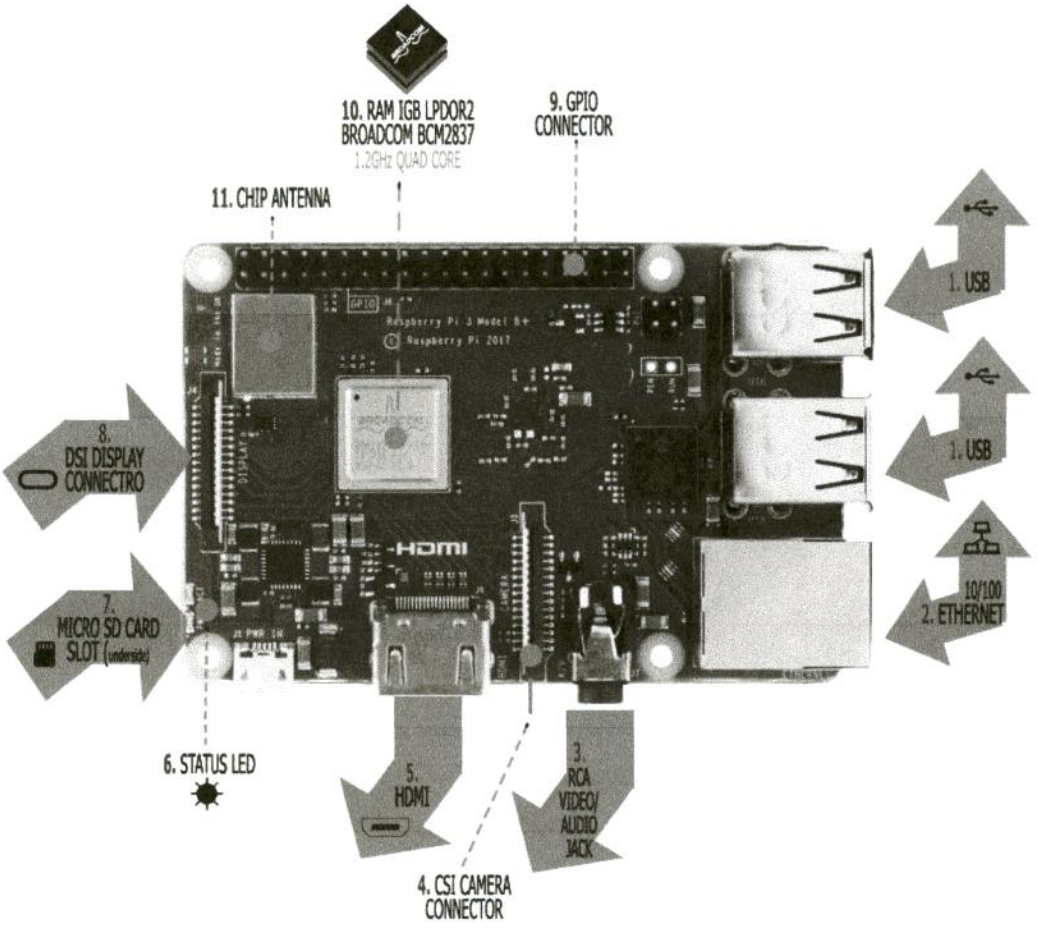


Imagen 1: Unidad computacional empleada para la invención.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN:

En la actualidad la búsqueda de la estandarización y adopción de modelos de gestión para las empresas, son adoptados de manera consiente o de obligatorio cumplimiento mediante la emisión de circulares o decretos.

Muchos de los modelos de gestión están basados en estándares internacionales o buenas practicas, a la hora de implementarlos surgen algunos problemas comunes, los costos asociados a la implementación, la adquisición de múltiples herramientas independientes, la falta de mano de obra calificada o certificada, la

centralización de la información, los modelos de capacitación, la evaluación del modelo implementado, y el sostenimiento del mismo.

Para reducir los costos y solucionar los problemas anteriores se crea HackInspector, una unidad computacional configura para la implementación de un SGSI (Sistema de Gestión en Seguridad de la Información), que integra hardware (unidad computacional), específicamente Raspberry pi 3 (sin limitarse únicamente a dicha plataforma de hardware open source), una serie de algoritmos programados que permiten el uso de las siguientes funcionalidades:

1. Funcionalidad de registro de licencia, para activación de las funciones configuradas en la unidad computacional.

2. Ejecución y/o programación de escaneos a aplicaciones web, captura de trafico de red para detección de amenazas en redes inalámbricas y búsqueda de vulnerabilidades de seguridad informática en los equipos conectados en la misma red que la unidad computacional configurada (HackInspector).

3. Descubrimiento y listado de equipos conectados en la red a analizar.

4. Búsqueda y alertamiento de vulnerabilidades cero day, sobre los activos de información ingresados por el usuario.

5. Visualización de reportes generados por el HackInspector.

6. Funcionalidad para gestión de activos

7. Funcionalidad para la gestión de incidentes

8. Check list de normas internaciones o estándares

9. Centralización de documentación

10. Funcionalidad de seguridad para asignación de contraseñas o mecanismos de recuperación

11. Funcionalidad para la gestión de usuarios

12. Funcionalidad para adicionar nuevas funcionalidades

13. Registro de logs de auditorias

14. Funcionalidad de cambio de idioma.

15. Adquisición de data

16. Alertamiento Defacement

La unidad computacional interpreta cada uno de los algoritmos programados y contenidos en la unidad de almacenamiento, los interpreta y los expone al usuario en forma de funcionalidades a través de una interfaz web sirviendo así la unidad computacional (HackInspector) como un servidor web local.

A continuación, Descripción detallada de las funcionalidades configuradas:

- **Funcionalidad de registro y validación:** El proceso de activación de las funcionalidades configuradas en la unidad computacional, fue diseñado para que un usuario sin conocimientos técnicos avanzados en informática pueda realizarlo, es necesario conectar la unidad computacional a través de clave de red a un computador y acceder a través de navegación web a una

dirección IP especifica configurada en la unidad (sirviendo la unidad computacional como un servidor web local).

Para hacer uso de las funcionalidades, se requiere de un proceso de registro y activación de licencia, en la funcionalidad de registro, el usuario deberá ingresar su nombre o nombre de la empresa, un correo electrónico, seleccionar una red inalámbrica la cual le proporcionará conexión a internet al dispositivo o en su defecto deberá ingresar la modalidad de conexión (DHCP o dirección Ip estática) a través de una red cableada, posterior a ello deberá ingresar la licencia de activación.

En el momento de registro la unidad computacional configurada, realizara una petición hacia un servidor alojado en la nube, el cual validara los permisos de acceso a funcionalidades de la licencia, almacenara el correo electrónico ingresado y retornara un mensaje codificado a la unidad computacional, quien a su vez interpretara dicho mensaje y de manera interna otorgara permisos para que el usuario pueda o no ver las funcionalidades configuradas, acorde al tipo de licencia ingresada.

Adicional a este proceso, el servidor alojado en la nube enviará un correo electrónico con un link de activación al usuario registrado, con el fin de validar que el correo, exista, este link de activación podrá ser usado una única vez y tendrá una duración máxima de un día para su activación.

Una vez el usuario recibe el correo electrónico y abre el enlace de activación, el servidor recibirá dicha información y marcará como valido el registro de dicha unidad computacional registrada y licenciada.

Posterior a ello la unidad computacional se reiniciará, al iniciar su sistema operativo enviará un correo electrónico, con la nueva IP obtenida de la interfaz de red bien sea por Wireless o por ethernet, según configuración

del usuario, a partir de ese punto el usuario deberá acceder a dicha IP a través de un navegador web, para acceder a las funcionalidades licenciadas.

De igual forma, de existir algún problema de conectividad, de existir un dispositivo de almacenamiento extraíble conectado en algún puerto USB disponible en la unidad computacional, al momento de iniciar, el HackInspector Creara un archivo llamado ip.txt con los datos de la IP asignada a la unidad.

Para evitar fraudes con las licencias, en el momento de registro, la unidad computacional envía al servidor alojado en la nube, una serie de valores adquiridos de las características propias de los componentes de hardware de la unidad computacional, como por ejemplo la dirección MAC de la tarjeta de red ethernet, dirección MAC de la tarjeta de red inalámbrica y tarjeta de Bluetooth.

Cada vez que el usuario quiera hacer uso de alguna funcionalidad, la unidad computacional (HackInspector) validará, si dicha licencia está asociada a las características de hardware con la cual fue registrada, a su vez que se halla validado el correo de activación y si tiene los permisos necesarios para poder hacer uso de dicha funcionalidad.

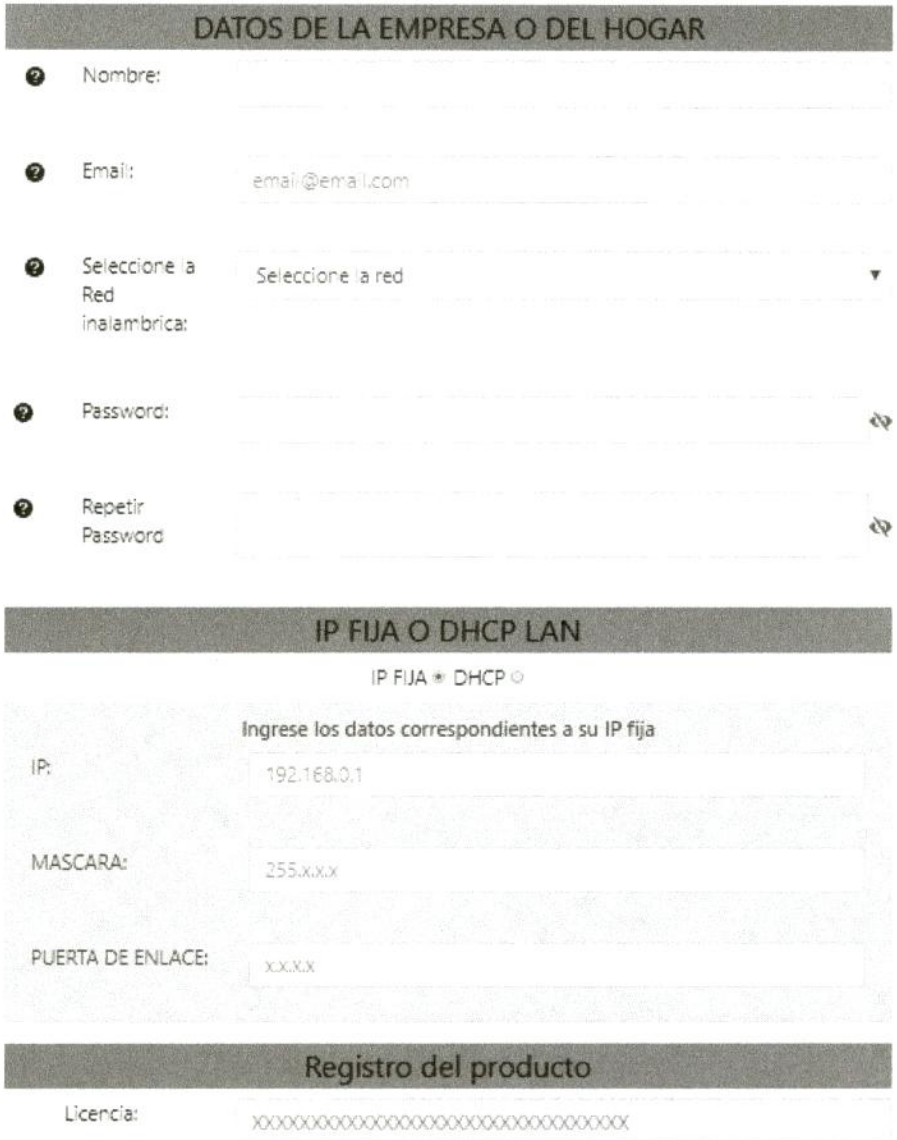


Imagen 2: Proceso de registro y activación de licencia.

- **Ejecución y/o programación de escaneos a aplicaciones web, captura de trafico de red para detección de amenazas en redes inalámbricas y búsqueda de vulnerabilidades de seguridad informática en los equipos conectados en la misma red que la unidad computacional configurada (HackInspector):**

  La unidad computacional fue configurada para realizar tres tipos de escaneos, haciendo uso de los componentes de red que la componen (tarjeta de red inalámbrica y tarjeta de red ethernet): escaneo de vulnerabilidades a la red cableada o inalámbrica a la cual está conectada, escaneo de vulnerabilidades a aplicaciones web y escaneo o monitoreo a red inalámbrica.

  Los escaneos de vulnerabilidades están orientados a detectar fallas de seguridad basadas en el OWASP TOP 10; Los escaneos pueden ser ejecutados de forma inmediata o de manera programada.

  Al terminar los escaneos configurados por el usuario a través de la interfaz web, la unidad computacional crea los reportes y los deja alojados en la sección reportes.

Imagen 3: Proceso de ejecución escaneo web

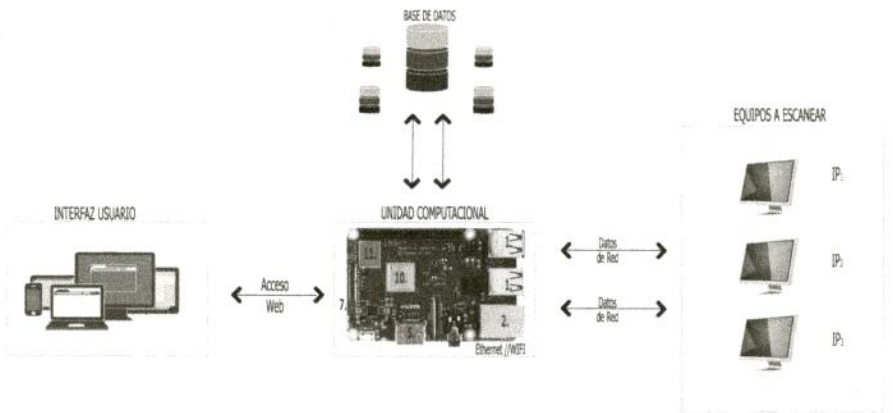


Imagen 4: Proceso de ejecución escaneo de red

Imagen 5: Proceso de ejecución monitoreo wifi

- **Descubrimiento y listado de equipos conectados en la red a analizar:**

  La unidad computacional configurada detecta que equipos están conectados en la misma red (haciendo uso de la interfaz Wireless (11) y ethernet (2)), los enlista de manera ordenada, permitiendo al usuario visualizar la información recolectada (nombre del equipo, dirección MAC e IP asociada al equipo) en la interfaz web.

  En esta funcionalidad el usuario, podrá, seleccionar que equipos son de confianza y crear una lista blanca, la unidad computacional configurada

monitoreará de manera periódica la red y de detectarse algún equipo conectado que no pertenezca a la lista blanca, generará un alertamiento vía correo electrónico notificando el incidente y generará un documento alojándolo en la sección de reportes.

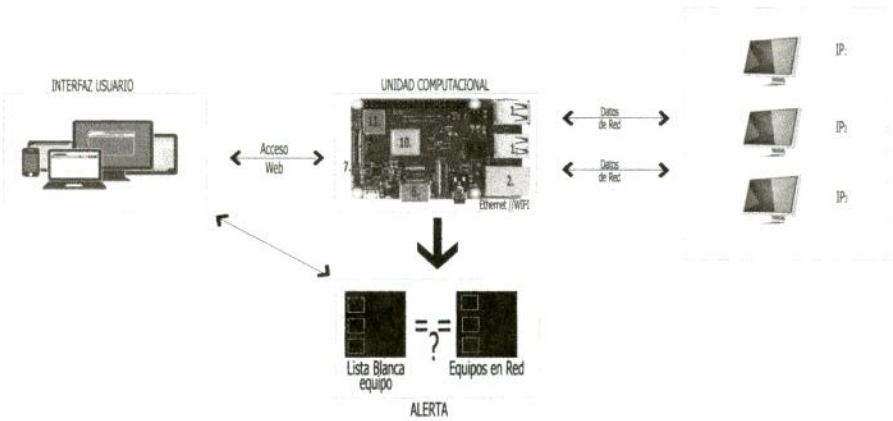


Imagen 6: Descubrimiento de equipos conectados en red.

- **Búsqueda y alertamiento de vulnerabilidades cero day, sobre los activos de información ingresados por el usuario.**

El HackInspector (Unidad computacional configurada), de manera periódica, realiza una consulta directa a través de petición GET a la URL de entidades de buenas prácticas o estándares internacionales (Por ejemplo, NIST), con el fin de extraer la información, almacenarla de manera local en la unidad computacional y mostrarla al usuario final, en diferentes idiomas haciendo uso de servicios públicos para traducción.

HackInspector (Unidad computacional configurada), realiza una consulta periódica a la página oficial de la NIST (NATIONAL VULNERABILITY DATABASE)(https://nvd.nist.gov/vuln), para detectar vulnerabilidades 0 day o de día cero, reportadas por la comunidad, correspondientes a la fecha en la cual se realiza la consulta, de existir vulnerabilidades reportadas, la

unidad computacional muestra en la sección vulns, las nuevas vulnerabilidades reportadas, en el idioma que seleccione el usuario, inicialmente Español e Inglés.

Como cada una de las vulnerabilidades reportadas está asociada a un activo Tecnológico, el usuario contará con un formulario, donde podrá ingresar los nombres de los activos tecnológicos presentes en su organización, empresa u hogar, de esta forma la unidad computacional comparará si existe una vulnerabilidad reportada de día cero que afecta a alguno de sus activos, y de ser así, enviara una notificación vía correo electrónico indicando que uno de los activos tecnológicos ingresados en el formulario cuenta con una vulnerabilidad, y en la sección vulns podrá ver el link que redirecciona hacia la NIST, donde se expone de manera detallada la información sobre la vulnerabilidad y como solventarla.

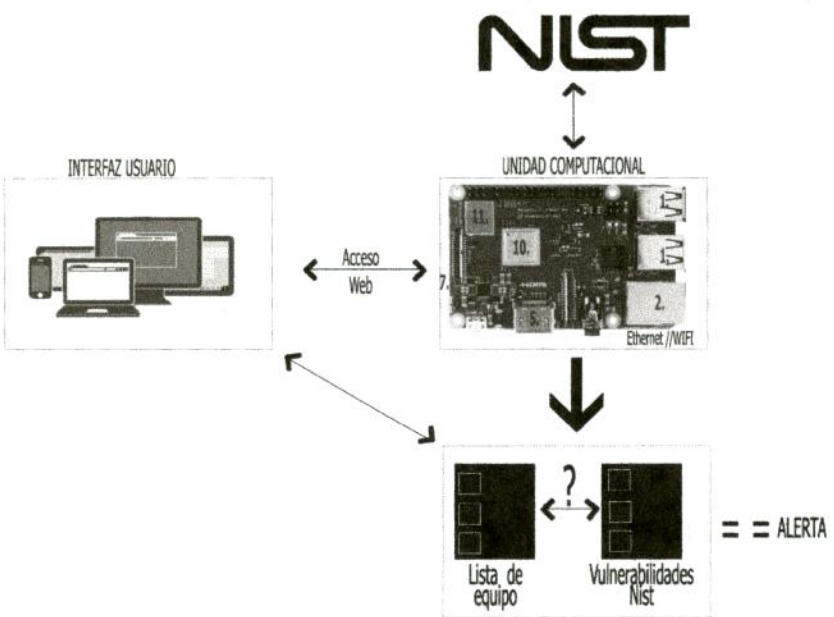


Imagen 7: Alertamientos de vulnerabilidades 0 day reportadas por la NIST

- **Funcionalidad de visualización de reportes:**

Cada vez que se ejecute un escaneo exitoso programado o ejecutado por el usuario, la unidad computacional, enviara un correo electrónico al usuario notificando el nombre del reporte generado y la finalización del escaneo.

En la sección de reportes, la unidad computacional, visualizara los reportes almacenados, que pueden ser de varios tipos:1. Reportes de escaneo de red,2. Reportes de escaneo WEB,3. Reporte de escaneo wifi,4. Reporte de equipos conectados en la red.

Los usuarios podrán descargar de manera local los informes, así como borrarlos de manera local de la unidad computacional, de igual forma, de existir un dispositivo de almacenamiento extraíble conectado en un puerto disponible USB, la unidad computacional guardara el reporte generado en la raíz del dispositivo.

Imagen 8: Visualización del área de reportes

- **Funcionalidad para gestión de activos:**

La unidad computacional fue configurada para incluir una funcionalidad para la gestión de activos, permite a los usuarios cargar sus activos tecnológicos, ordenarlos, asignarlos y clasificarlos acorde a las categorías expuestas en la iso27001.

De esta forma el usuario podrá centralizar de manera documental sus activos, de igual forma podrá exportarlos a formato compatible con Excel o importar una lista de activos ya existente al sistema.

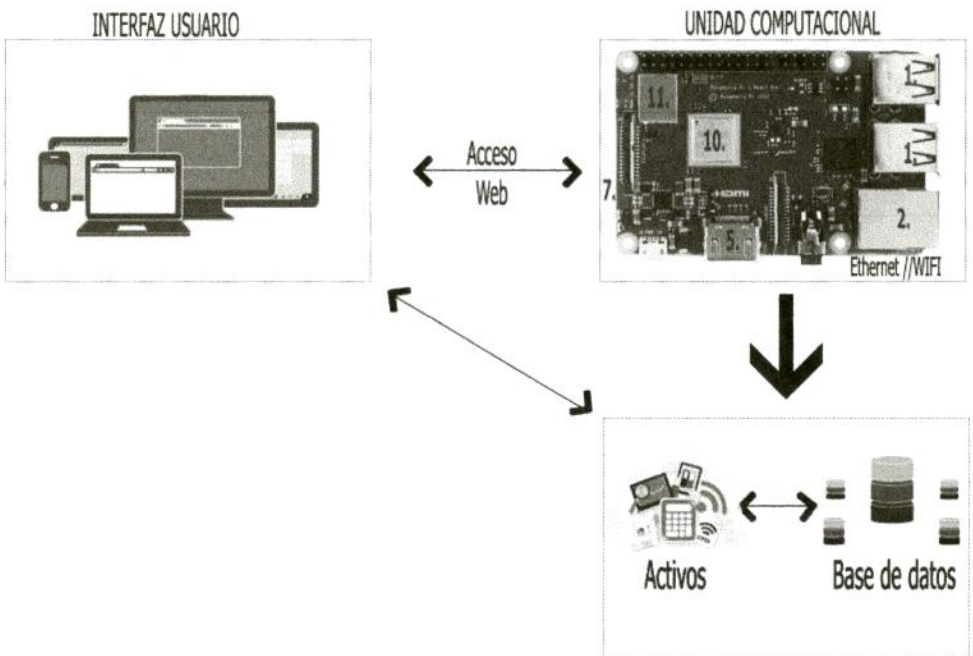


Imagen 9: funcionalidad gestión de activos.

- **Funcionalidad para la gestión de incidentes:**

El módulo de gestión de incidentes permite a los usuarios reportar incidentes de seguridad establecidos por la ISO27001, y asignar un responsable para el tratamiento de dicho incidente.

Al momento de reportar un incidente, la unidad computacional realiza dos acciones, la primera, enviar un correo electrónico a la persona registrada en la unidad computacional, con los datos del incidente y la segunda de manera segura y codificada, envía la información del incidente hacia un servidor en internet, en el cual se almacena dicha información, para posteriores análisis, estadísticas y mejoras en los servicios.

Solo el administrador de la unidad computacional podrá, eliminar los incidentes reportados, de igual forma podrá realizar una exportación de los incidentes registrados en la plataforma.

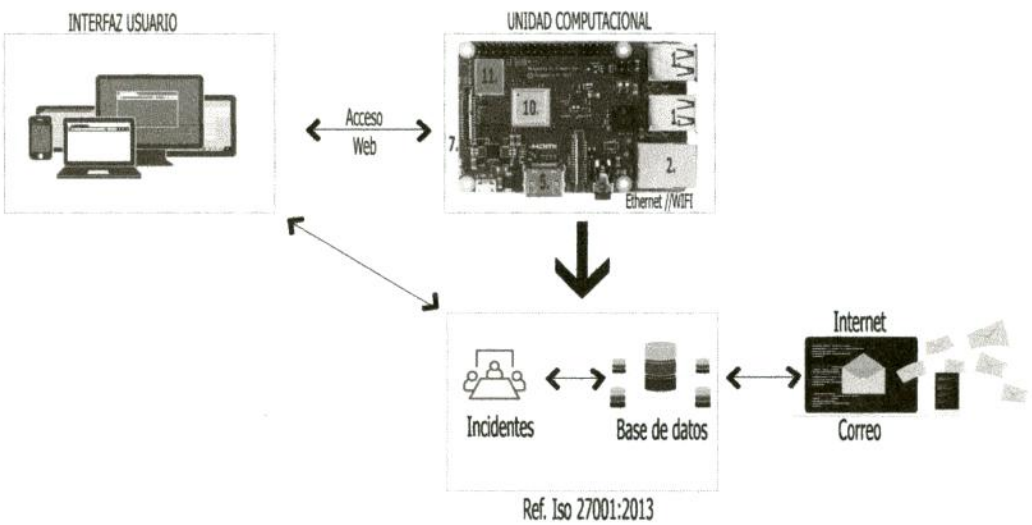


Imagen 10: módulo de gestión de incidentes.

- **Check list de normas internaciones o estándares:**

  La unidad computacional (Hack Inspector) cuenta con una funcionalidad configurada que permite a los usuarios realizar un autodiagnóstico de cualquier norma o estándar internacional, ya que es posible cargar el formulario con las preguntas de cumplimiento del estándar o buena práctica en la unidad computacional y el usuario las diligencia.

  En el caso puntual la unidad computacional en su primera versión oficial, integra el check list de la norma ISO27001 sin limitarse solo a dicha norma, el usuario puede ir diligenciando cada sección del check list y a su vez de manera automática la unidad computacional en la sección de visualización actualizaría las gráficas correspondientes de cumplimiento para que el usuario pueda generar presentaciones gerenciales de manera rápida y práctica.

  Cada vez que el usuario selecciona una pregunta de cumple o no cumple, la unidad computacional almacena de manera automática dicha respuesta en un base de datos contenida en la misma unidad, lo que le permite al usuario tomarse el tiempo que necesite para diligenciar el cuestionario.

  Por otra parte, la unida computacional puede generar un reporte gerencial del check list diligenciado por el usuario, el usuario puede seleccionar el idioma del reporte y exportarlo en formato pdf.

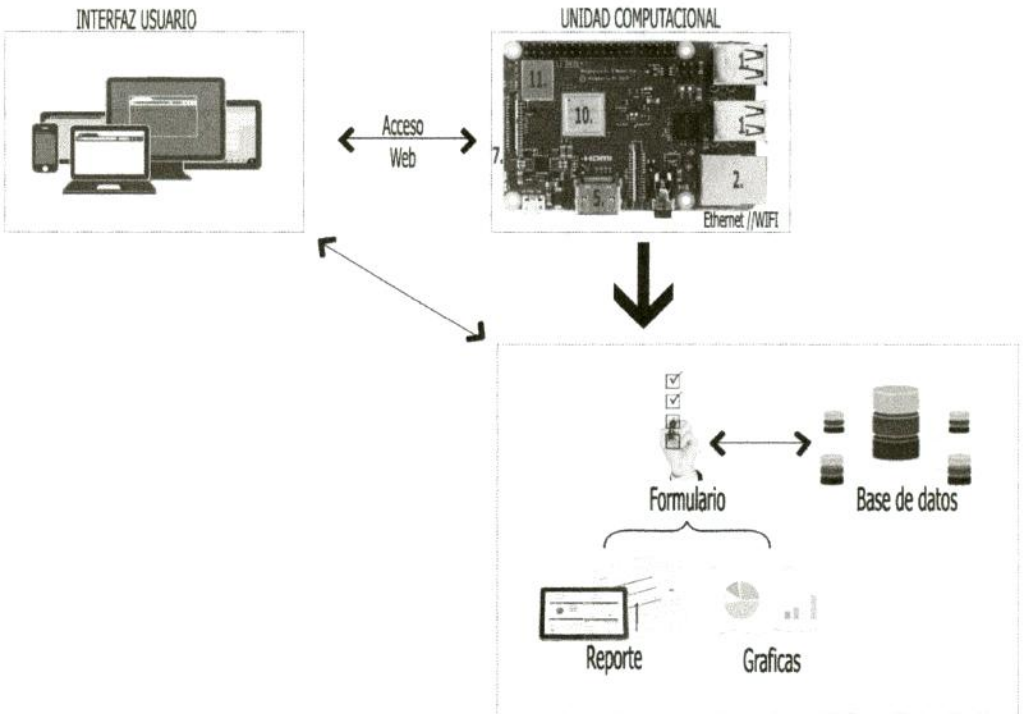


Imagen 11: Configuración modulo Autogestión.

- **Centralización de documentación:**

La unidad computacional configurada (HackInspector), permite a los usuarios transformar cualquier dispositivo de almacenamiento extraíble con puerto USB, en un repositorio de archivos que se pueden compartir en la red.

La unidad computacional configurada, monta en su sistema operativo los dispositivos conectados en alguna de las ranuras de USB que posee, lee los dispositivos y si encuentra dentro de este una carpeta con nombre Formatos, comparte su contenido con los usuarios en la sección formatos de la interfaz web.

De esta manera los usuarios podrían compartir cualquier contenido dentro de dicha carpeta y a su vez, compartirlo en la red, esta funcionalidad fue diseñada para que los usuarios creen un repositorio de formatos o capacitaciones acorde a la norma aplicable a la organización, en este caso ISO27001.

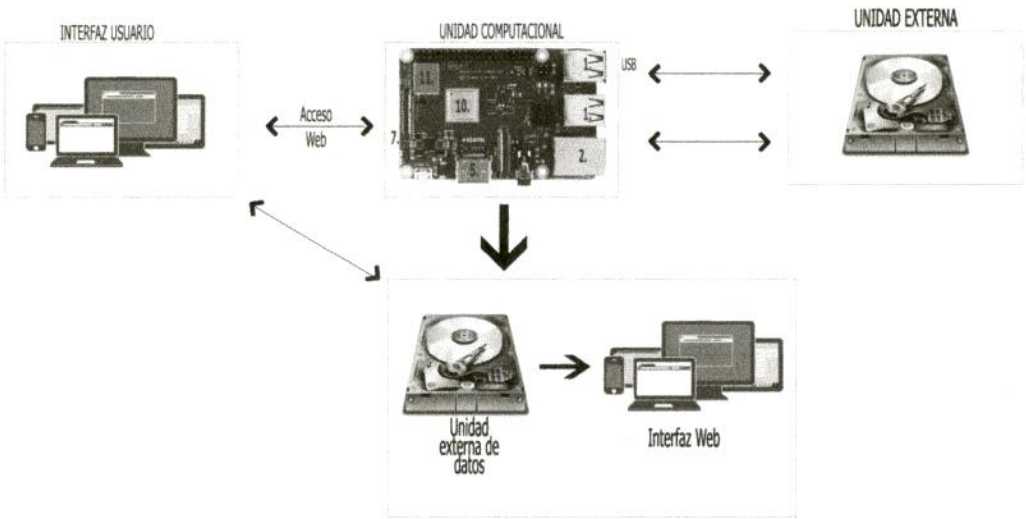


Imagen 12: módulo de Formatos.

- **Funcionalidad de seguridad para asignación de contraseñas o mecanismos de recuperación:**

  La unidad computacional cuenta con una interfaz web, la cual permite cambiar la contraseña que por efectos de fábrica será root, de igual forma el usuario podrá establecer mecanismos como frases de recuperación en caso de olvidarla.

  La contraseña se almacena en forma local en una base de datos MYSQL, en la cual se almacenan de forma segura a través de cifrado. En caso de que el usuario olvide su contraseña y sus frases de recuperación, podrá acceder a una url específica, la cual solicitara el correo electrónico con el cual se registró y la licencia de activación, ingresando estos datos, la unidad computacional configurada retornara la contraseña por defecto (root) para poder acceder.

Imagen 13: Visualización función cambio de contraseña.

Imagen 14: Visualización función Preguntas de Seguridad.

- **Funcionalidad para la gestión de usuarios:**

El administrador de la unidad computacional configurada, podrá crear roles y perfiles de usuarios, podrá definir usuarios, sus contraseñas y los permisos que estos tendrán dentro de la plataforma, de esta manera, el administrador podrá definir si un usuario tiene acceso solo a escaneos, por ejemplo, o si otro usuario tendrá acceso a las funcionalidades completas del dispositivo.

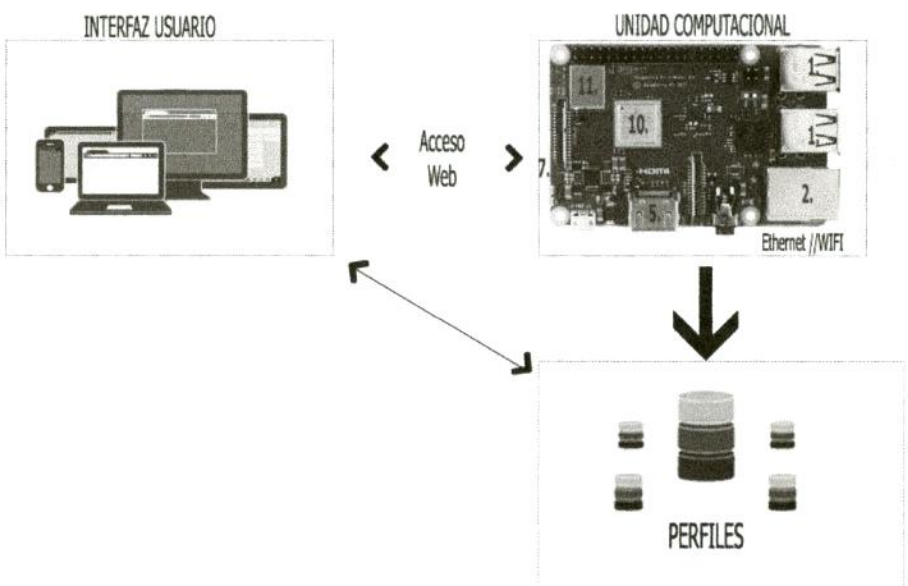


Imagen 15: Gestión de usuarios.

- **Funcionalidad para adicionar nuevas funcionalidades:**

  La unidad computacional (Hack Inspector) es escalable, lo cual le permite adicionar o quitar funcionalidades, para ello se implementó una funcionalidad de Upgrade, esta funcionalidad solicitara al usuario que cargue al sistema operativo un archivo .rar a través de la interfaz web.

  Este archivo .rar al ser cargado en la unidad computacional, adicionará o eliminará funcionalidades, luego de ser cargado la unidad computacional se reinicia, y al iniciar el usuario podrá ver las nuevas funcionalidades implementadas.

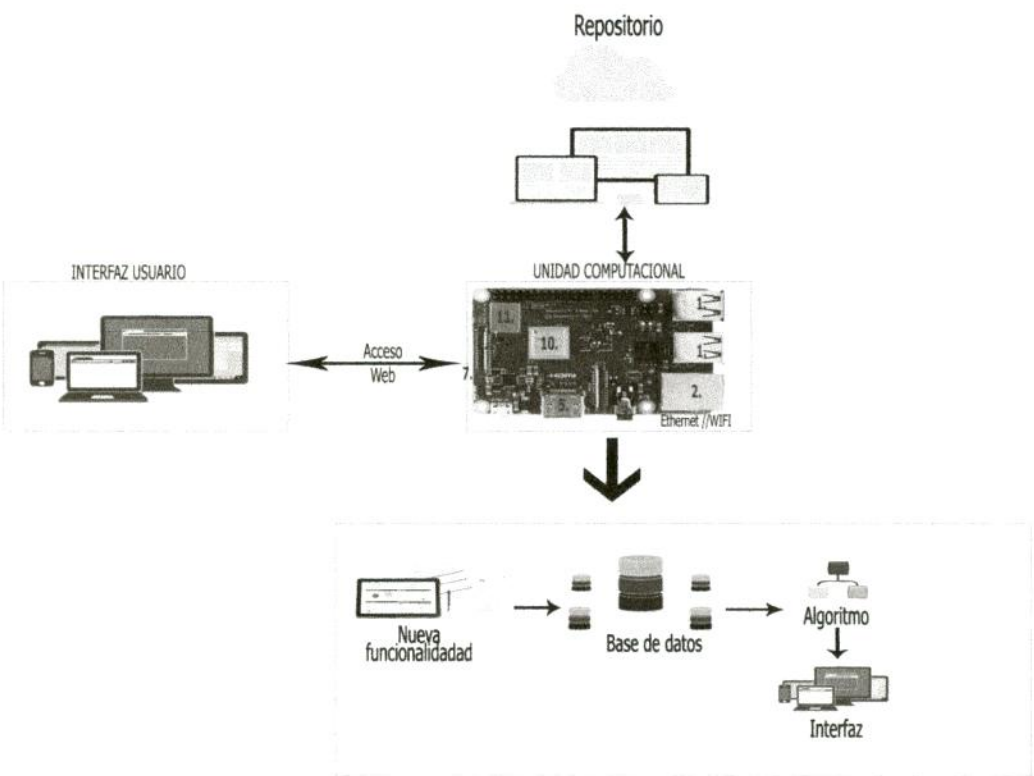
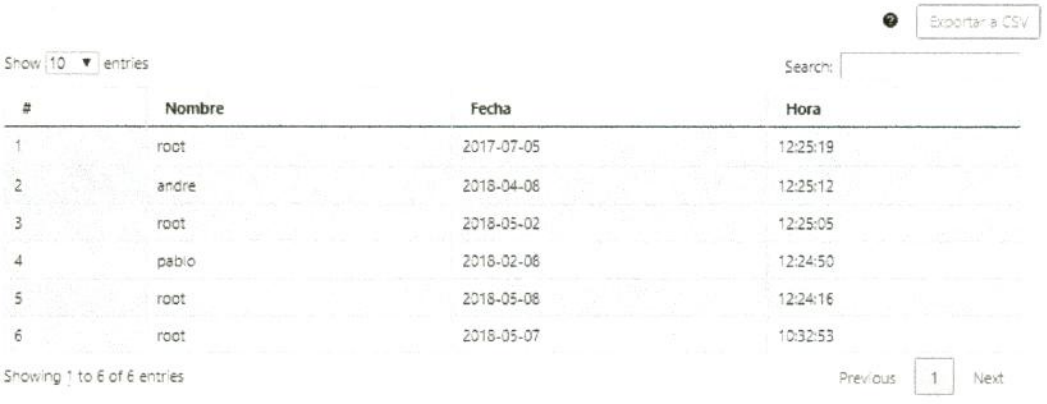


Imagen 16: Visualización función Upgrade

- **Registro de logs de auditorías:**

  La unidad computacional configurada, le permite al usuario administrador, acceder a una funcionalidad de logs, esta función muestra los últimos accesos de los usuarios a la plataforma, funcionalidad que permite llevar un control o auditoria sobre los usuarios registrados.



Exportar a CSV

Show 10 entries Search:

#	Nombre	Fecha	Hora
1	root	2017-07-05	12:25:19
2	andre	2018-04-06	12:25:12
3	root	2018-05-02	12:25:05
4	pablo	2018-02-06	12:24:50
5	root	2018-05-06	12:24:16
6	root	2018-05-07	10:32:53

Showing 1 to 6 of 6 entries Previous 1 Next

Imagen 17: Visualización función panel visor de logs, los datos expuestos en la imagen son ficticios con el fin de ilustrar la funcionalidad.

- **Funcionalidad de cambio de idioma:**

  La unidad computacional se configura para que sea una plataforma multilenguaje, lo que permite seleccionar al usuario el lenguaje de la plataforma, siendo estos por defecto el inglés y el español.

Imagen 18: Visualización función cambio de idioma, los datos expuestos en la imagen son ficticios con el fin de ilustrar la funcionalidad.

- **Adquisición de data**

  La unidad computacional fue configurada para que, a ciertas horas del día, envié a través de internet información generada por el usuario o por los

escaneos, con el fin de crear un repositorio de información para analizarla y/o mejorar las configuraciones realizadas a la unidad computacional.

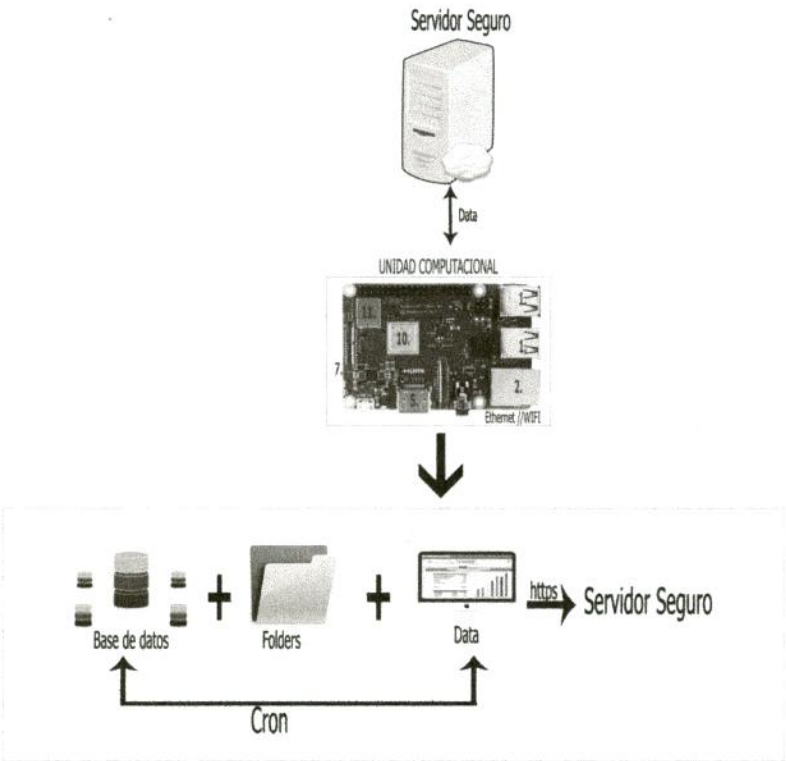


Imagen 19: Adquisición de data

- **Alertamiento Defacement**

Un defacement hace alusión a la manipulación no autorizada de la parte visual o grafica de una página web por parte de personas mal intencionadas o ciber delincuentes.

La unidad computacional (HackInspector) se configuro con el fin de poder monitorear páginas web y generar alertas de posibles cambios sobre las mismas. Para ello la unidad computacional en primera instancia recibe a través de la interfaz de usuario los dominios o páginas web a monitorear, posterior a ello valida que dichos dominios si existan o se encuentran activos, de ser así, realiza una captura de imagen de la página y la almacena de forma local, de manera paralela almacena el código html del

dominio, con estos datos, cada x periodo de tiempo la unidad computacional podrá repetir el proceso y comparar si existen cambios en las páginas, de existir algún cambio, notifica mediante correo electrónico al usuario, para que tome las medidas del caso.

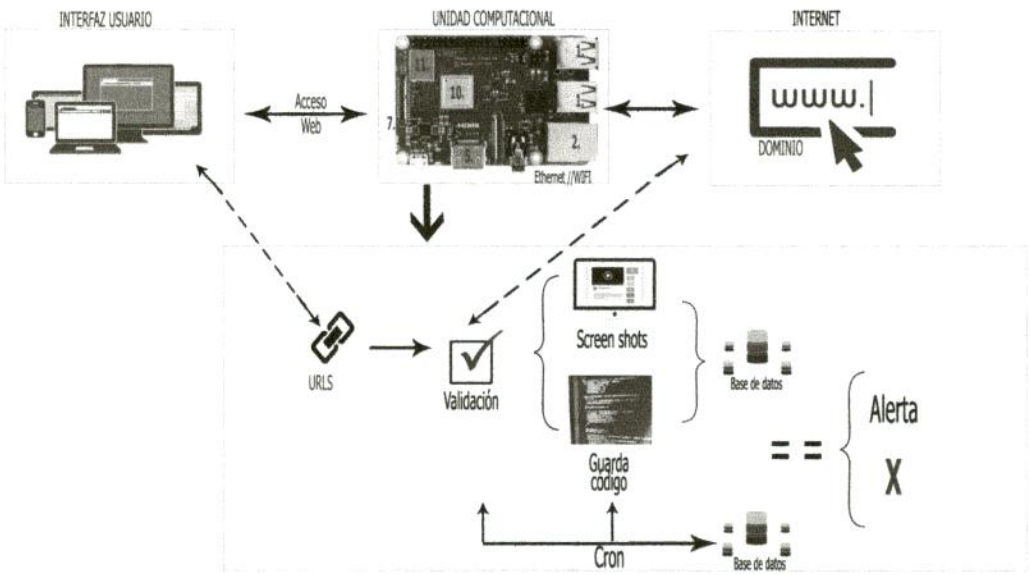


Imagen 20: Alerta Defacement