

UNIVERSIDAD CATÓLICA BOLIVIANA “SAN PABLO”

UNIDAD ACADÉMICA REGIONAL COCHABAMBA

Departamento de Ciencias Exactas e Ingeniería

Carrera de Ingeniería de Sistemas



Plan de Contingencia del Ministerio de Energías

Proyecto Final de la Materia de Seguridad de Sistemas

Julia Valentina Gutiérrez Munzón

Cochabamba – Bolivia

Junio de 2019

ÍNDICE GENERAL

INTRODUCCIÓN	1
1. ANTECEDENTES.....	1
2. PROBLEMA	5
3. OBJETIVOS.....	5
4. MARCO PRÁCTICO.....	5
4.1. Análisis de riesgos del Ministerio de Energías	5
4.1.1. Teoría del análisis de riesgos.....	5
4.1.2. Aplicación de la metodología de análisis de riesgos.....	6
4.2. Diseñar una red segura para el Ministerio de Energías	7
4.2.1. Teoría de redes, componentes de seguridad, IDS, IPS, Firewalls	7
4.2.2. Diseño de red segura del Ministerio de Energías	8
4.3. Elaborar política de seguridad de la infraestructura crítica para el Ministerio de Energías.....	9
4.3.1. Elaboración de la política de seguridad.....	10
4.4. Implementar herramientas de pruebas de seguridad con Python: Escalado de privilegios.....	11
4.4.1. Implementación.....	11
4.5. Realizar pruebas de seguridad a servidores web	12
4.5.1. Pruebas de seguridad.....	12
5. RESULTADOS	14
6. CONCLUSIONES Y RECOMENDACIONES.....	14
BIBLIOGRAFÍA	15
Anexo 1.....	1

Anexo 2.....	2
Anexo 3.....	2
Anexo 4.....	7
Anexo 5.....	8

ÍNDICE DE FIGURAS

Figura 1 Organigrama del Ministerio de Energías.....	1
Figura 2 Mapa de procesos	4
Figura 3 Principales riesgos detectados.	7
Figura 4 Matriz de riesgos	7
Figura 5 Topología de red.....	9
Figura 6 Monitor de procesos	12
Figura 7 Análisis con OWASP	13
Figura 8 Resultado del Análisis con OWASP	13

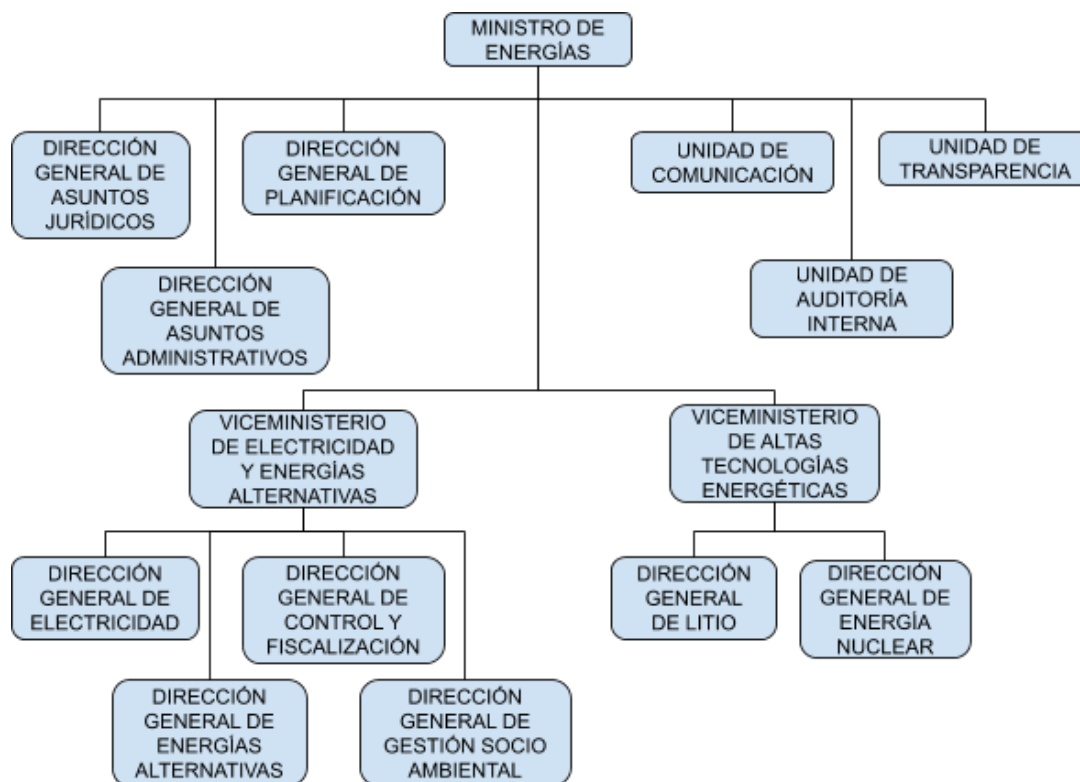
INTRODUCCIÓN

El Suministro de Energía es una infraestructura crítica básica. Esta infraestructura es capaz de producir y distribuir energía, en especial eléctrica a todo el territorio nacional. Es importante que los recursos energéticos estén disponibles en todo momento, para satisfacer las necesidades de alimentación, vivienda, educación, salud, entretenimiento y otros.

1. ANTECEDENTES

En Bolivia la institución encargada de proveer energía a nivel nacional es el Ministerio de Energías. Este ministerio está organizado en direcciones, unidades y viceministerios.

Figura 1 Organigrama del Ministerio de Energías



Fuente: Elaboración propia 2019

El ministerio posee 8 dependencias directas que tienen las siguientes funciones [1]:

- **Unidad de Comunicación Social**

Asesorar y apoyar al ministerio de hidrocarburos y energía, en la imagen institucional y la generación de información externa sobre el cumplimiento de objetivos.

- **Unidad de Auditoría Interna**

Evaluar las acciones realizadas por el ministerio de hidrocarburos y energía en el marco de lo establecido en la ley 1178.

- **Unidad de Transparencia**

Llevar adelante procesos de transparentación dentro del ministerio de hidrocarburos y energía y sus entidades bajo tuición, ejecutando acciones preventivas y correctivas a favor de los intereses del estado boliviano con honestidad e idoneidad en aplicación a la normativa que rige al estado plurinacional, instituidas en la constitución política del estado y la normativa vigente, bajo los lineamientos de transparencia, lucha preventiva contra la corrupción, normativización y participación ciudadana y control social.

- **Dirección General de Planificación**

Orientar y coordinar la toma de decisiones y las acciones del ministerio de hidrocarburos y energía en el corto, mediano y largo plazo.

- **Dirección Asuntos Administrativos**

Administrar los recursos humanos, económicos y financieros del ministerio de hidrocarburos y energía bajo los principios establecidos en la ley 1178.

- **Dirección Asuntos Jurídicos**

Prestar asesoramiento jurídico especializado al ministro, viceministros y demás componentes de la estructura central del ministerio de manera eficaz y eficiente.

- **Viceministerio de Electricidad y Energías Alternativas**

Proponer políticas para el sector de electricidad y el desarrollo de aplicación de energías alternativas convencionales y no convencionales en el marco de la CPE, establecer las directrices para la planificación del desarrollo del sector en el mediano y largo plazo y velar el cumplimiento de la normativa vigente en el sector de electricidad. [2]

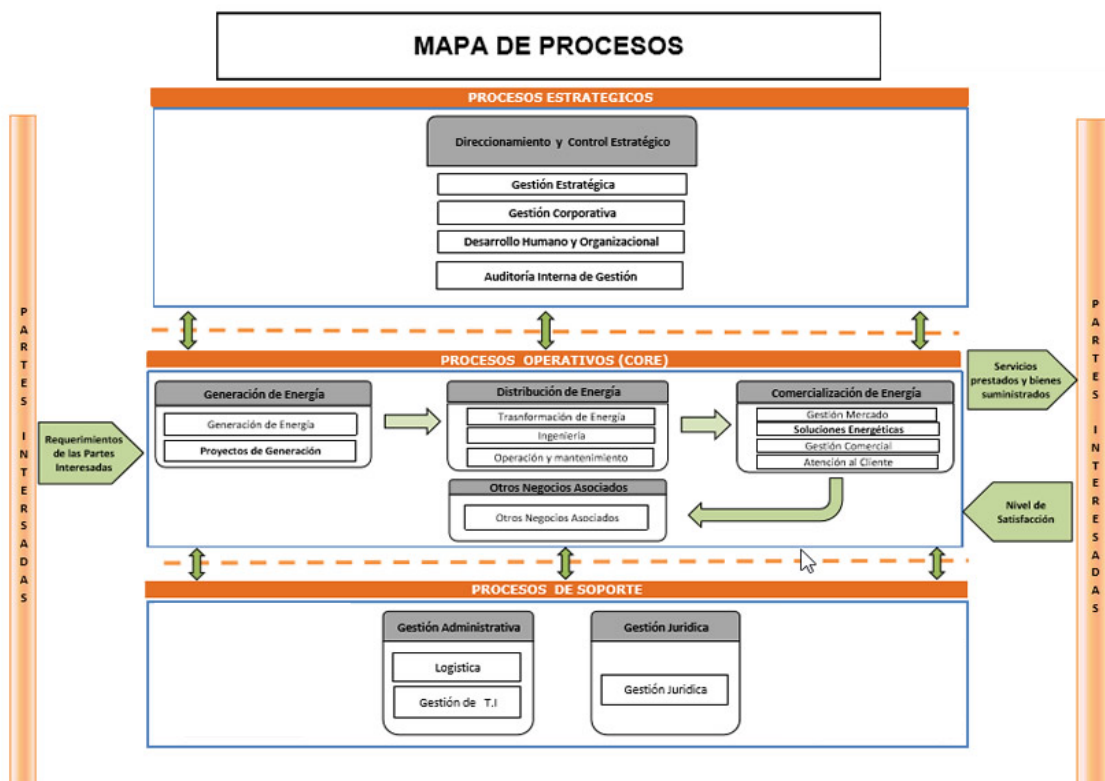
- **Viceministerio de Altas Tecnologías Energéticas**

Tiene la función de planificar, proponer, evaluar, definir y establecer políticas y lineamientos para el sector energético, coordinando con los viceministerios respectivos y supervisando a todas las entidades del sector energético y bajo su tuición, orientadas a lograr la ejecución de programas y proyectos de investigación y aplicación energética velando por el uso eficiente de nuestros recursos energéticos y el cumplimiento de la política y normativa ambiental del sector energético. [2]

A su vez los 2 viceministerios, están organizados en otras direcciones que le permiten trabajar de mejor manera. Esto nos lleva a un total de 14 dependencias de la oficina principal que es la del ministro con el cual sumarían 15.

Los objetivos estratégicos del ministerio de energías definen sus alineamientos y servicios. (ver anexo 1) De igual manera el mapa de procesos muestra los principales procesos estratégicos, operativos y de soporte. (Figura 2)

Figura 2 Mapa de procesos



Fuente: [3]

Los activos reconocidos en esta organización son los siguientes:

- 9 ambientes
- 15 computadoras
- 9 routers
- 9 servidores
- 15 antivirus
- 15 paquetes de *Office*
- 15 impresoras

- 15 escritorios

2. PROBLEMA

La falta de información y carencia de mecanismos de seguridad en el Ministerio de Energías respecto a políticas de seguridad y planes de contingencia, conllevan a que la misma se exponga a posibles riesgos que pueden afectar los pilares de la seguridad, en especial la disponibilidad del servicio.

3. OBJETIVOS

3.1. Objetivo General

Desarrollar un plan de continuidad de negocios del Ministerio de Energías de Bolivia.

3.2. Objetivos Específicos

- Análisis de riesgos del Ministerio de Energías
- Diseñar una red segura para el Ministerio de Energías
- Elaborar políticas de seguridad del Ministerio de Energías y un plan de contingencia
- Implementar herramientas de pruebas de seguridad con *Python*: Escalado de privilegios
- Realizar pruebas de seguridad a su página web

4. MARCO PRÁCTICO

4.1. Análisis de riesgos del Ministerio de Energías

4.1.1. Teoría del análisis de riesgos

El análisis de riesgos es la herramienta a través de la cual se puede obtener una visión clara y priorizada de los riesgos a los que se enfrenta una entidad: tiene como propósito identificar los principales riesgos a los que una entidad está expuesta, ya sean desastres

naturales, fallos en infraestructura o riesgos introducidos por el propio personal. En este sentido pretende identificar los riesgos más significativos que pueden afectar a la operativa de la entidad y priorizar medidas a implantar para minimizar la probabilidad de materialización de dichos riesgos o el impacto en caso de materializarse. [4]

El análisis de los riesgos determinará cuáles son los factores de riesgo que potencialmente tendrían un mayor efecto sobre nuestro proyecto y, por lo tanto, deben ser gestionados por el emprendedor con especial atención. [5]

Una de las metodologías más usadas para realizar el análisis de riesgos es la metodología MAGERIT.

MAGERIT es la metodología de análisis y gestión de riesgos desarrollada por un equipo del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales del consejo Superior de Administración Electrónico. El nombre de MAGERIT viene de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las administraciones públicas. No obstante también proporciona un marco válido para el desarrollo de análisis de riesgos en entidades privadas. [4]

4.1.2. Aplicación de la metodología de análisis de riesgos

La metodología usada para el análisis de riesgos fue la metodología MAGERIT (ver anexo 2).

Primero se identificó los activos del Ministerio de Energías, viendo a qué tipo pertenecen. Luego, se identificó las posibles amenazas para los mismos, tomando en cuenta la probabilidad de ocurrencia y el impacto que puede tener en la organización. A través del impacto y probabilidad se encontró el riesgo. El riesgo es producto de la probabilidad por el impacto. La puntuación de 1 es la más baja y la 3 es la más alta (ver anexo 3).

Los activos que mayor riesgo tienen son los servidores y PCs.

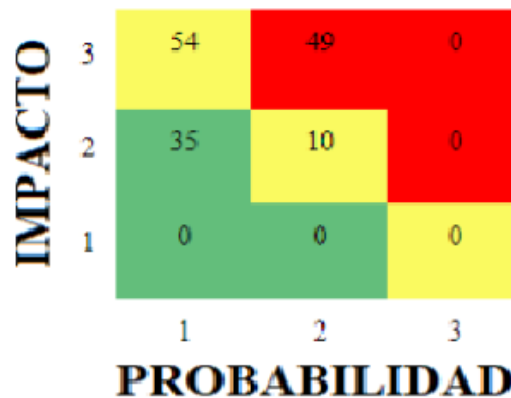
Figura 3 Principales riesgos detectados.

ACTIVO	TIPO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
Servidor 01 (Despacho Ministro)	Hardware	Denegación de servicio	2	3	6
PC 01(Despacho Ministro)	Hardware	Infección por virus	2	3	6

Fuente: Elaboración propia 2019

Con el análisis realizado se logró obtener los activos con su respectivo riesgo y en base a eso se realizó la matriz de riesgos.

Figura 4 Matriz de riesgos



Fuente: Elaboración propia 2019

4.2. Diseñar una red segura para el Ministerio de Energías

4.2.1. Teoría de redes, componentes de seguridad, IDS, IPS, Firewalls

Al momento de diseñar la topología de red para el Ministerio de Energías se consideró 3 elementos que colaboran con la seguridad de la red. Estos son:

- *Firewall*: es un sistema diseñado para prevenir el acceso no autorizado hacia o desde una red privada. Se puede implementar en forma de *hardware*, de software o en una combinación de ambos. Los cortafuegos impiden que los usuarios no autorizados accedan a redes privadas conectadas a Internet, especialmente a intranets. Todos los mensajes que entran o salen desde tu red local pasan por él, para que examine cada mensaje y bloquee los que no cumplan los criterios de seguridad especificados. [6]
- Sistema de detección de intrusos (IDS): un IDS está diseñado para analizar paquetes completos, tanto de encabezado como de carga útil, en busca de eventos conocidos. Cuando se detecta un evento conocido, se genera un mensaje de registro que detalla el evento. El IDS contiene una base de datos de firmas de ataques conocidas y compara el tráfico entrante con la base de datos. Si se detecta un ataque, entonces el IDS informa del ataque. La función principal de un producto IDS es advertirle sobre actividades sospechosas que tienen lugar, pero no prevenirlas. [7]
- Sistema de prevención de intrusiones (IPS): el IPS se encuentra entre su *firewall* y el resto de su red. Porque puede impedir que el tráfico sospechoso llegue al resto de la red. El IPS se encarga de supervisar los paquetes entrantes y para qué se utilizan realmente antes de decidir dejar los paquetes en la red. Un IPS inspeccionará el contenido de la solicitud y podrá eliminar, alertar o posiblemente limpiar una solicitud de red maliciosa basada en ese contenido. La determinación de lo que es malicioso se basa en el análisis de comportamiento o mediante el uso de firmas. [7]

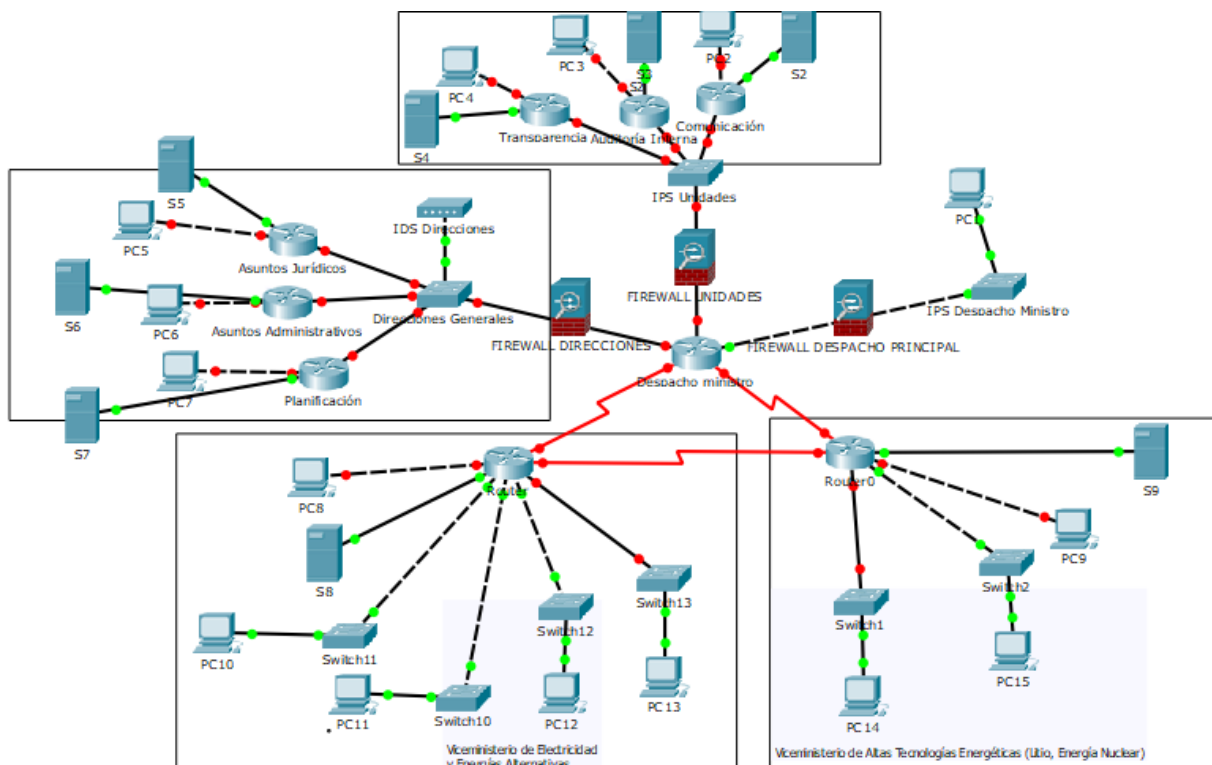
4.2.2. Diseño de red segura del Ministerio de Energías

Al diseñar la red, se consideró la cantidad de PCs, *routers* y servidores tomados en cuenta anteriormente. Eso fue punto de partida para el inicio de la topología. A su vez, se consideró el organigrama del Ministerio de Energías, para tomar en cuenta las subredes de la misma.

Se usa *firewalls* para que los usuarios no autorizados no puedan acceder a las Direcciones Generales, Unidades y la Oficina del Ministro. Es importante que se tenga bastante control

a estas áreas, en especial por las Unidades de Transparencia y de Auditoría que tienen información que debe ser resguardada.

Figura 5 Topología de red



Fuente: Elaboración propia 2019

4.3. Elaborar política de seguridad de la infraestructura crítica para el Ministerio de Energías

La política de seguridad es un conjunto de reglas aplicadas a las actividades del sistema y a los recursos de comunicación pertenecientes a una organización. Estas reglas abarcan áreas como la seguridad física, personal, administrativa y de la red.

A su vez, la políticas de seguridad proporcionan una base para la planificación de la seguridad al diseñar nuevas aplicaciones o ampliar la red actual.

4.3.1. Elaboración de la política de seguridad

Al ver los resultados que nos ofrece el análisis de riesgos, se observa que es necesario emitir políticas de seguridad para los siguientes activos:

- Servidores
- PCs

Servidores

- Todo servidor dentro de la organización deberá tener un *backup* (copia de respaldo) que pueda facilitar el acceso a la información en caso de denegación del servicio.
- El mantenimiento de los servidores se realizará de forma constante para evitar problemas con los mismos y será realizado únicamente por personal autorizado.

PCs

- Toda PC dentro de la organización debe de tener el software necesario para las tareas encargadas y contar con modalidades de protección como ser antivirus.
- Toda PC de la organización debe de ser usada únicamente para desempeñar y cumplir las tareas de la organización no con otros fines.
- La protección física de cada PC estará a cargo de la persona a quién se le asignó. En caso de presentarse algún problema con el dispositivo, este deberá ser reportado a las autoridades correspondientes.
- Cada equipo debe ser mantenido de forma constante, además debe de recibir las actualizaciones de software necesarias.
- En caso de que un equipo sea infectado por un virus, este debe ser desconectado de la red, para no propagar el mismo. Posteriormente se deben realizar las acciones necesarias como de reinstalar el SO o borrar los archivos infectados, según la gravedad.

4.4. Implementar herramientas de pruebas de seguridad con *Python*: Escalado de privilegios

El escalado de privilegios es el acto de explotación de un error, fallo de diseño o configuración de una aplicación, dentro de un sistema operativo o aplicación, para conseguir acceso a recursos del sistema que normalmente están protegidos frente a una aplicación o usuario. [8]

Se usa los procesos de alto privilegio que manejan archivos o ejecutan binarios para de esa manera se pueda crear una interfaz flexible que monitorea la creación de nuevos procesos. A partir de esos procesos, se verá la ruta de archivos, los usuarios y sus privilegios.

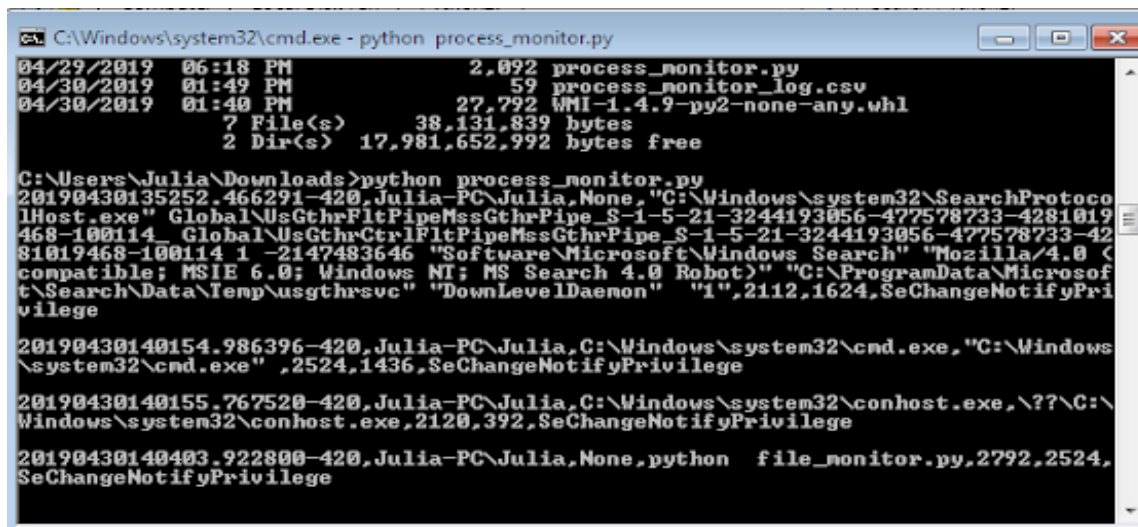
4.4.1. Implementación

Es importante el control de privilegios en esta organización para limitar a los usuarios a no acceder a recursos no autorizados y ver las actividades que realizan.

Primero se creó el programa de monitor de procesos en lenguaje *python*, una vez creado el programa se lo ejecuta y mostrará en consola todas las actividades que realizan los usuarios en tiempo real.

Como se puede observar, en la consola, se ve el registro de todas las actividades realizadas en el sistema.

Figura 6 Monitor de procesos



```
C:\Windows\system32\cmd.exe - python process_monitor.py
04/29/2019 06:18 PM 2,092 process_monitor.py
04/30/2019 01:49 PM 59 process_monitor_log.csv
04/30/2019 01:40 PM 27,792 WMI-1.4.9-py2-none-any.whl
7 File(s) 38,131,839 bytes
2 Dir(s) 17,981,652,992 bytes free

C:\Users\Julia\Downloads>python process_monitor.py
20190430135252.466291-420,Julia-PC\Julia,None,"C:\Windows\system32\SearchProtocol
Host.exe" Global\UsGthrFltPipeMsgGthrPipe_S-1-5-21-3244193056-477578733-4281019
468-100114 Global\UsGthrCtrlFltPipeMsgGthrPipe_S-1-5-21-3244193056-477578733-42
81019468-100114 1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (
compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)" "C:\ProgramData\Microsof
t\Search\Data\Temp\usgthrsvc" "DownLevelDaemon" "1",2112,1624,SeChangeNotifyPri
vilege

20190430140154.986396-420,Julia-PC\Julia,C:\Windows\system32\cmd.exe,"C:\Windows
\system32\cmd.exe",2524,1436,SeChangeNotifyPrivilege

20190430140155.767520-420,Julia-PC\Julia,C:\Windows\system32\conhost.exe,??C:\
Windows\system32\conhost.exe,2120,392,SeChangeNotifyPrivilege

20190430140403.922800-420,Julia-PC\Julia,None,python file_monitor.py,2792,2524,
SeChangeNotifyPrivilege
```

Fuente: Elaboración propia 2019

4.5. Realizar pruebas de seguridad a servidores web

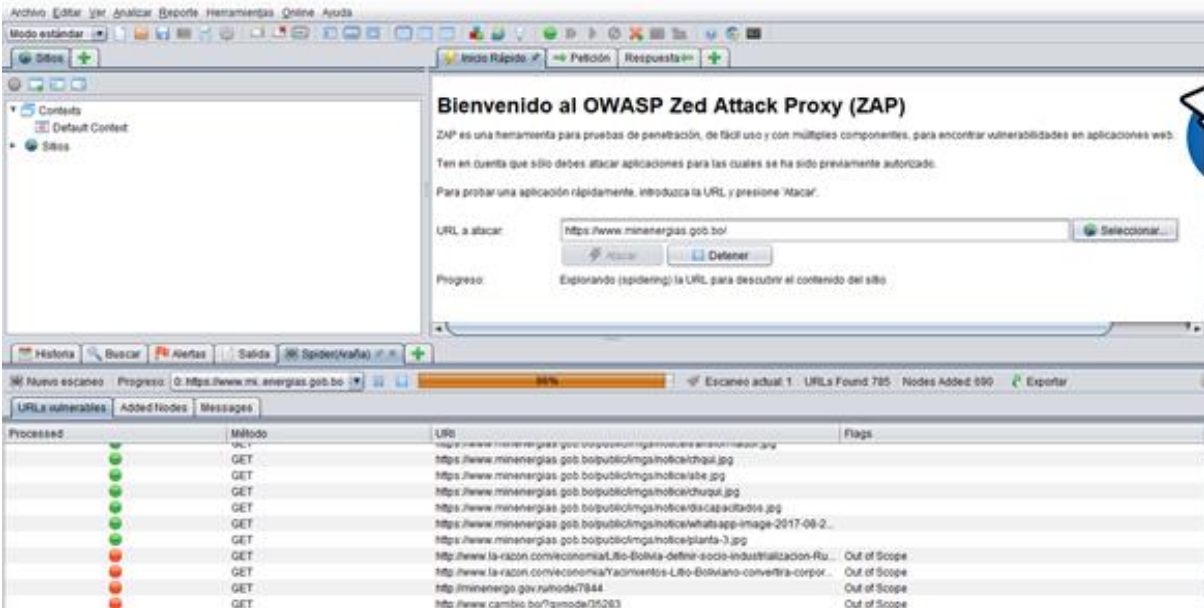
La realización de pruebas de seguridad a servidores web es una tarea de suma importancia para mantener seguros a nuestros servidores. Esta tarea nos ayuda a evitar el gran número de ciberataques que se pueden sufrir.

A su vez, si existe mayor cuidado del servidor, se garantizará que el servicio este siempre disponible.

4.5.1. Pruebas de seguridad

Se realizó un análisis de vulnerabilidades con la herramienta OWASP a la página del · <https://www.minenergias.gob.bo/>.

Figura 7 Análisis con OWASP



Fuente: Elaboración propia 2019

Al realizar el análisis, se obtuvo como resultado 5 posibles alertas de vulnerabilidad en la página web analizada con un riesgo mínimo. Sin embargo, a pesar de que son riesgos bajos pueden ocasionar problemas posteriores.

Figura 8 Resultado del Análisis con OWASP

Risk Level	Number of Alerts
High	0
Medium	0
Low	5
Informational	0

Fuente: Elaboración propia 2019

Es necesario corregir estas alertas (ver anexo 4) para que nuestro servidor sea seguro y no exista el riesgo de exponernos a algún delito informático como por ejemplo el *sniffing*.

5. RESULTADOS

- El análisis de riesgos permitió identificar los activos sensibles a riesgos de la organización.
- El diseño de redes nos permitió identificar la topología que se debe tener para poder resguardar la información.
- La política de seguridad nos da medidas para el mejor cuidado de los activos dentro de la organización.
- Construir herramientas como un monitor de proceso, usando el escalado de privilegios, nos ayuda a controlar mejor las tareas realizadas y así poder ver ciertas amenazas presentadas.
- Al realizar pruebas de seguridad a su página web podemos identificar las vulnerabilidades existentes y sus posibles soluciones.

6. CONCLUSIONES Y RECOMENDACIONES

Al ser una organización establecida a nivel nacional, el Ministerio de Energías, es necesario que considere ciertos aspectos para prevenir problemas de seguridad, en especial velar por la Disponibilidad de su servicio, ya que este es indispensable en la vida diaria de las personas.

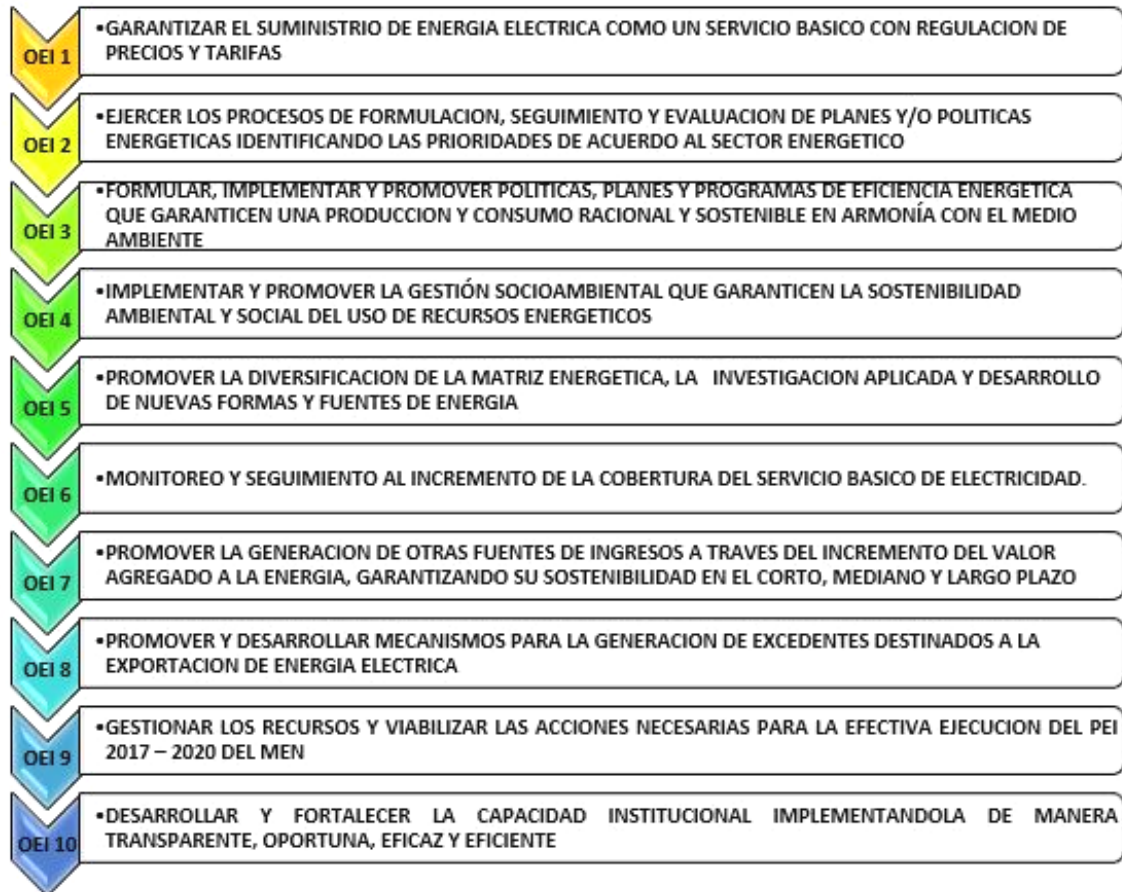
BIBLIOGRAFÍA

- [1] MINISTERIO DE ENERGÍAS (s.f). Manual de Organización y Funciones del Ministerio de Energías. La Paz: s.e.
- [2] MINISTERIO DE ENERGÍAS (s.f). “Viceministerios del Ministerio de Energías de Bolivia”. En: < <https://www.minenergias.gob.bo> > , (fecha de consulta 4/06/2019).
- [3] EEP (s.f). “Mapa de Procesos”. En: <<http://www.eep.com.co/la-empresa/iso-9001/mapa-de-procesos>> , (fecha de consulta 28/05/2019).
- [4] HUERTA, Antonio (2012). “Introducción al análisis de riesgos – Metodologías (I)”. En: <<https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i>>, (fecha de consulta 8/06/2019).
- [5] COMUNIDAD DE MADRID (s.f). “Análisis y cuantificación del Riesgo”. En: <http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/4AnalisisycuantificaciondelRiesgo%28AR%29_es.pdf>, (fecha de consulta 10/06/2019).
- [6] PANDASECURITY (2019). “¿Qué es un Firewall?”. En: <<https://www.pandasecurity.com/spain/mediacenter/seguridad/que-es-un-firewall/>>, (fecha de consulta 30/05/2019).
- [7] GIMÉNEZ Y GÓMEZ (2008). “Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral”. En: <http://www.adminso.es/images/1/1d/PFC_marisa.pdf>, (fecha de consulta 2/06/2019).
- [8] MEJOR ANTIVIRUS (s.f). “Escalado de privilegios”. En: < <http://www.mejor-antivirus.es/terminologia-informatica/escalado-de-privilegios.html> >, (fecha de consulta 4/06/2019).

[9] RAMOS, Alejandro (2012). “MAGERIT v3”. En: <
<http://www.securitybydefault.com/2012/10/ccn-cert-magerit-v3-y-17-nuevas-guias.html>
>, (fecha de consulta 4/06/2019).

Anexo 1

Objetivos estratégicos del Ministerio de Energías



Fuente: [2]

Anexo 2 Metodología Magerit



Fuente: [9]

Anexo 3 Tabla de Análisis de Riesgos de Activos relevantes

ANÁLISIS DE RIESGOS							
ACTIVO	TIPO	AMENAZA	PROB ABILI DAD	IMPA CTO	RIE SG O		
Antivirus 01 (Despacho Ministro)	Software	Caída del servicio	2	3	6		
Antivirus 02 (Unidad de Comunicación Social)	Software	Caída del servicio	2	3	6		
Antivirus 03 (Unidad de Auditoría Interna)	Software	Caída del servicio	2	3	6		
Antivirus 04 (Unidad de Transparencia)	Software	Caída del servicio	2	3	6		
Antivirus 05 (Dirección General de Planificación)	Software	Caída del servicio	2	3	6		

Antivirus 06 (Dirección Asuntos Administrativos)	Software	Caída del servicio	2	3	6
Antivirus 07 (Dirección Asuntos Jurídicos)	Software	Caída del servicio	2	3	6
Antivirus 08 (Viceministerio de Electricidad y Energías Alternativas)	Software	Caída del servicio	2	3	6
Antivirus 09 (Viceministerio de Altas Tecnologías Energéticas)	Software	Caída del servicio	2	3	6
Antivirus 10 (Dirección General de Electricidad)	Software	Caída del servicio	2	3	6
Antivirus 11 (Dirección General de Energías Alternativas)	Software	Caída del servicio	2	3	6
Antivirus 12 (Dirección General de Control y Fiscalización)	Software	Caída del servicio	2	3	6
Antivirus 14 (Dirección General de Gestión Socio Ambiental)	Software	Caída del servicio	2	3	6
Antivirus 15 (Dirección General de Litio)	Software	Caída del servicio	2	3	6
Antivirus 13 (Dirección General de Energía Nuclear)	Software	Caída del servicio	2	3	6
Servidor 01 (Despacho Ministro)	Hardware	Denegación de servicio	2	3	6
Servidor 02 (Unidad de Comunicación Social)	Hardware	Denegación de servicio	2	3	6
Servidor 03 (Unidad de Auditoría Interna)	Hardware	Denegación de servicio	2	3	6
Servidor 04 (Unidad de Transparencia)	Hardware	Denegación de servicio	2	3	6
Servidor 05(Dirección General de Planificación)	Hardware	Denegación de servicio	2	3	6
Servidor 06(Dirección Asuntos Administrativos)	Hardware	Denegación de servicio	2	3	6
Servidor 07(Dirección Asuntos Jurídicos)	Hardware	Denegación de servicio	2	3	6
Servidor 08 (Viceministerio de Electricidad y Energías Alternativas)	Hardware	Denegación de servicio	2	3	6

Servidor 09 (Viceministerio de Altas Tecnologías Energéticas)	Hardware	Denegación de servicio	2	3	6
Servidor 01(Despacho Ministro)	Hardware	Corte del suministro eléctrico	1	3	3
Servidor 02(Unidad de Comunicación Social)	Hardware	Corte del suministro eléctrico	1	3	3
Servidor 03(Unidad de Auditoría Interna)	Hardware	Corte del suministro eléctrico	1	3	3
Servidor 04(Unidad de Transparencia)	Hardware	Corte del suministro eléctrico	1	3	3
Servidor 05(Dirección General de Planificación)	Hardware	Corte del suministro eléctrico	1	3	3
Servidor 06(Dirección Asuntos Administrativos)	Hardware	Corte del suministro eléctrico	1	3	3
Servidor 07(Dirección Asuntos Jurídicos)	Hardware	Corte del suministro eléctrico	1	3	3
Servidor 08(Viceministerio de Electricidad y Energías Alternativas)	Hardware	Corte del suministro eléctrico	1	3	3
Servidor 09(Viceministerio de Altas Tecnologías Energéticas)	Hardware	Corte del suministro eléctrico	1	3	3
Servidor 01(Despacho Ministro)	Hardware	Fuga de información	1	3	3
Servidor 02(Unidad de Comunicación Social)	Hardware	Fuga de información	1	3	3
Servidor 03(Unidad de Auditoría Interna)	Hardware	Fuga de información	1	3	3
Servidor 04(Unidad de Transparencia)	Hardware	Fuga de información	1	3	3
Servidor 05(Dirección General de Planificación)	Hardware	Fuga de información	1	3	3
Servidor 06(Dirección Asuntos Administrativos)	Hardware	Fuga de información	1	3	3
Servidor 07(Dirección Asuntos Jurídicos)	Hardware	Fuga de información	1	3	3
Servidor 08 (Viceministerio de Electricidad y Energías Alternativas)	Hardware	Fuga de información	1	3	3
Servidor 09 (Viceministerio de Altas Tecnologías Energéticas)	Hardware	Fuga de información	1	3	3

PC 01(Despacho Ministro)	Hardware	Fuga de información	1	3	3
PC 02(Unidad de Comunicación Social)	Hardware	Fuga de información	1	3	3
PC 03(Unidad de Auditoría Interna)	Hardware	Fuga de información	1	3	3
PC 04(Unidad de Transparencia)	Hardware	Fuga de información	1	3	3
PC 05(Dirección General de Planificación)	Hardware	Fuga de información	1	3	3
PC 06(Dirección Asuntos Administrativos)	Hardware	Fuga de información	1	3	3
PC 07(Dirección Asuntos Jurídicos)	Hardware	Fuga de información	1	3	3
PC 08(Viceministerio de Electricidad y Energías Alternativas)	Hardware	Fuga de información	1	3	3
PC 09(Viceministerio de Altas Tecnologías Energéticas)	Hardware	Fuga de información	1	3	3
PC 10(Dirección General de Electricidad)	Hardware	Fuga de información	2	2	4
PC 11(Dirección General de Energías Alternativas)	Hardware	Fuga de información	2	2	4
PC 12(Dirección General de Control y Fiscalización)	Hardware	Fuga de información	2	2	4
PC 14(Dirección General de Gestión Socio Ambiental)	Hardware	Fuga de información	2	2	4
PC 15(Dirección General de Litio)	Hardware	Fuga de información	2	2	4
PC 13(Dirección General de Energía Nuclear)	Hardware	Fuga de información	2	2	4
PC 01(Despacho Ministro)	Hardware	Infección por virus	2	3	6
PC 02(Unidad de Comunicación Social)	Hardware	Infección por virus	2	3	6
PC 03(Unidad de Auditoría Interna)	Hardware	Infección por virus	2	3	6
PC 04(Unidad de Transparencia)	Hardware	Infección por virus	2	3	6
PC 05(Dirección General de Planificación)	Hardware	Infección por virus	2	3	6
PC 06(Dirección Asuntos Administrativos)	Hardware	Infección por virus	2	3	6
PC 07(Dirección Asuntos Jurídicos)	Hardware	Infección por virus	2	3	6

PC 08(Viceministerio de Electricidad y Energías Alternativas)	Hardware	Infección por virus	2	3	6
PC 09(Viceministerio de Altas Tecnologías Energéticas)	Hardware	Infección por virus	2	3	6
PC 10(Dirección General de Electricidad)	Hardware	Infección por virus	2	3	6
PC 11(Dirección General de Energías Alternativas)	Hardware	Infección por virus	2	3	6
PC 12(Dirección General de Control y Fiscalización)	Hardware	Infección por virus	2	3	6
PC 14(Dirección General de Gestión Socio Ambiental)	Hardware	Infección por virus	2	3	6
PC 15(Dirección General de Litio)	Hardware	Infección por virus	2	3	6
PC 13(Dirección General de Energía Nuclear)	Hardware	Infección por virus	2	3	6

Fuente: Elaboración propia 2019

Anexo 4

Código del monitor de procesos en lenguaje *Python*

```
import win32con
import win32api
import win32security
import wmi
import sys
import os

LOG_FILE = "process_monitor_log.csv"
def get_process_privileges(pid):
    try:
        # obtain a handle to the target process
        hproc = win32api.OpenProcess(win32con.PROCESS_QUERY_INFORMATION, False, pid)
        # open the main process token
        htok = win32security.OpenProcessToken(hproc, win32con.TOKEN_QUERY)
        # retrieve the list of privileges enabled
        privs = win32security.GetTokenInformation(htok, win32security.TokenPrivileges)
        # iterate over privileges and output the ones that are enabled
        priv_list = []
        for priv_id, priv_flags in privs:
            # check if the privilege is enabled
            if priv_flags == 3:
                priv_list.append(win32security.LookupPrivilegeName(None, priv_id))
    except:
        priv_list.append("N/A")
    return "|".join(priv_list)

def log_to_file(message):
    fd = open(LOG_FILE, "ab")
    fd.write("%s\r\n" % message)
    fd.close()
    return

# create a log file header
if not os.path.isfile(LOG_FILE):
    log_to_file("Time,User,Executable,CommandLine,PID,ParentPID,Privileges")
# instantiate the WMI interface
c = wmi.WMI()
# create our process monitor
process_watcher = c.Win32_Process.watch_for("creation")
while True:
    try:
        new_process = process_watcher()
        proc_owner = new_process.GetOwner()
        proc_owner = "%s\\%s" % (proc_owner[0],proc_owner[2])
        create_date = new_process.CreationDate
        executable = new_process.ExecutablePath
        cmdline = new_process.CommandLine
        pid = new_process.ProcessId
        parent_pid = new_process.ParentProcessId
        privileges = get_process_privileges(pid)
        process_log_message = "%s,%s,%s,%s,%s,%s,%s" % (create_date, proc_owner, executable, cmdline, pid, parent_pid,privileges)
        print "%s\r\n" % process_log_message
        log_to_file(process_log_message)
    except:
        pass
```

Fuente: Elaboración propia 2019

Anexo 5

Resultados de riesgos detectados con OWASP

Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Low (Medium)	Protección de buscador de web XSS no disponible
Description	La protección del buscador de web XSS no está disponible, o está deshabilitada por la configuración de la cabecera de respuesta de HTTP 'X-XSS-Protection' en el servidor de web
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Low (Medium)	Cookie sin bandera asegurada
Description	Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser accedida mediante conexiones sin cifrar.
Low (Medium)	Inclusión de archivos de origen JavaScript Cross-Domain
Description	Las páginas incluyen uno o mas archivos encriptados de un dominio de terceros.

Fuente: Elaboración propia 2019