switch Aruba 1930.

Con las entrevistas y revisiones en conjunto con el personal de Networking, Jefatura y Gerencia de Infraestructura se pudo analizar el estado en la que se encuentra la actualización de firmware de los switches Aruba 1930 y se determina que es necesario realizar una actualización urgente para cubrir las posibles brechas de seguridad.

Se establecen las ubicaciones de las rutas de la automatización, IOS Firmware y archivos que se generarán para que sean alcanzables desde los equipos switches en red de la cadena de comida rápida.

Se coordinaron las pruebas controladas de actualización con switches Aruba 1930 en escenarios de prueba ubicados en los locales de la cadena de comida rápida.

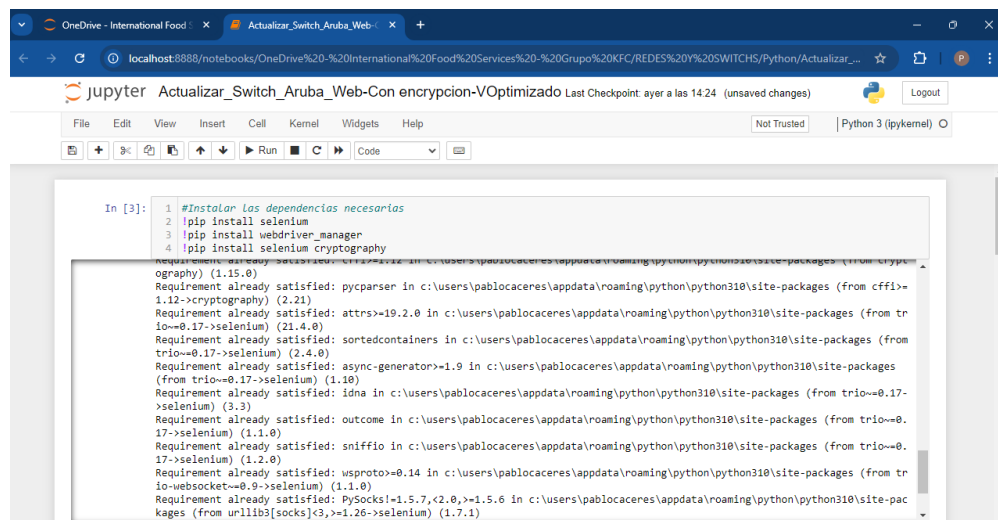
Se verificó el funcionamiento de la automatización con las pruebas, correos de notificaciones y validaciones con los informes realizados con la funcionalidad “pandas” de Python.

## 2.4 Pruebas

Se valida la automatización con la herramienta Jupyter Notebook desde donde se ejecuta los scripts de automatización.

**Figura 12**

*Código en Jupyter Notebook – Vista inicial*



*Nota:* La figura representa el panel del aplicativo Jupyter Notebook.

**Figura 13**

*Código en Jupyter Notebook - Dependencias*

```
In [ ]: 1 #Instalar las dependencias necesarias
        2 !pip install selenium
        3 !pip install webdriver_manager
        4 !pip install selenium cryptography
```

*Nota:* La figura representa a las dependencias necesarias para el correcto funcionamiento.



Se revisa y valida las dependencias / aplicaciones necesarias para el funcionamiento de la automatización.

Para la conexión segura se genera la encriptación de la clave de acceso a los switch Aruba 1930 mediante el uso de la dependencia “fernet”, la que permite generar y manejar encriptación simétrica con la capa de seguridad AES / SHA 256 con 128-bit de clave. (Contributors, 2013-2024)

**Figura 14**

*Script para encriptar la clave de switch*

```
In [3]: 1 #Script para encriptar la clave de switch - Seguridad
2 from cryptography.fernet import Fernet
3
4 # Generar y guardar una clave
5 key = Fernet.generate_key()
6 with open(r'D:\python\switchslave.key', 'wb') as key_file:
7     key_file.write(key)
8
9 # Encriptar un mensaje
10 fernet = Fernet(key)
11 #clave_encriptada = fernet.encrypt(b'SLapeoar!9907')
12 clave_encriptada = fernet.encrypt(B'%env CLAVE_ADMIN')
13
14 # Guardar el mensaje encriptado en un archivo
15 with open(r'D:\python\clave_encriptada.txt', 'wb') as enc_file:
16     enc_file.write(clave_encriptada)
17
18 #Clave encriptada exitosamente
19 print("Mensaje encriptado correctamente")
20 print("Clave encriptada:", clave_encriptada)
21
```

Mensaje encriptado correctamente  
Clave encriptada: b'gAAAAABmtGf9V0FVj3nZ9yCvbb7aGn3Ntloxpb1YHjBebZG4PKkDYplttLD2lHnPQ4hEgHU0J9mjTf7YI16n7IA86-0EgnOfid-Wtmy3oh5YNlwU-AqiSIis='

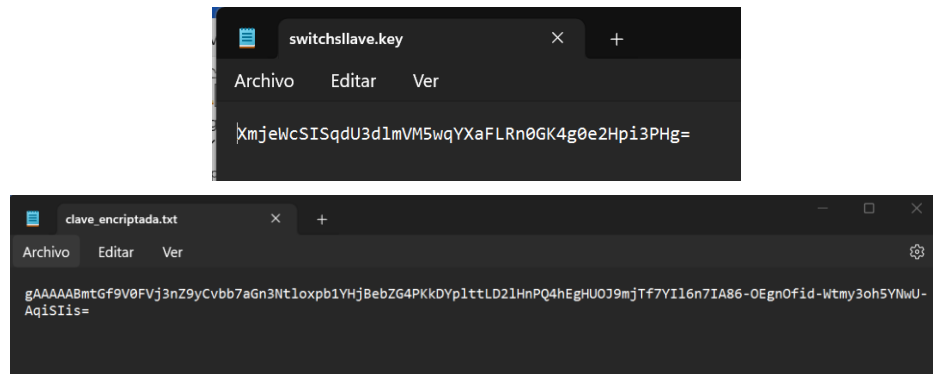
**Nota:** La figura presenta el script para generar encriptación de la clave para el acceso a los switches Aruba 1930.

El resultado del script imprime un mensaje de encriptado correctamente y la clave completa encriptada para validar el funcionamiento, el proceso utiliza una llave que es generada y será utilizada para encriptar la contraseña.

**Figura 15**

*Archivos para encriptar contraseña*

Nombre	Fecha de modificación	Tipo	Tamaño
clave_encriptada.txt	8/8/2024 1:38	Documento de texto	1 KB
switchslave.key	8/8/2024 1:38	Entradas de registro	1 KB



*Nota:* La figura presenta los archivos generados y necesarios para encriptar la contraseña del acceso a los switches Aruba 1930

Para el siguiente paso se procede a desencriptar la clave encriptada debido a que no es posible enviar la clave encriptada en la pantalla del web login del switch Aruba 1930.

**Figura 16**

*Script para desencriptar la clave de switch*

```
In [5]: 1 #Script para desencriptar la clave de switch
2 from selenium import webdriver
3 from cryptography.fernet import Fernet, InvalidToken
4
5 # Especificar las rutas de los archivos
6 key_path = r'D:\python\switchsllave.key'
7 clave_encryptada_path = r'D:\python\clave_encryptada.txt'
8 try:
9     # Leer la clave de encriptación
10    with open(key_path, 'rb') as key_file:
11        key = key_file.read()
12
13    # Leer el mensaje encriptado
14    with open(clave_encryptada_path, 'rb') as enc_file:
15        clave_encryptada = enc_file.read()
16
17    # Desencriptar el mensaje
18    fernet = Fernet(key)
19    clave_desencriptada = fernet.decrypt(clave_encryptada).decode()
20
21    # Mensaje de confirmación si se desencripta correctamente
22    print("Clave encriptada:", clave_encryptada)
23    print("Mensaje desencriptado correctamente:", '#####')
24    #print("Su clave desencriptada es:", clave_desencriptada)
25
26 except FileNotFoundError:
27     print(f"Error: No se encontró el archivo en la ruta especificada.")
28 except InvalidToken:
29     print(f"Error: No se pudo desencriptar el mensaje. La clave de encriptación podría ser incorrecta o el mensaje está corrupto.")
30 except Exception as e:
31     print(f"Error desconocido: {str(e)}")
```

Clave encriptada: b'gAAAAABmtGf9V0FVj3nZ9yCvbb7aGn3Nt1oxpb1YHjBebZG4PKkDYp1ttLD21HnPQ4hEgHU0J9mjTf7YI16n7IA86-0EgnOfid-Wtmy3oh5YNwU-AqiSiIs='  
Mensaje desencriptado correctamente: #####

*Nota:* La figura presenta el script para desencriptar la contraseña de acceso a los switches Aruba 1930

El resultado del script imprime un mensaje de referencia con la clave encriptado y con la clave desencriptada, por seguridad oculta con “#####”, el proceso consulta la ubicación de la llave previamente generada al igual que la ubicación del mensaje encriptado, se agrega una validación en caso de que no exista los archivos necesarios para desencriptar el mensaje.

Para el proceso principal de cargar el Firmware del Switch Aruba 1930 se utiliza las dependencias de Selenium que permitirán utilizar la automatización mediante el uso del subproceso Webdriver el que navegará en el entorno web entregando el resultado esperado.

**Figura 17**

*Script para cargar el firmware en switch Aruba*

```
In [5]: 1 #Script para cargar el Firmware IOS en Swtich Aruba 1930
2 from selenium import webdriver
3 from selenium.webdriver.common.by import By
4 from selenium.webdriver.support.ui import WebDriverWait
5 from selenium.webdriver.support import expected_conditions as EC
6 from selenium.webdriver.chrome.service import Service
7 from selenium.webdriver.support.select import Select
8 import pandas as pd
9 import time
10 import smtplib
11 from email.mime.multipart import MIMEMultipart
12 from email.mime.text import MIMEText
13 from datetime import datetime
14
15 #Función para esperar hasta que el texto 'Succeeded' aparezca en pantalla
16 def esperar_texto_succeeded(element, timeout=700):
17     WebDriverWait(browser, timeout).until(
18         EC.text_to_be_present_in_element((By.ID, element), 'Succeeded')
19     )
20
21 #Arreglo de lista de switches y status
22 data = {'Switch': [], 'Status': []}
23
24 # Configuración del navegador
25 CHROMEDRIVER_PATH = "D:\\python\\chromedriver126.0.6478.exe"
26 path = Service(CHROMEDRIVER_PATH)
27 browser = webdriver.Chrome(service=path)
28
29 #Credenciales y rutas
30 username = '%env USER_SWITCH'
31 iospath = "InstantOn_1930_2.6.0.74.swi"
32 path = "D:\\python\\switchsaruba2.txt"
33
34 with open(path, "r") as file:
35     switches = [line.strip() for line in file]
36
37 try:
38     for ip in switches:
39         print(ip)
40         try:
41             # Abre cada URL por IP
42             browser.get('http://' + ip)
43             time.sleep(4)
44             # Ingresar a La administración
45             browser.find_element(By.NAME, "inputUsername").send_keys(username)
46             #print (clave_desencriptada)
47             browser.find_element(By.NAME, "inputPassword").send_keys(clave_desencriptada)
48             browser.find_element(By.CLASS_NAME, "btn").click()
49
50             # Obtener La versión de IOS Actual.
51             time.sleep(8)
52             ver_sw = browser.find_element(By.ID, "lblDeviceVersion")
53             text_ver = ver_sw.text
54             print(text_ver)
55
56             # Si La versión es estable entonces salta al siguiente.
57             if '2.6.0' in text_ver:
58                 print("Ya actualizado")
59                 data['Switch'].append(ip)
60                 data['Status'].append('YA_ACTUALIZADO')
61                 continue
62             else:
63                 print("Continúa revisión")
```

```

64
65     # Navegación para la carga del IOS.
66     WebDriverWait(browser, 5).until(EC.presence_of_element_located((By.LINK_TEXT, "Maintenance"))).click()
67     time.sleep(3)
68     WebDriverWait(browser, 5).until(EC.presence_of_element_located((By.LINK_TEXT, "Backup and Update Files"))).click()
69
70     # Seleccionando opción Update.
71     time.sleep(2)
72     WebDriverWait(browser, 5).until(EC.presence_of_element_located((By.ID, "lblrbOperationType_0"))).click()
73     browser.find_element(By.ID, "btnNext").click()
74
75     # Seleccionando opción Backup Image.
76     time.sleep(2)
77     Select(browser.find_element(By.ID, "slctFileType")).select_by_value("1")
78     browser.find_element(By.ID, "btnNext").click()
79
80     # Seleccionando opción TFTP.
81     time.sleep(2)
82     WebDriverWait(browser, 5).until(EC.presence_of_element_located((By.ID, "lblrbTransferProtocol_1"))).click()
83     browser.find_element(By.ID, "btnNext").click()
84
85     # Seleccionar ruta del IOS por TFTP.
86     time.sleep(2)
87     browser.find_element(By.ID, "txtServerAddressTFTP").send_keys("192.168.100.123")
88     browser.find_element(By.ID, "txtFileNameTFTP").send_keys(iospath)
89
90     # Carga de URL con La ruta del IOS.
91     time.sleep(2)
92     WebDriverWait(browser, 5).until(EC.presence_of_element_located((By.ID, "buttonTransferProtocolTFTP"))).click()
93
94     # Esperar hasta que el texto 'Succeeded' aparezca
95     esperar_texto_succeeded("lblStatusModal")
96     status = browser.find_element(By.ID, "lblStatusModal").text
97     print(status)
98
99     if 'Succeeded' in status:
100         # Si el estado es 'Succeeded' en pantalla, hace clic en el botón de Cancelar reinicio
101         WebDriverWait(browser, 5).until(EC.presence_of_element_located((By.ID, "modalStatusButtonOk"))).click()
102         data['Switch'].append(ip)
103         data['Status'].append('OK')
104     else:
105         data['Switch'].append(ip)
106         data['Status'].append('CONFIGURACION_FALLIDA')
107
108     except Exception as e:
109         print(e)
110         data['Switch'].append(ip)
111         data['Status'].append('CONEXION_FALLIDA')
112
113 finally:
114     file.close()
115     browser.quit() # Las instancias de WebDriver se cierran
116
117 #Visualización Reporte de Status en Data Frame
118 report = pd.DataFrame(data)
119 print (report)
120
121 # Envío de correo Reporte de Carga de Firmware
122 # Configuración del servidor SMTP y credenciales
123 smtp_server = 'smtp.gmail.com'
124 smtp_port = 587
125 usuario_correo = %env CORREO_GMAIL
126 clave_correo = %env CLAVE_GMAIL
127
128 # Configuración del correo
129 de_direccion = %env CORREO_GMAIL
130 a_direccion = 'pablo.caceres@kfc.com.ec'
131
132 # Obtener La fecha y hora actual
133 now = datetime.now()
134 fecha_formato = now.strftime("%Y-%m-%d %H:%M:%S")
135
136 # Asunto del correo con fecha y hora
137 subject = f'Automatización Carga de Firmware Finalizado - {fecha_formato}'
138 body = f"\nReporte de Automatización de Carga de Firmware Aruba 1930 GRUPOKFC\n\n {report.to_string()}\n\nRealizado por Pablo"
139
140 # Crear el mensaje MIME *Extensión multiproposito de correo electronico
141 msg = MIMEText(body, 'plain')
142 msg['From'] = de_direccion
143 msg['To'] = a_direccion
144 msg['Subject'] = subject
145 msg.attach(MIMEText(body, 'plain'))

```

```

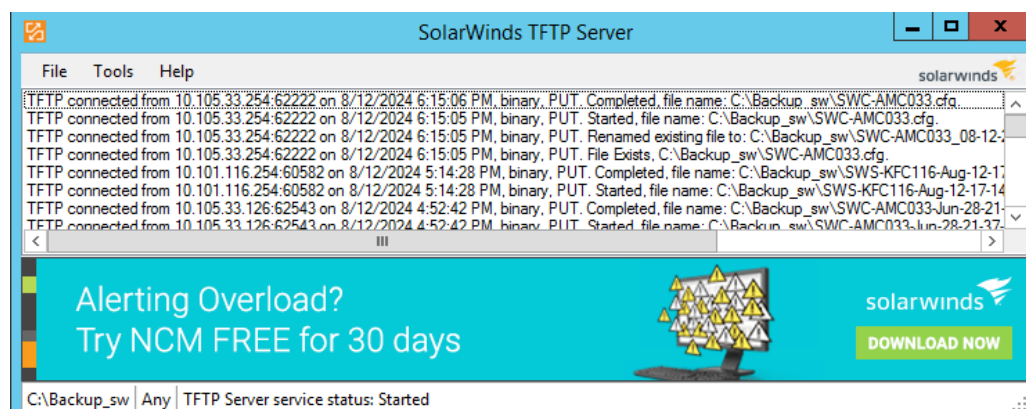
146
147 # Validacion y envio el correo
148 try:
149     server = smtplib.SMTP(smtp_server, smtp_port)
150     server.starttls()
151     server.login(usuario_correo, clave_correo)
152     text = msg.as_string()
153     server.sendmail(de_direccion, a_direccion, text)
154     server.quit()
155     print("Correo enviado exitosamente.")
156 except Exception as e:
157     print(f"Error al enviar el correo: {e}")
158
159 #Fin de La automatizacion
160 print("\n\n#####")
161 print("#")
162 print("# FINALIZADO")
163 print("#")
164 print("#####")
165

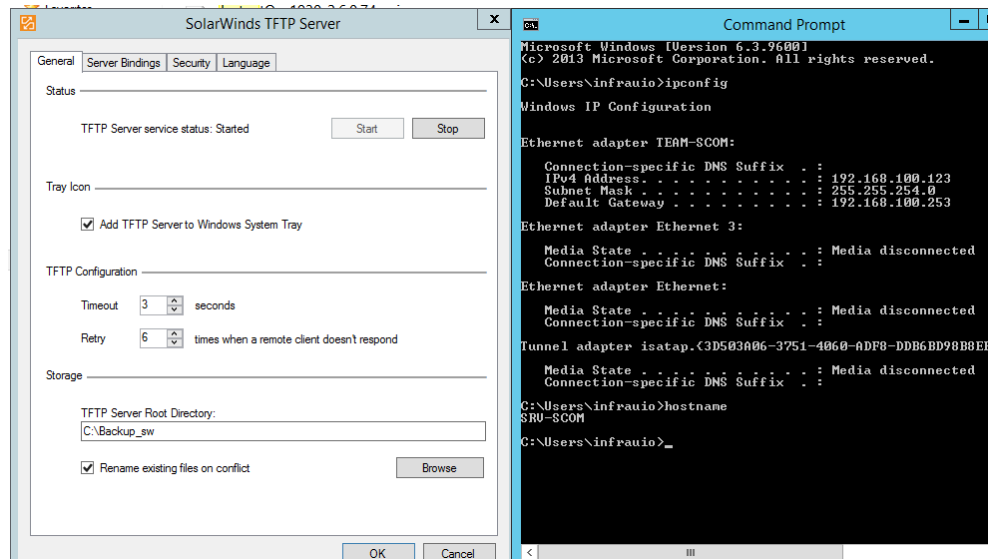
```

*Nota:* La figura presenta el script para cargar la imagen IOS del firmware del switch Aruba 1930.

El script levanta una conexión de un navegador de Chrome con el uso de Webdriver de Selenium para controlar y realizar automatizaciones como el acceso a ID o acciones como clickear en botones. En el script identificamos la necesidad de utilizar un servidor de tipo TFTP para poder cargar la imagen IOS con la versión 2.6.0, el mismo que es instalado y configurado en un servidor de la red interna de la empresa con el fin de poder tener acceso a todos los equipos de red mediante el enlace de datos/sdwan disponible en la empresa.

**Figura 18**  
*Servidor TFTP*





*Nota:* La figura presenta el servidor TFTP implementado con el programa SolarWinds (Solarwinds Worldwide, 2024) en el servidor 192.168.100.123 ubicado en el Data Center de UIO.

Una vez cargada la imagen del IOS en el switch procede a terminar la automatización, con la respectiva validación de: si no responde la IP del switch almacena en un array el mensaje de “CONECCION\_FALLIDA”, en caso de avanzar en la configuración, pero por algún motivo perder conexión el mensaje de “CONFIGURACION\_FALLIDA” y en caso de terminar con éxito “OK”. Genera un reporte corto con pandas y lo envía por correo al administrador.

**Figura 19**  
*Resultado del Script de carga Firmware*

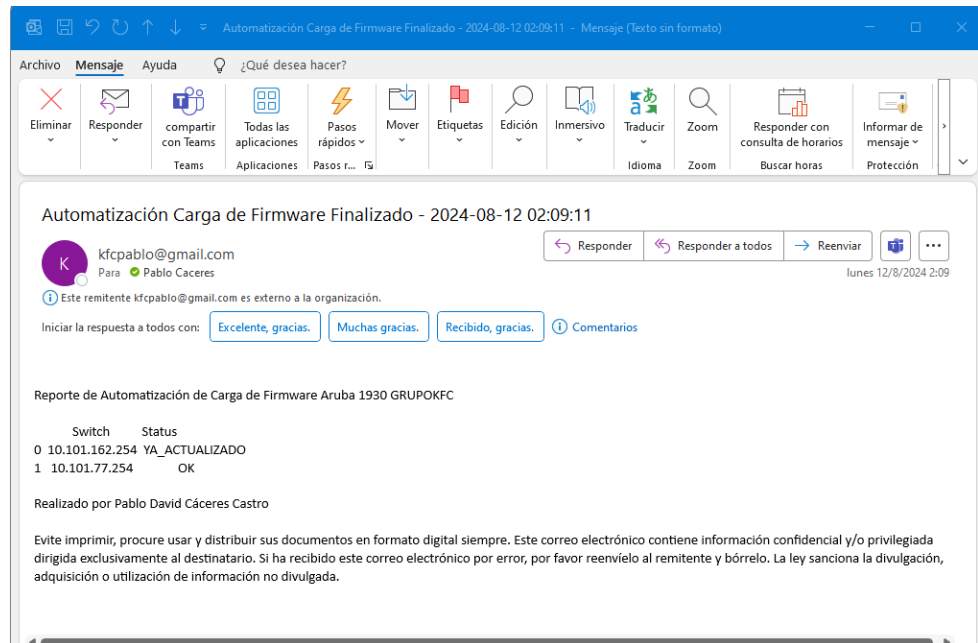
```
10.101.162.254
2.6.0
Ya actualizado
10.101.77.254

continúa revisión
Operation Succeeded
      Switch      Status
0 10.101.162.254  YA_ACTUALIZADO
1 10.101.77.254   OK
Correo enviado exitosamente.

#####
#                               #
#           FINALIZADO         #
#                               #
#####
```

*Nota:* La figura presenta los mensajes de control que se han implementado en el script de carga de IOS Firmware.

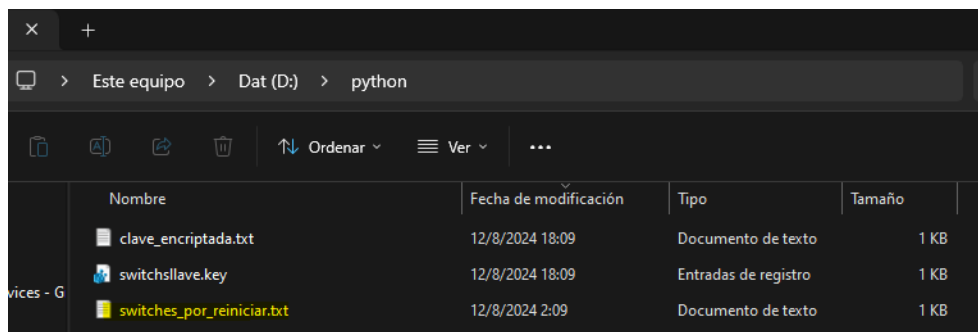
**Figura 20**  
*Correo de notificación carga de IOS*

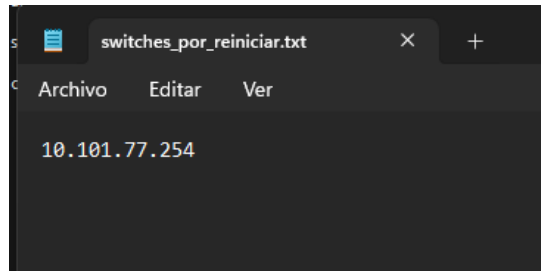


*Nota:* La figura presenta el correo de notificación de finalización del script de carga de IOS Firmware.

**Figura 21**  
*Filtrar los switches que tienen el estado 'OK'*

```
In [7]: 1 # Filtrar Los switches que tienen el estado 'OK'
2 switches_ok = report[report['Status'] == 'OK']['Switch'].tolist()
3
4 # Guardar La Lista de switches 'OK' en un archivo
5 with open('D:\\python\\switches_por_reiniciar.txt', 'w') as f:
6     for Switch in switches_ok:
7         f.write(Switch + '\n')
8
9 print("Lista de switches 'OK' guardada en 'D:\\python\\switches_por_reiniciar.txt'")
10 #enviar a un correo al administrador. Para Reiniciar
```





*Nota:* La figura presenta el script para filtrar los switches que cargaron el IOS de Firmware.

En el script para filtrar los switches se genera un archivo “.txt” en donde se almacena las IPs de los switches filtrados únicamente por los que, sí completaron la carga del IOS Firmware de Aruba, el dato es extraído del script anterior “Script para cargar el Firmware IOS en Switch Aruba 1930”.

El siguiente proceso es reiniciar los switches Aruba 1930 que tienen cargada la imagen IOS con el parche de actualización, para lo que se debe tener en cuenta que no es viable realizarlo en horario laboral debido a que los equipos de red switches Aruba 1930 se encuentran en producción ubicados en los locales de la marca. En función a esta premisa se tiene socializado el horario de ventana de mantenimiento desde las 1:00 am a 6:00 am GMT – 5.

## Figura 22

*Script para reiniciar los switches Aruba 1930*

```
In [28]: 1 # Script para reiniciar Los switches Aruba 1930
2 from selenium import webdriver
3 from selenium.webdriver.common.by import By
4 from selenium.webdriver.support.ui import WebDriverWait
5 from selenium.webdriver.support import expected_conditions as EC
6 from selenium.webdriver.chrome.service import Service
7 import pandas as pd
8 import time
9 import smtplib
10 from email.mime.multipart import MIMEMultipart
11 from email.mime.text import MIMEText
12 from datetime import datetime
13 from selenium.common.exceptions import TimeoutException
14
15 # Arreglo de lista de switches y status
16 data = {'Switch': [], 'Status': []}
17
18 # Iniciar el navegador
19 path = Service("D:\\python\\chromedriver126.0.6478.exe")
20 browser = webdriver.Chrome(service=path)
21
22 # Leer la lista de switches desde el archivo
23 switches_ok = []
24 with open('D:\\python\\switches_por_reiniciar.txt', 'r') as f:
25     switches_ok = [line.strip() for line in f.readlines()]
26
```



```

27 # Función para esperar texto y refrescar
28 def actualizar_navegador(browser, ip, data, max_attempts=3, wait_time=30):
29
30     attempts = 0
31     found = False
32     while attempts < max_attempts:
33         try:
34             WebDriverWait(browser, 10).until(
35                 EC.presence_of_element_located((By.XPATH, "//*[contains(text(), 'Aruba Instant On')]"))
36             )
37             found = True
38             print("Switch Aruba 1930 en Línea.")
39             break
40         except:
41             print("Reiniciando Switch Aruba 1930 - Intentando de nuevo...")
42             time.sleep(wait_time)
43             browser.refresh()
44             attempts += 1
45
46     if not found:
47         raise Exception("Switch Aruba inactivo después de varios intentos - Comunicarse con el local.")
48
49     print(f"Switch {ip} Actualizado Exitosamente.")
50     data['Switch'].append(ip)
51     data['Status'].append('OK')
52
53 # Reiniciar switches con estado 'OK'
54 for ip in switches_ok:
55     print(ip)
56
57     try:
58         # Abre cada URL por IP
59         browser.get('http://' + ip)
60         time.sleep(4)
61
62         # Parte 1: Reinicio inicial - Instalación de IOS
63         # Ingresar a la administración
64         browser.find_element(By.NAME, "inputUsername").send_keys(username)
65         browser.find_element(By.NAME, "inputPassword").send_keys(clave_desencriptada)
66         browser.find_element(By.CLASS_NAME, "btn").click()
67
68         # Navegar a opción de reinicio
69         WebDriverWait(browser, 5).until(EC.presence_of_element_located((By.LINK_TEXT, "Maintenance"))).click()
70         time.sleep(3)
71         WebDriverWait(browser, 5).until(EC.presence_of_element_located((By.LINK_TEXT, "Reset"))).click()
72
73         # Confirmar reinicio
74         WebDriverWait(browser, 15).until(EC.presence_of_element_located((By.ID, "btnReboot"))).click()
75
76         try:
77             # Validar que uno de los dos botones de reset esté seleccionable
78             reboot_button = WebDriverWait(browser, 15).until(
79                 EC.element_to_be_clickable((By.ID, "modalRebootButtonApply"))
80             )
81             reboot_button.click()
82         except TimeoutException:
83             try:
84                 confirm_reboot_button = WebDriverWait(browser, 15).until(
85                     EC.element_to_be_clickable((By.ID, "modalConfirmButtonSaveReboot"))
86                 )
87                 confirm_reboot_button.click()
88             except TimeoutException:
89                 print("Ninguno de los botones de reinicio fue encontrado.")
90
91
92     # Esperar reinicio del switch y actualización pantalla
93     print("Esperando a que el switch termine el reinicio Parte 1")
94     time.sleep(400)
95     browser.refresh()
96
97     # Verificar si el texto "Aruba Instant On" aparece después del reinicio
98     actualizar_navegador(browser, ip, data)
99
100 except Exception as e:
101     print(f"Error reiniciando el switch {ip} en Parte 1: {e}")
102     data['Switch'].append(ip)
103     data['Status'].append('CONEXION_FALLIDA')
104     continue
105
106 try:
107     # Parte 2: Instalar Actualización
108     # Ingresar a la administración
109     time.sleep(10)
110     browser.find_element(By.NAME, "inputUsername").send_keys(username)
111     browser.find_element(By.NAME, "inputPassword").send_keys(clave_desencriptada)
112     browser.find_element(By.CLASS_NAME, "btn").click()
113
114     # Actualizar versión
115     time.sleep(10)
116     WebDriverWait(browser, 10).until(EC.presence_of_element_located((By.ID, "modalInstallUpdate"))).click()
117
118     # Esperar reinicio del switch y actualización pantalla
119     print("Esperando a que el switch termine el reinicio Parte 2")
120     time.sleep(400)
121     browser.refresh()

```

```

122
123     # Verificar si el texto "Aruba Instant On" aparece después del reinicio
124     # Solo actualizar el estado si no fue actualizado en La Parte 1
125     if ip not in data['Switch']:
126         actualizar_navegador(browser, ip, data)
127
128     except Exception as e:
129         print(f"Error reiniciando el switch {ip} en Parte 2: {e}")
130         if ip not in data['Switch']:
131             data['Switch'].append(ip)
132             data['Status'].append('CONEXION_FALLIDA')
133
134     browser.quit()

```

```

137 # Visualización Reporte de Status en Data Frame
138 report = pd.DataFrame(data)
139 print(report)
140
141 # Envio de correo Reporte Final
142 # Configuración del servidor SMTP y credenciales
143 smtp_server = 'smtp.gmail.com'
144 smtp_port = 587
145 usuario_correo = %env CORREO_GMAIL
146 clave_correo = %env CLAVE_GMAIL
147
148 # Configuración del correo
149 de_direccion = %env CORREO_GMAIL
150 a_direccion = 'pablo.caceres@kfc.com.ec'
151
152 # Obtener La fecha y hora actual
153 now = datetime.now()
154 fecha_formato = now.strftime("%Y-%m-%d %H:%M:%S")
155
156 # Asunto del correo con fecha y hora
157 subject = f'Automatización Actualización Firmware Aruba 1930 Finalizado - {fecha_formato}'
158 body = f"\nReporte de Automatización Firmware Actualizado Aruba 1930 GRUPOKFC\n\n {report.to_string()}\n\nRealizado por Pablo David Cáceres Castro\n\n"
159
160 # Crear el mensaje MIME "Extension multiproposito de correo electronico"
161 msg = MIMEText(body, 'plain')
162 msg['From'] = de_direccion
163 msg['To'] = a_direccion
164 msg['Subject'] = subject
165 msg.attach(MIMEText(body, 'plain'))
166
167 # Validación y envío el correo
168 try:
169     server = smtplib.SMTP(smtp_server, smtp_port)
170     server.starttls()
171     server.login(usuario_correo, clave_correo)
172     text = msg.as_string()
173     server.sendmail(de_direccion, a_direccion, text)
174     server.quit()
175     print("\nCorreo enviado exitosamente.")
176 except Exception as e:
177     print(f"Error al enviar el correo: {e}")
178
179 print("\n\n#####")
180 print("#")
181 print("# FINALIZADO #")
182 print("#")
183 print("#")
184 print("#####")

```

*Nota:* La figura presenta el script para reiniciar los switches Aruba 1930.

### Figura 23

*Resultados de Script en pantalla*

```

10.101.56.254
Esperando a que el switch termine el reinicio Parte 1
Switch Aruba 1930 en Linea.
Switch 10.101.56.254 Actualizado Exitosamente.
Esperando a que el switch termine el reinicio Parte 2
Switch Aruba 1930 reiniciando - Intentando de nuevo...
Switch Aruba 1930 en Linea.
Switch 10.101.56.254 Actualizado Exitosamente.
Switch Status
0 10.101.56.254 OK

```

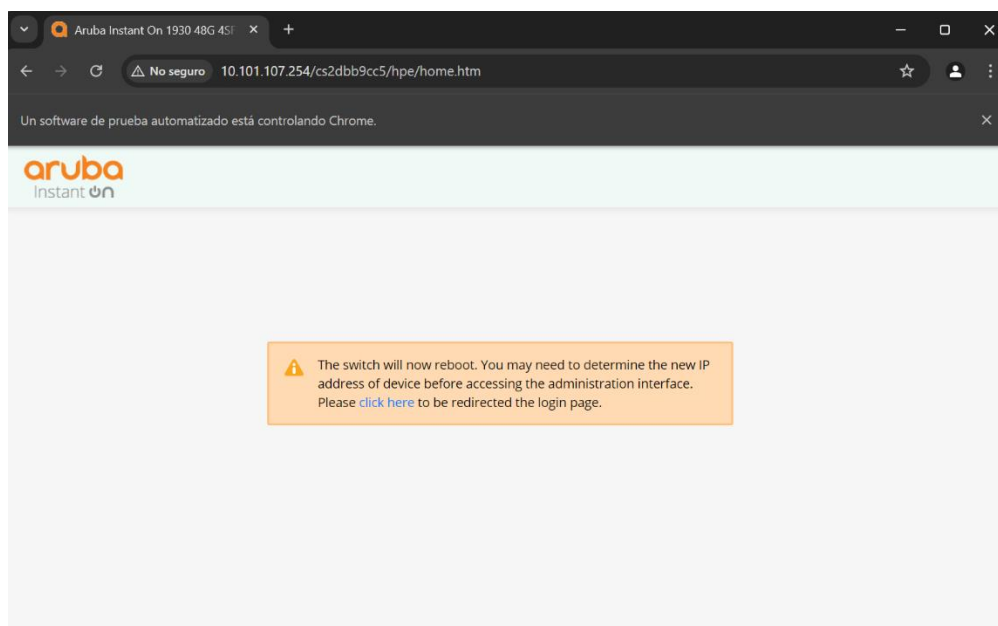
*Nota:* La figura presenta el resultado del script al finalizar la automatización para reiniciar los switches Aruba 1930.

El script se compone de una validación en 2 partes, las que consisten en 2 reinicios del equipo switches Aruba 1930. El primer reinicio se utiliza para que el switches Aruba

1930 identifique el parche cargado y lo detecte como actualización ver figura 24. El segundo reinicio se requiere una vez que se envía la instalación del parche, ver figura 25.

**Figura 24**

*Pantalla de espera reinicio*



*Nota:* La figura presenta la pantalla de espera al seleccionar el botón de reiniciar el dispositivo.

**Figura 25**

*Pantalla instalar actualización firmware*



*Nota:* La figura presenta la pantalla para la instalación de la actualización del firmware previamente cargada en el switch Aruba 1930.

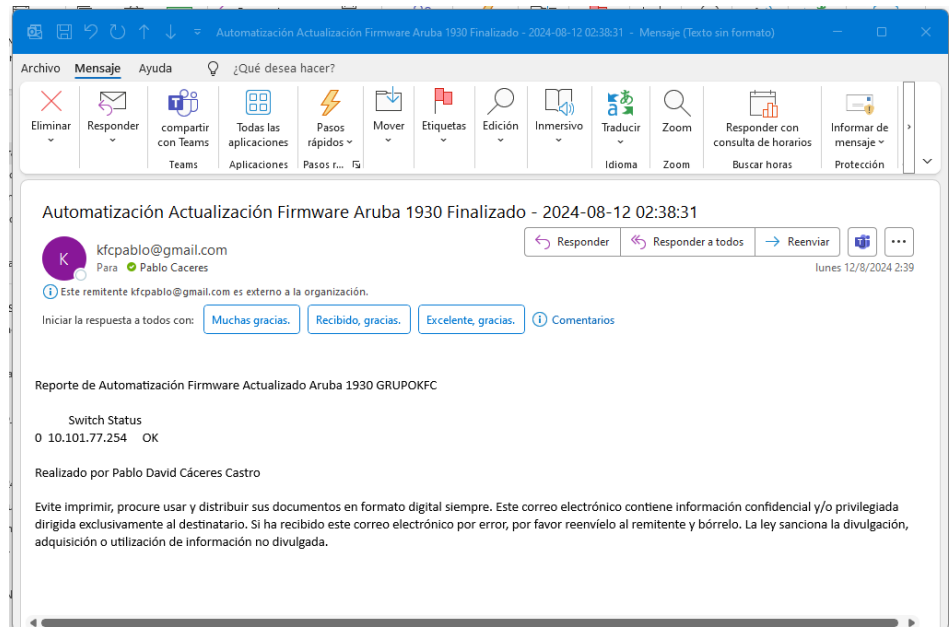
Una vez terminados los reinicios y la instalación del parche de actualización per se, culmina el proceso y la automatización con la supervisión del operador de networking finaliza.

**Tabla 4**  
*Tiempos ejecución Scripts*

Tabla de tiempos Scripts	Minutos
Encriptar clave	<1
Desencriptar clave	<1
Carga de Firmware	4 a 8
Filtrar switches con Firmware cargado	<1
Reinicio de Switch 1era Parte	7 a 8
Reinicio de Switch 2da Parte	7 a 8
<b>Tiempo total aproximado</b>	<b>± 23</b>

*Nota:* La tabla indica los tiempos aproximados utilizados para la ejecución de los scripts de la automatización.

**Figura 26**  
*Correo de notificación reinicio de switches Aruba 1930*



*Nota:* La figura presenta el correo de notificación de finalización del script de reinicio de switches Aruba 1930 y fin de la automatización.

## 2.5 Implementación

En el proceso de la implementación del proyecto se contemplan los siguientes requisitos necesarios para el despliegue de la automatización:

- Cerciorarse que el equipo desde donde se realice el despliegue de la automatización se encuentre en un segmento de red habilitado para tener comunicación con los segmentos de los locales.
- Cerciorarse que el equipo para la automatización no tenga otro proceso que pueda interrumpir el despliegue.
- Asegurarse que el equipo disponga de las versiones compatibles de Python, Selenium y Chromedriver126.0.6478 necesarios para el funcionamiento.
- Asegurarse que durante el proceso el switch Aruba del local no sea desconectado o reiniciado.
- Programar un reinicio controlado del switch Aruba fuera de horario laboral, para no interrumpir a la operación.

## 2.6 Requerimientos de hardware y software

Para el desarrollo de la presente automatización los requerimientos son los siguientes:

### Software para servidor/ pruebas

- Python
- Jupyter Notebook
- Navegador Chrome
- Driver: chromedriver126.0.6478
- Selenium

- TFTP Server

***Hardware para servidor y usuario redes***

- Laptop para realizar configuraciones.
- Equipo/Servidor con acceso a la red interna
- Switches Aruba 1930 (Sucursales de comida rápida)

## CONCLUSIONES

- El estado situacional actual de la multinacional de comida rápida con respecto a la gestión de actualizaciones de firmware de los equipos de red marca Aruba modelo 1930. Para esto se realizaron entrevistas con los encargados del área de Networking y Jefatura de Infraestructura para recabar la información de la situación actual y poder disponer de un panorama para la solución a diseñar.
- El diseño del prototipo de la automatización de actualizaciones de firmware para los equipos switches Aruba modelo 1930, ha permitido la posibilidad de estandarizar las configuraciones y pasos necesarios para disponer de una automatización adecuada a la solución requerida.
- Con la implementación de este proyecto, a nivel personal, ha permitido investigar y conocer más a fondo sobre las tecnologías de automatización para escenarios de pruebas controlados y no controlados para el despliegue de configuraciones en equipos de red.
- El evaluar el comportamiento del prototipo de la automatización mediante pruebas de actualizaciones de firmware controladas ha permitido modificar la automatización para un mejor funcionamiento acorde a lo requerido por el negocio.
- Se ha validado con la actualización de la versión del firmware exitoso, y el correcto funcionamiento de los switches luego de la actualización, permitiendo el control centralizado a 1 solo operador de networking que con el debido control podrá actualizar el firmware de los switches de la cadena de comida rápida en 1 sola jornada.

## RECOMENDACIONES

- Se recomienda implementar un equipo o servidor centralizador dentro de la red de la empresa desde donde se realizará la ejecución de la automatización.
- Se recomienda realizar el proceso de automatización en modo consecutivo IP por IP, ya que por la limitación de recursos el desplegar múltiples ventanas colapsaría al equipo desde donde se realiza la automatización.
- Se recomienda tener un equipo con características de al menos Core i7 y 8 GB de RAM ya que el proceso de automatización utiliza aproximadamente 1.1 GB de RAM por ventana de automatización levantada/habilitada.
- Se recomienda quitar la suspensión automática o bloqueo en el equipo desde donde se ejecuta la automatización mientras se realiza el proceso para evitar la interrupción o fallo de este.
- Se debe planificar los reinicios requeridos fuera de horario para no afectar el funcionamiento de los switches Aruba ubicados en los locales.
- Se recomienda realizar la ejecución de la automatización en un horario con baja carga operativa y de transacciones en el local, para no afectar el correcto funcionamiento en el entorno de red del local.
- Realizar un mantenimiento continuó de la automatización y pruebas para validar que de la versión del IOS publicado de parte de Aruba sea compatible con la automatización, en sus nuevas versiones de IOS y así tener la versión de IOS estable y actualizada en el entorno de red empresarial.
- Se recomienda realizar la automatización de manera controlada con la supervisión de un operador, debido a que en caso de perder comunicación con el switch es necesario poder solventarlo lo más pronto posible con el administrador del local.



## REFERENCIAS BIBLIOGRÁFICAS

- Ansible pricing 2024. (s/f). TrustRadius. Recuperado el 13 de agosto de 2024, de <https://www.trustradius.com/products/red-hat-ansible-automation-platform/pricing>
- Congo Pastrana, J. W. (2018). Aplicaciones del software libre Python para prácticas de laboratorio aplicado a la asignatura de tratamiento digital de señales de la Universidad Tecnológica Israel. UISRAEL-EC-ELDT-378.242-2018-042([Tipo de tesis para optar un grado o título inédita]), 96p. Quito.
- Contributors, I. (2013-2024). <https://cryptography.io/en/latest/fernet/>. <https://cryptography.io/en/latest/fernet/>: <https://cryptography.io/en/latest/fernet/>
- Deepthi Wilson. R, M. B. (2017). A Comprehensive Review on Selenium Automation Testing Tool, . INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCETEIT, Volume 5(20), 3. <https://doi.org/10.17577/IJERTCONV5IS20027>
- International IT. (5 de julio de 2022). [www.internationalit.com](http://www.internationalit.com): <https://www.internationalit.com/post/qu%C3%A9-es-la-gesti%C3%B3n-de-red-y-por-qu%C3%A9-es-importante?lang=es#:~:text=La%20gesti%C3%B3n%20de%20red%20es,de%20manera%20efectiva%20y%20r%C3%A1pida>.
- jupyter.org/. (2024). <https://jupyter.org/>. <https://jupyter.org/>: <https://jupyter.org/>
- LLagua, A. (9 de 12 de 2012). <https://alejollagua.blogspot.com>. <https://alejollagua.blogspot.com>: <https://alejollagua.blogspot.com/2012/12/calculo-del-tiempo-de-transferencia-de.html>
- ManageEngine Network Configuration Management (NCM) pricing 2024. (s/f). TrustRadius. Recuperado el 13 de agosto de 2024, de

<https://www.trustradius.com/products/manageengine-network-configuration-management-ncm/pricing>

Pactomundial.org. (s.f.). <https://www.pactomundial.org/ods/9-industria-innovacion-e-infraestructura/>.  
<https://www.pactomundial.org/ods/9-industria-innovacion-e-infraestructura/>

Pozo, C. (2017). Conectividad remota cliente - servidor a través de túneles IPv6 y seguridad IPSec, en ambientes multiplataforma. p23.  
<https://doi.org/16868/1/69002>

Red Hat. (25 de 11 de 2021). <https://www.redhat.com/es/topics/security/what-is-cve>.  
<https://www.redhat.com>: <https://www.redhat.com/es/topics/security/what-is-cve>

Red Hat. (14 de febrero de 2023). <https://www.redhat.com/es/topics/automation/whats-it-automation>.  
[www.redhat.com](https://www.redhat.com):  
<https://www.redhat.com/es/topics/automation/whats-it-automation>

Red Hat. (20 de 09 de 2023). <https://www.redhat.com/es/topics/automation>.  
<https://www.redhat.com/>: <https://www.redhat.com/es/topics/automation>

Selenium. (s/f). Selenium. Recuperado el 13 de agosto de 2024, de  
<https://www.selenium.dev/>

SolarWinds Worldwide. (2024). <https://documentation.solarwinds.com/>.  
<https://documentation.solarwinds.com/>:  
[https://documentation.solarwinds.com/en/success\\_center/ncm/content/ncm-using-the-tftp-server.htm](https://documentation.solarwinds.com/en/success_center/ncm/content/ncm-using-the-tftp-server.htm)


Velazquez, A. (s.f.). <https://www.questionpro.com>. <https://www.questionpro.com>:  
<https://www.questionpro.com/blog/es/investigacion-experimental/#:~:text=La%20investigaci%C3%B3n%20experimental%20es%20cualquier,miden%20como%20sujeto%20del%20experimento>.

## ANEXOS

### ANEXO 1: Encuesta de factibilidad- Capitulo 1:

Link:

[https://docs.google.com/forms/d/e/1FAIpQLScrdBK9DKVlbYiZ4UPAlojQUCyUUOwDN4oII7Cws27tl\\_dNYw/viewform](https://docs.google.com/forms/d/e/1FAIpQLScrdBK9DKVlbYiZ4UPAlojQUCyUUOwDN4oII7Cws27tl_dNYw/viewform)



### Encuesta Upgrade Automatización IOS Aruba

Networking KFC - Orientado a Jefatura y Gerencia de Infraestructura IT

e1721306239@uisrael.edu.ec [Cambiar de cuenta](#)

 No compartido

\* Indica que la pregunta es obligatoria

¿Esta de acuerdo en utilizar una solución de automatización para actualizar el IOS de los Switchs Aruba de la marca KFC en EC? \*

Ingresar respuesta en MAYUSCULAS

- ☐ Totalmente de acuerdo
- ☐ Algo de acuerdo
- ☐ Nada de acuerdo
- ☐ Otro: \_\_\_\_\_

¿Esta de acuerdo en que se implemente una solución de automatización de upgrade de IOS para Switchs Aruba con costo cero? \*

☐ Totalmente de acuerdo

☐ Algo de acuerdo

☐ Nada de acuerdo

☐ Otro: \_\_\_\_\_

¿Está de acuerdo en que se corrija vulnerabilidades de ciberseguridad con actualización de IOS de networking en los switchs Aruba de los locales de KFC EC? \*

☐ Totalmente de acuerdo

☐ Algo de acuerdo

☐ Nada de acuerdo

☐ Otro: \_\_\_\_\_

*Disclaimer*

*Los datos personales solicitados no serán utilizados con fines comerciales, únicamente para el control y registro de esta encuesta.*

Enviar

Página 1 de 1

Borrar formulario

## ANEXO 2: VARIABLES DE ENTORNO

```
In [2]: 1 #Variables de Entorno
        2 %env CLAVE_GMAIL= nedu gjmr xxos oxar
        3 %env CLAVE_ADMIN= Slapeoar!9907
        4 %env CORREO_GMAIL= kfcapablo@gmail.com
        5 %env USER_SWITCH= admin
        6

env: CLAVE_GMAIL=nedu gjmr xxos oxar
env: CLAVE_ADMIN=Slapeoar!9907
env: CORREO_GMAIL=kfcapablo@gmail.com
env: USER_SWITCH=admin
```

Nota: Variables utilizadas en la automatización.

**ANEXO3****Tabla 5***Inventario Switches Aruba 1930 KFC Ecuador*

N°	Nombre para mostrar	IP REGULARIZADA	NOMBRE_SWITCH	PUERTOS_SWITCH	MARCA_SWITCH	MODELO_SWITCH	VERSION_SWITCH	ACCESO	REGION
1	kfck02 (9 de Octubre)	10.101.2.254	SWC-KFC002	48	ARUBA	1930	2.6.0	WEB	COSTA
2	kfck08 (El Bosque)	10.101.8.254	SWS-KFC008	24	ARUBA	1930	2.6.0	WEB	SIERRA
3	kfck10 (Recreo)	10.101.10.254	SW-K010	24	ARUBA	1930	1.0.2.0 (125)	WEB	SIERRA
4	kfck100 (Quicentro Sur PA)	10.101.100.254	SW-KFC100	24	ARUBA	1930	2.6.0	WEB	SIERRA
5	kfck101 (Quicentro Sur PB)	10.101.101.254	SWS-KFC101	24	ARUBA	1930	2.6.0	WEB	SIERRA
6	kfck107 (Gran Aki Ibarra)	10.101.107.254	SWS-KFC107	48	ARUBA	1930	2.6.0	WEB	SIERRA
7	kfck11 (Bosque Patio)	10.101.11.254	SWS-KFC011	24	ARUBA	1930	2.6.0	WEB	SIERRA
8	kfck110 (City Mall)	10.101.110.254	SWC-KFC110	48	ARUBA	1930	1.0.2.0 (125)	WEB	COSTA
9	kfck112 (Cayambe)	10.101.112.254	SWS-KFC112	48	ARUBA	1930	2.6.0	WEB	SIERRA
10	kfck114 (Laguna Mall Ibarra)	10.101.114.254	SW-K114	24	ARUBA	1930	1.0.2.0 (125)	WEB	SIERRA
11	Kfck115 (Entrada de la 8)	10.101.115.254	SWC-KFC115	24	ARUBA	1930	1.0.2.0 (125)	WEB	COSTA
12	kfck117 (La 29 y Sedalana)	10.101.117.254	SWC-KFC117	24	ARUBA	1930	1.0.2.0 (125)	WEB	COSTA
13	kfck12 (Rio Centro Puntilla)	10.101.12.254	SWC-KFC012	48	ARUBA	1930	1.0.2.0 (125)	WEB	COSTA
14	kfck16 (Granados)	10.101.16.254	SWS-KFC016	48	ARUBA	1930	2.6.0	WEB	SIERRA
15	kfck161 (Mall del Rio)	10.101.161.254	SWC-KFC161	24	ARUBA	1930	1.0.4.0 (125)	WEB	COSTA
16	kfck162 (Estacion de servicio)	10.101.162.254	SWC-KFC162	24	ARUBA	1930	2.6.0	WEB	COSTA
17	kfck163 (San Rafael)	10.101.163.254	SW-KFC163	24	ARUBA	1930	1.0.2.0 (125)	WEB	SIERRA
18	kfck165 (Plaza Tia Duran)	10.101.165.254	SWC-KFC165	48	ARUBA	1930	1.0.2.0 (125)	WEB	COSTA
19	Kfck167 ( San Francisco)	10.101.167.254	SWS-KFC167	48	ARUBA	1930	2.6.0	WEB	SIERRA
20	Kfck168 (Coral Carapungo)	10.101.168.254	SWS-KFC168	48	ARUBA	1930	2.6.0	WEB	SIERRA
21	kfck169 (Plaza Pacifico)	10.101.169.254	SWC-KFC169	48	ARUBA	1930	2.6.0	WEB	COSTA

22	kfck17 (Colonial)	10.101.17.254	SWS-K017	24	ARUBA	1930	1.0.2.0 (125)	WEB	SIERRA
23	kfck170 (Machachi)	10.101.170.254	SWS-KFC170	48	ARUBA	1930	2.6.0	WEB	SIERRA
24	kfck171 (Shell Abu Dabi)	10.101.171.254	SWC-KFC171	24	ARUBA	1930	2.6.0	WEB	COSTA
25	kfck172 (Mall del Norte)	10.101.172.254	SWC-K172	24	ARUBA	1930	2.6.0	WEB	COSTA
26	Kfck173 (CC Oasis GYE)	10.101.173.254	SWC-KFC173	48	ARUBA	1930	2.6.0	WEB	COSTA
27	kfck174 (Mall del Rio PB Cuenca)	10.101.174.254	SWC-KFC174	24	ARUBA	1930		WEB	COSTA
28	kfck175 (Via a la costa)	10.101.175.254	SWC-K175	48	ARUBA	1930	2.6.0	WEB	COSTA
29	kfck25 (Mobil Duran)	10.101.25.254	SWC-KFC025	24	ARUBA	1930	1.0.2.0 (125)	WEB	COSTA
30	kfck27 (Colon)	10.101.27.254	SWS-KFC027	24	ARUBA	1930	2.6.0	WEB	SIERRA
31	kfck28 (Sto Domingo)	10.101.28.254	SW-K028	24	ARUBA	1930	1.0.2.0 (125)	WEB	SIERRA
32	kfck36 (Power Center)	10.101.36.254	SWC-KFC036	24	ARUBA	1930	2.6.0	WEB	COSTA
33	kfck37 (Gran AKI Gye)	10.101.37.254	SWC-KFC037	24	ARUBA	1930	1.0.2.0 (125)	WEB	COSTA
34	kfck38 (Mobil)	10.101.38.254	SWS-K038	24	ARUBA	1930	1.0.2.0 (125)	WEB	COSTA
35	kfck40 (Riobamba Paseo Shopping)	10.101.40.254	SW-KFC040	24	ARUBA	1930	2.6.0	WEB	SIERRA
36	kfck41 (Cuenca)	10.101.41.254	SWS-K041	48	ARUBA	1930	2.6.0	WEB	COSTA
37	kfck42 (Portoviejo)	10.101.42.254	SW-K042	24	ARUBA	1930	2.6.0	WEB	COSTA
38	kfck44 (Baca Ortiz)	10.101.44.254	SWS-KFC044	48	ARUBA	1930	2.6.0	WEB	SIERRA
39	kfck48 (Salinas)	10.101.48.254	SWC-KFC048	48	ARUBA	1930	1.0.2.0 (125)	WEB	COSTA
40	kfck49 (Shell Sur)	10.101.49.254	SWS-KFC049	24	ARUBA	1930	2.6.0	WEB	SIERRA
41	kfck53 (Shopping Babahoyo)	10.101.53.254	SWC-KFC053	24	ARUBA	1930	1.0.2.0 (125)	WEB	COSTA
42	kfck55 (Cordova)	10.101.55.254	SWC-K055	24	ARUBA	1930	2.6.0	WEB	COSTA
43	kfck56 (La Escala)	10.101.56.254	SW-K056	24	ARUBA	1930	2.6.0	WEB	SIERRA
44	kfck59 (Mall del Sur PB)	10.101.59.254	SWC-KFC059	24	ARUBA	1930	1.0.2.0 (125)	WEB	COSTA

kfck61 (Cuenca Mall del Rio								
45	PB)	10.101.61.254	SWC-KFC061	48	ARUBA	1930	1.0.2.0 (125)	WEB COSTA
46	kfck62 (La Malteria Latacunga)	10.101.62.254	SW-K062	24	ARUBA	1930	2.6.0	WEB SIERRA
47	kfck67 (Mobil Beneficencia)	10.101.67.254	SWC-KFC067	24	ARUBA	1930	2.6.0	WEB COSTA
48	kfck75 (Mobil Kennedy)	10.101.75.254	SWC-KFC075	24	ARUBA	1930	2.6.0	WEB COSTA
49	kfck76 (Plaza Centenario)	10.101.76.254	SWC-KFC076	48	ARUBA	1930	2.6.0	WEB COSTA
50	kfck77 (Rio Centro Ceibos)	10.101.77.254	SWC-KFC077	24	ARUBA	1930	2.6.0	WEB COSTA
51	kfck79 (Babahoyo)	10.101.79.254	SW-K079	24	ARUBA	1930	1.0.2.0 (125)	WEB COSTA
52	kfck80 (Riobamba)	10.101.80.254	SWS-K080	24	ARUBA	1930	2.6.0	WEB SIERRA
kfck81 (Sto Domingo P								
53	Shoping)	10.101.81.254	SW-K081	24	ARUBA	1930	1.0.2.0 (125)	WEB SIERRA
54	kfck82 (Shopping Playas)	10.101.82.254	SWC-K082	24	ARUBA	1930	2.6.0	WEB COSTA
55	kfck84 (Aeropuerto UIO)	10.101.84.254	SWS-K084	24	ARUBA	1930	1.0.2.0 (125)	WEB SIERRA
56	kfck85 (Mobil Ceibos)	10.101.85.254	SWC-KFC085	24	ARUBA	1930	1.0.2.0 (125)	WEB COSTA
57	kfck94 (Outlet Duran)	10.101.94.254	SW-K094	24	ARUBA	1930	1.0.2.0 (125)	WEB COSTA
kfck95 (Paseo Shopin Via								
58	Daule)	10.101.95.254	SW-K095	24	ARUBA	1930	1.0.2.0 (125)	WEB COSTA
59	kfck99 (Cuenca)	10.101.99.254	SWC-K099	24	ARUBA	1930	1.0.2.0 (125)	WEB COSTA

Nota: Nombre, ubicación y descripción básica de los Switches Aruba 1930 de la marca KFC Ecuador.

## ANEXO 4: Reporte CVE HPE – Aruba Instant ON 1930

24/7/24, 10:01

HPESBNW04270 rev.2 - HPE Aruba Instant On 1930 switch, Denial of Service



**SECURITY BULLETIN**

**Document ID:** hpesbnw04270en\_us  
**Version:** 2  
**Severity:** High  
**HPESBNW04270 rev.2 - HPE Aruba Instant On 1930 switch, Denial of Service**

**NOTICE:** The information in this Security Bulletin should be acted upon as soon as possible.

**Release Date:** 2022-04-06  
**Last Updated:** 2024-06-18

**Potential Security Impact:** Remote: Denial of Service (DoS)  
**Source:** Hewlett Packard Enterprise, HPE Product Security Response Team

**VULNERABILITY SUMMARY**

**Note:** Information originally published in [hpe\\_aruba\\_networking - 2022-005.txt](#)  
**Note:** A CSAF version of this document exists at [hpe\\_aruba\\_networking - 2022-005.json](#)

Aruba Product Security Advisory  
Advisory ID: ARUBA-PSA-2022-005  
CVE: CVE-2021-41004, CVE-2021-41005  
Publication Date: 2022-Apr-05  
Status: Confirmed  
Severity: High  
Revision: 1

**Title**  
Aruba Instant On Switch Denial of Service Vulnerabilities

**Overview**  
Aruba has discovered two Denial of Service vulnerabilities in Aruba Instant On 1930 Switches. CVE-2021-41005 requires authentication to be exploited and CVE-2021-41004 can be exploited without supplying any authentication information.

**Affected Products**

- Aruba Instant On 1930 switches firmware versions 1.0.7.0 and below when managed through the local web interface.

**Unaffected Products**

- All other Aruba Switches and all Aruba Access Points.
- Instant On 1930 Switches when managed through cloud-based mobile app and web portal.

**Details**  
Two Denial of Service vulnerabilities were discovered in Aruba Instant On 1930 Switches. These vulnerabilities can be exploited to cause the switch to reboot. CVE-2021-41004 does not require authentication credentials to exploit the Denial of Service condition. CVE-2021-41005 requires authentication in order to be successfully exploited.

These vulnerabilities only impact locally managed switches. Cloud managed switches are not impacted by these vulnerabilities.

Unauthenticated Denial of Service: (CVE-2021-41004) Internal references: ASIRT-881 Severity: High CVSSv3 Overall Score: 7.5 CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Authenticated Denial of Service: (CVE-2021-41005) Internal references: ASIRT-882 Severity: Medium CVSSv3 Overall Score: 6.5 CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

**References:**

- CVE-2021-41004
- CVE-2021-41005

**SUPPORTED SOFTWARE VERSIONS\*: ONLY impacted versions are listed.**



24/7/24, 10:01 HPESBNW04270 rev.2 - HPE Aruba Instant On 1930 switch, Denial of Service  
Aruba Instant On 1930 Switch Series - Firmware below v1.0.7.0 - see note in summary

BACKGROUND

HPE calculates CVSS using CVSS Version 3.1. If the score is provided from NIST, we will display Version 2.0, 3.0, or 3.1 as provided from NVD.

Reference	V3 Vector	V3 Base Score	V2 Vector	V2 Base Score
CVE-2021-41004	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5	(AV:N/AC:L/Au:N/C:N/I:N/A:C)	7.8
CVE-2021-41005	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5	(AV:N/AC:L/Au:S/C:N/I:N/A:C)	6.8

Information on CVSS is documented in HPE Customer Notice: HPSN-2008-002

These vulnerabilities were discovered by Nicholas Starke of Aruba Threat Labs.

RESOLUTION

Resolution

Upgrading to version 2.5.0.42 or above addresses both of these vulnerabilities. Firmware can be manually updated with the download from here: <https://community.arubaInstantOn.com/browse/blogs/blogviewer?blogkey=8aac4e14-50d9-4991-8c72-602a4d87768d>

Workaround and Mitigations

To further minimize the likelihood of an attacker exploiting these vulnerabilities, Aruba recommends that the web-based management interface for Aruba Instant On switches be restricted to a dedicated layer 2 segment/VLAN and/or controlled by firewall policies at layer 3 and above.

Exploitation and Public Discussion

Aruba is not aware of any public proof of concept code.

HISTORY

- Version:1 (rev.1) - 6 April 2022 Initial release
- Version:2 (rev.2) - 17 June 2024 Updating HPE and CSAF links for webpage conversion

**Third Party Security Patches:** Third party security patches that are to be installed on systems running Hewlett Packard Enterprise (HPE) software products should be applied in accordance with the customer's patch management policy.

**Support:** For issues about implementing the recommendations of this Security Bulletin, contact normal HPE Services support channel. For other issues about the content of this Security Bulletin, send e-mail to [security-alert@hpe.com](mailto:security-alert@hpe.com).

**Report:** To report a potential security vulnerability for any HPE supported product:

- Web Form: <https://www.hpe.com/info/report-security-vulnerability>
- Email: [security-alert@hpe.com](mailto:security-alert@hpe.com)
- Hewlett Packard Enterprise Product Security Response Policy: [https://support.hpe.com/hpsc/public/docDisplay?docLocale=en\\_US&docId=a00100637en\\_us](https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&docId=a00100637en_us)

**Subscribe:** To initiate a subscription to receive future HPE Security Bulletin alerts via Email: [http://www.hpe.com/support/Subscriber\\_Choice](http://www.hpe.com/support/Subscriber_Choice)

**Security Bulletin Archive:** A list of recently released Security Bulletins is available here: [http://www.hpe.com/support/Security\\_Bulletin\\_Archive](http://www.hpe.com/support/Security_Bulletin_Archive)

System management and security procedures must be reviewed frequently to maintain system integrity. HPE is continually reviewing and enhancing the security features of software products to provide customers with current secure solutions.

"HPE is broadly distributing this Security Bulletin in order to bring to the attention of users of the affected HPE products the important security information contained in this Bulletin. HPE recommends that all users determine the applicability of this information to their individual situations and take appropriate action. HPE does not warrant that this information is necessarily accurate or complete for all user situations and, consequently, HPE will not be responsible for any damages resulting from user's use or disregard of the information provided in this Bulletin. To the extent permitted by law, HPE disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose, title and non-infringement."

©Copyright 2024 Hewlett Packard Enterprise Development LP

Hewlett Packard Enterprise Development shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither HPE nor its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice. Hewlett Packard Enterprise Development and the names of Hewlett Packard Enterprise Development products

24/7/24, 10:01

HPESBNW04270 rev.2 - HPE Aruba Instant On 1930 switch, Denial of Service

referenced herein are trademarks of Hewlett Packard Enterprise Development in the United States and other countries.  
Other product and company names mentioned herein may be trademarks of their respective owners.



6%

INDICE DE SIMILITUD

2%

FUENTES DE INTERNET

0%

PUBLICACIONES

4%

TRABAJOS DEL  
ESTUDIANTE

FUENTES PRIMARIAS

1

Submitted to Universidad Tecnológica Israel

Trabajo del estudiante

2%

2

Submitted to UNIV DE LAS AMERICAS

Trabajo del estudiante

1%

3

Submitted to Universidad Manuela Beltrán

Trabajo del estudiante

<1%

4

Submitted to Fundación Universitaria CEIPA

Trabajo del estudiante

<1%

5

wn.com

Fuente de Internet

<1%

6

rio.upo.es

Fuente de Internet

<1%

7

seguridad0.com

Fuente de Internet

<1%

8

pdffox.com

Fuente de Internet

<1%

9

www.shipjournal.co

Fuente de Internet

<1%

10	<a href="https://es.slideshare.net">es.slideshare.net</a>	< 1 %
----	---	-------

Fuente de Internet

11	<a href="http://www.industriagraficaonline.com">www.industriagraficaonline.com</a>	< 1 %
----	--	-------

Fuente de Internet

12	<a href="http://www.lanota.com.co">www.lanota.com.co</a>	< 1 %
----	--	-------

Fuente de Internet

Excluir citas

Activo

Excluir coincidencias

Apagado

Excluir bibliografía

Activo