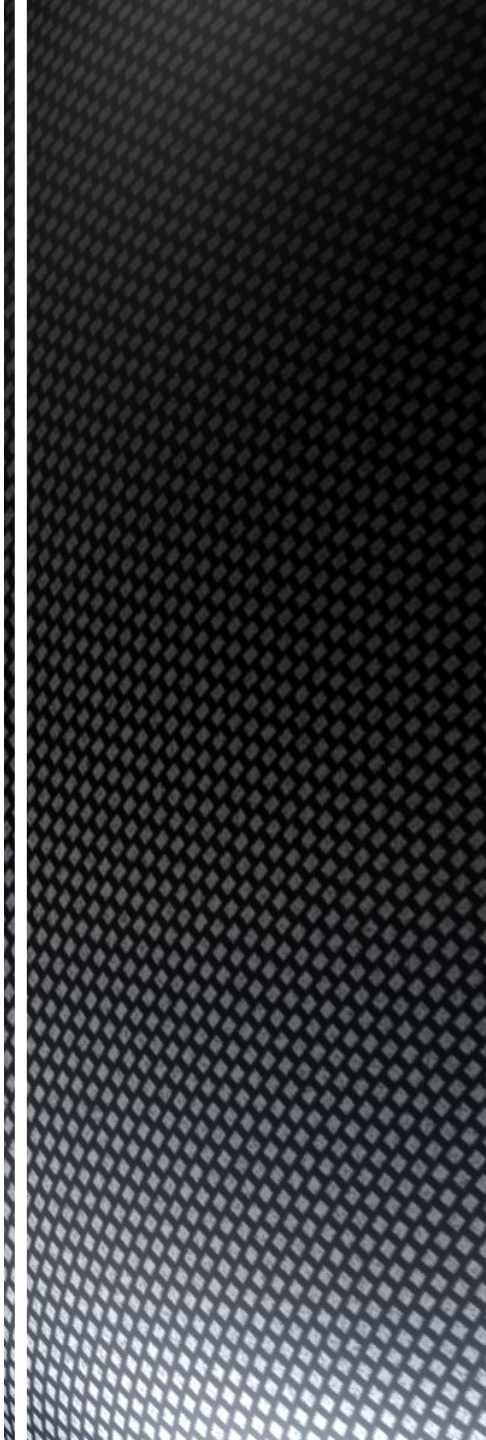
Impacto de las ISO 27000 en organizaciones

Estudio comparativo de herramientas para la implementación de un SGSI



Objetivos de la Tesis

- Estudiar la Norma ISO 27001
- Analizar aportes de la ISO 27004 al proceso de la ISO 27001
- Analizar herramientas de monitoreo y compliance para ver en que medida proveen soporte para implementar un SGSI bajo la ISO 27001.
- Generar una Especificación de Requerimientos

Objetos de Análisis
- ISO 27001 & ISO 27004

ISO 27001: Es la norma principal de requerimientos del sistema de gestión de seguridad de la información. Contiene un Anexo con objetivos de control y controles a ser implementados.

ISO 27004: Especifica las métricas y técnicas de medición que pueden ser aplicables para determinar la eficiencia y efectividad de la implementación de un SGSI y de los controles relacionados.

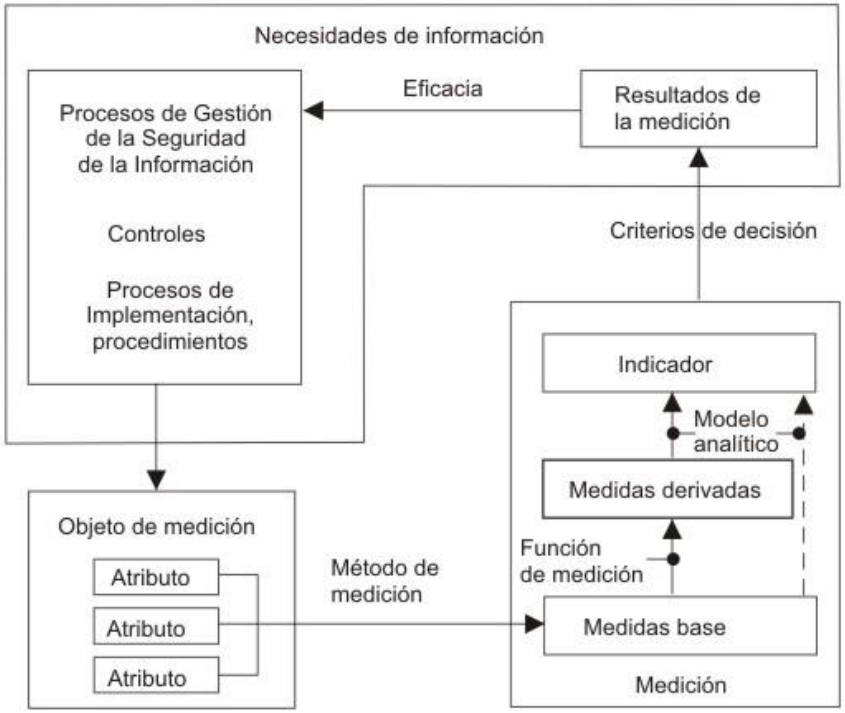
Objetos de Análisis
- Conceptos Teóricos

- ¿Qué es ISO?
- ¿Qué es un SGSI?

La norma define requerimientos generales y genéricos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI.

IRAM-ISO/IEC 27004:2011
- Programa y Modelo de Medición

La norma realiza recomendaciones para la implementación de un programa de medición eficaz.



Programa y Modelo de Medición

Objetos de Análisis
- Herramientas de Monitoreo y Compliance

Aquí se hace una reseña de las herramientas que serán analizadas.

Monitoreo:

Compliance:

Herramientas de Monitoreo y Compliance - OSSIM

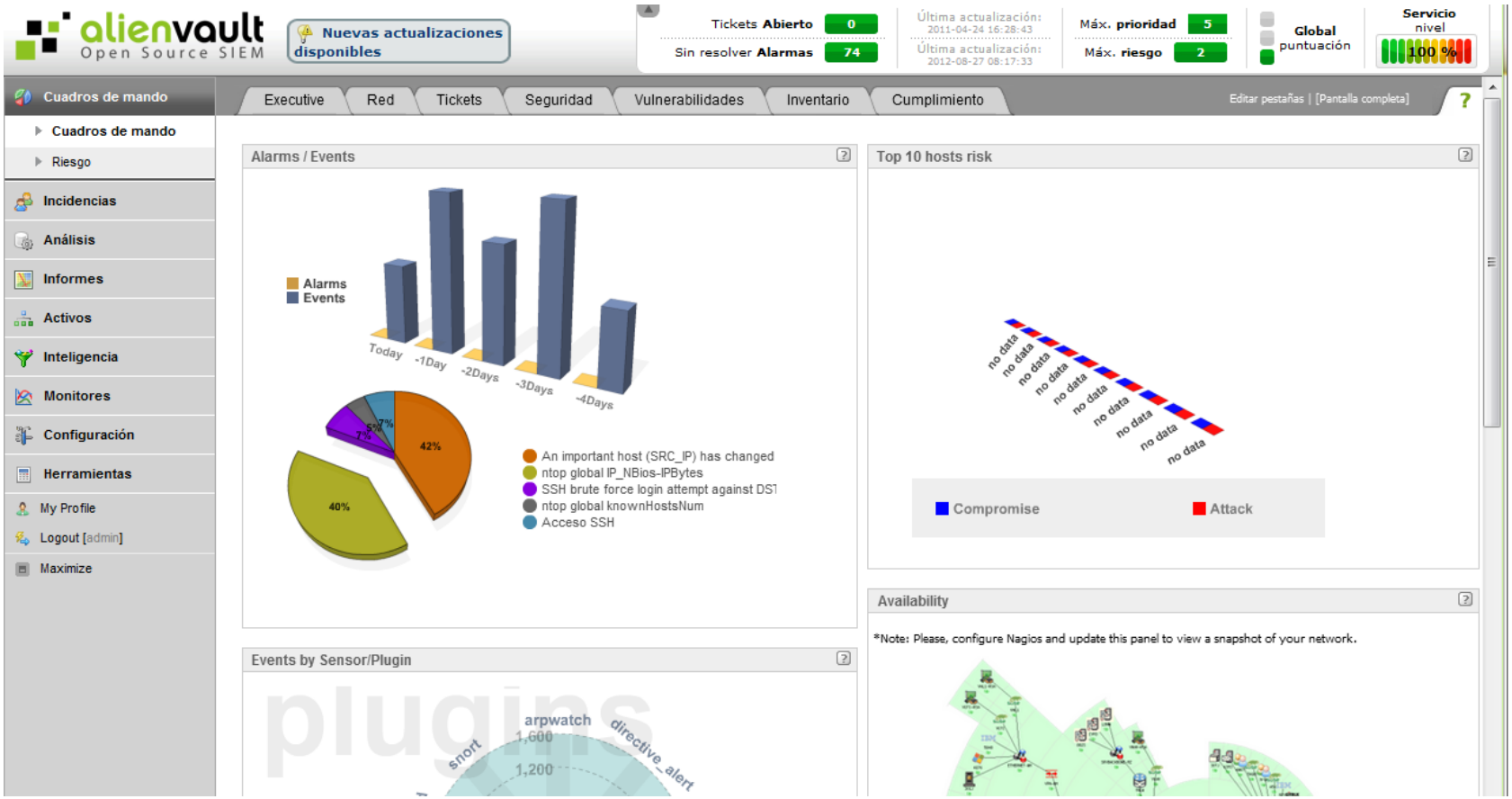
¿Que es OSSIM?

Es un herramienta de monitoreo y compliance gratuita y de código abierto aunque también puede encontrarse versiones comerciales mas completas.

- Analiza comunicación entre hosts
- Inventario de Activos
- Valoración de Activos
- Permite definir políticas y directivas
- Gestión de Compliance

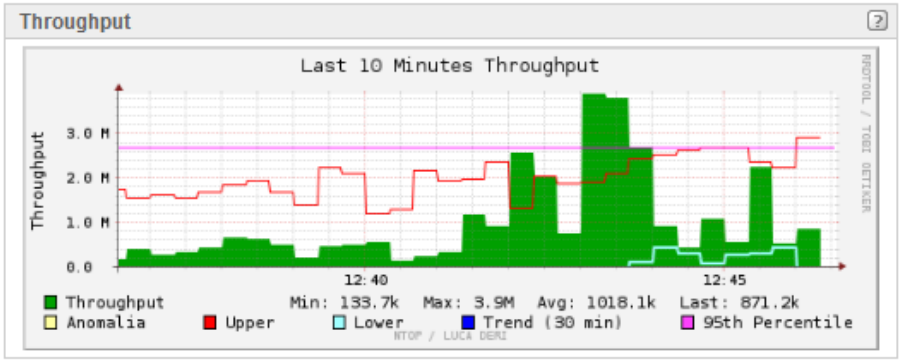
Herramientas de Monitoreo y Compliance - OSSIM

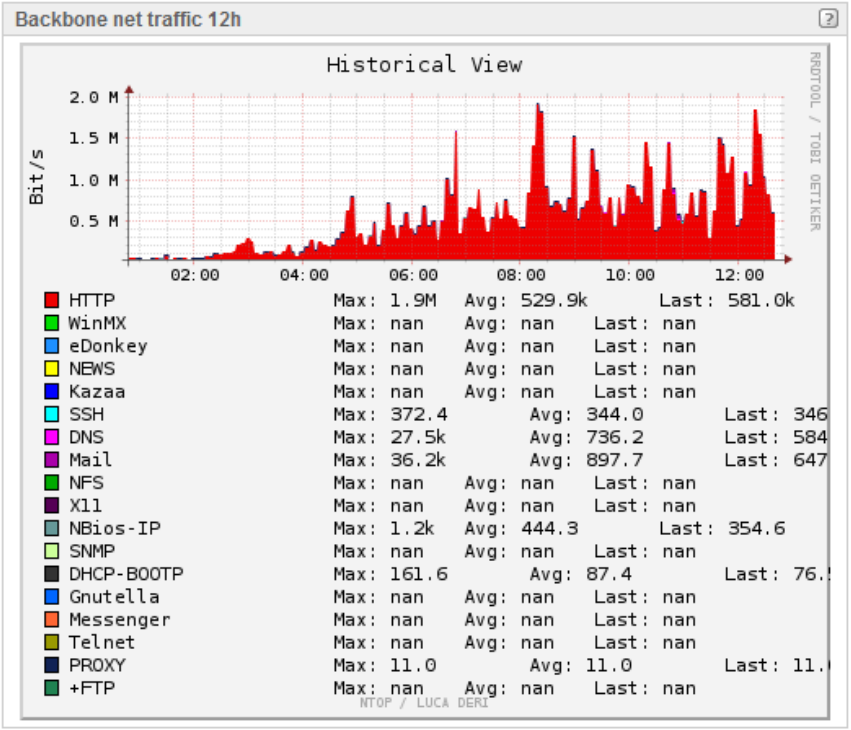
Vista Principal



Herramientas de Monitoreo y Compliance - OSSIM

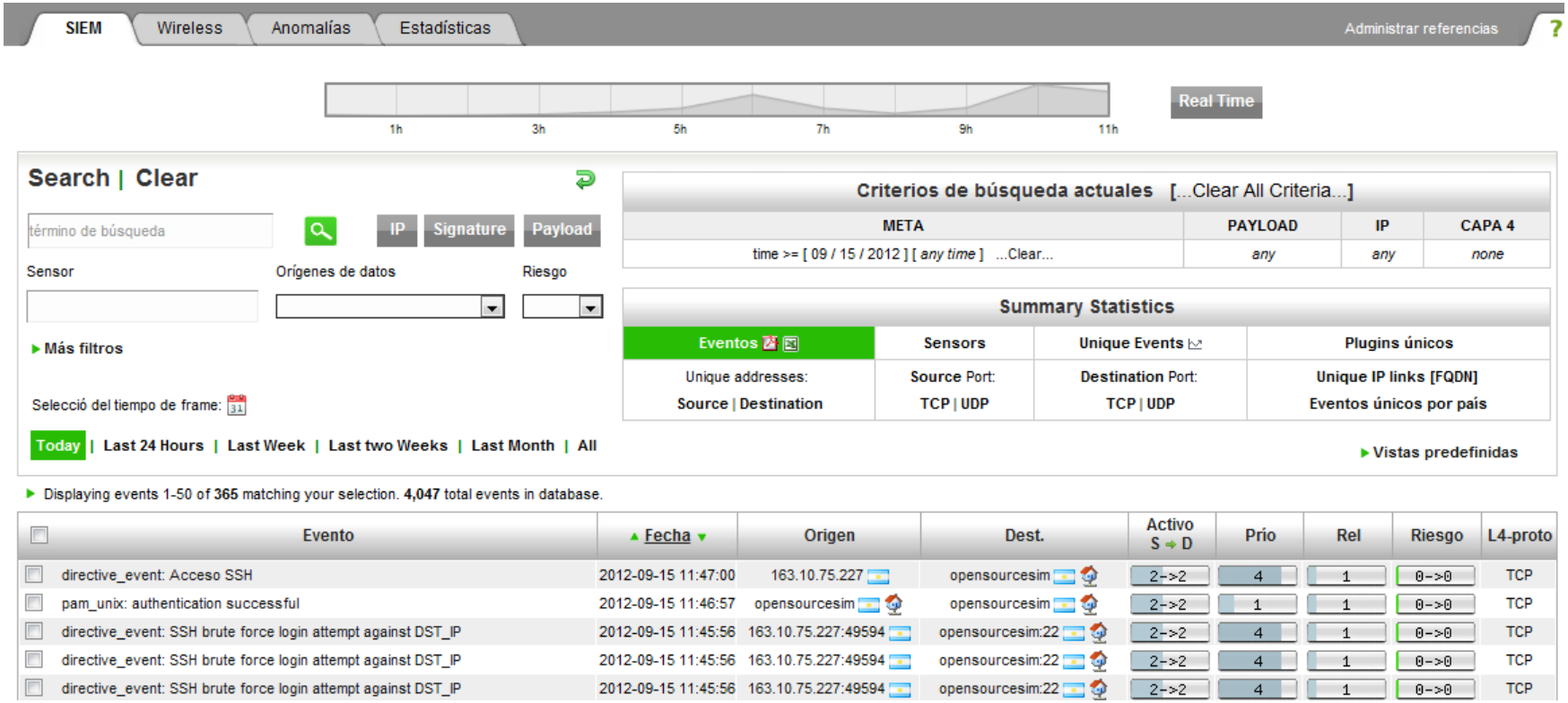
Gráfico general de Trafico en la red y discriminado por protocolo





Herramientas de Monitoreo y Compliance - OSSIM

SIEM – Eventos de la red



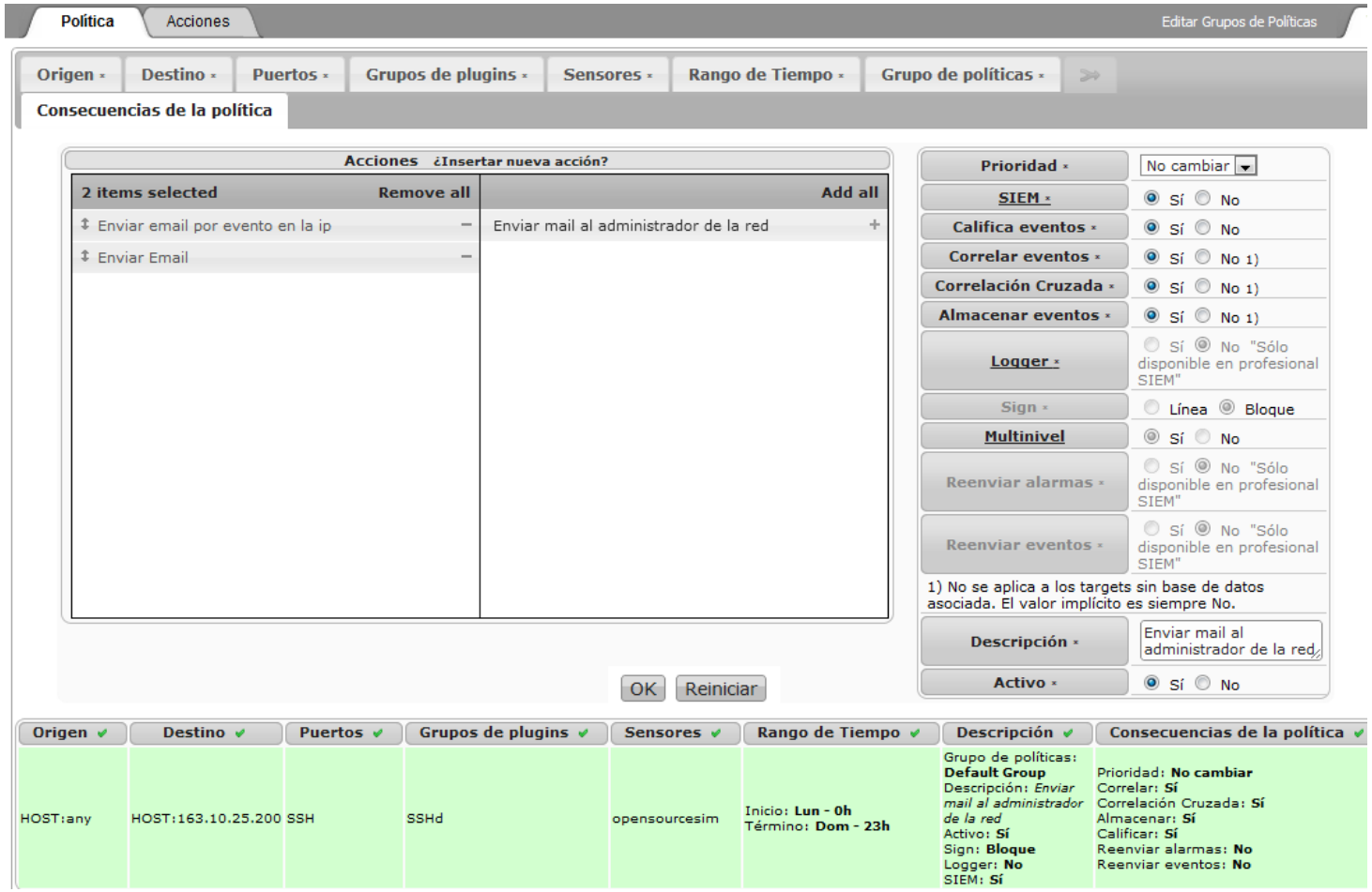
Herramientas de Monitoreo y Compliance - OSSIM

Políticas y Acciones

Estado	Orden	Prioridad	Origen	Destino	Grupo de Puertos	Grupo de Plugins	Sensores	Rango de Tiempo	Objetivos	Descripción
✗	1	-	ANY	opensourcesim.alienvault	ANY	Web Attacks	opensourcesim	Vie 20h - Lun 2h	ANY	Enviar mail al administrador de la red
✗	2	-	ANY	opensourcesim.alienvault	ANY	AtaquesDNS	opensourcesim	Vie 19h - Dom 23h	ANY	Enviar mail al administrador de la red
✓	3	-	ANY	opensourcesim.alienvault	SSH	SSHd	opensourcesim	Lun 0h - Dom 23h	ANY	Enviar mail al administrador de la red
✗	4	-	ANY	opensourcesim.alienvault	ANY	ossec	opensourcesim	Lun 10h - Dom 23h	ANY	Enviar mail al administrador de la red
✓	5	-	opensourcesim.alienvault	Switch Sec. Departamentos	ANY	Monitoreo	opensourcesim	Lun 0h - Dom 23h	ANY	Enviar mail

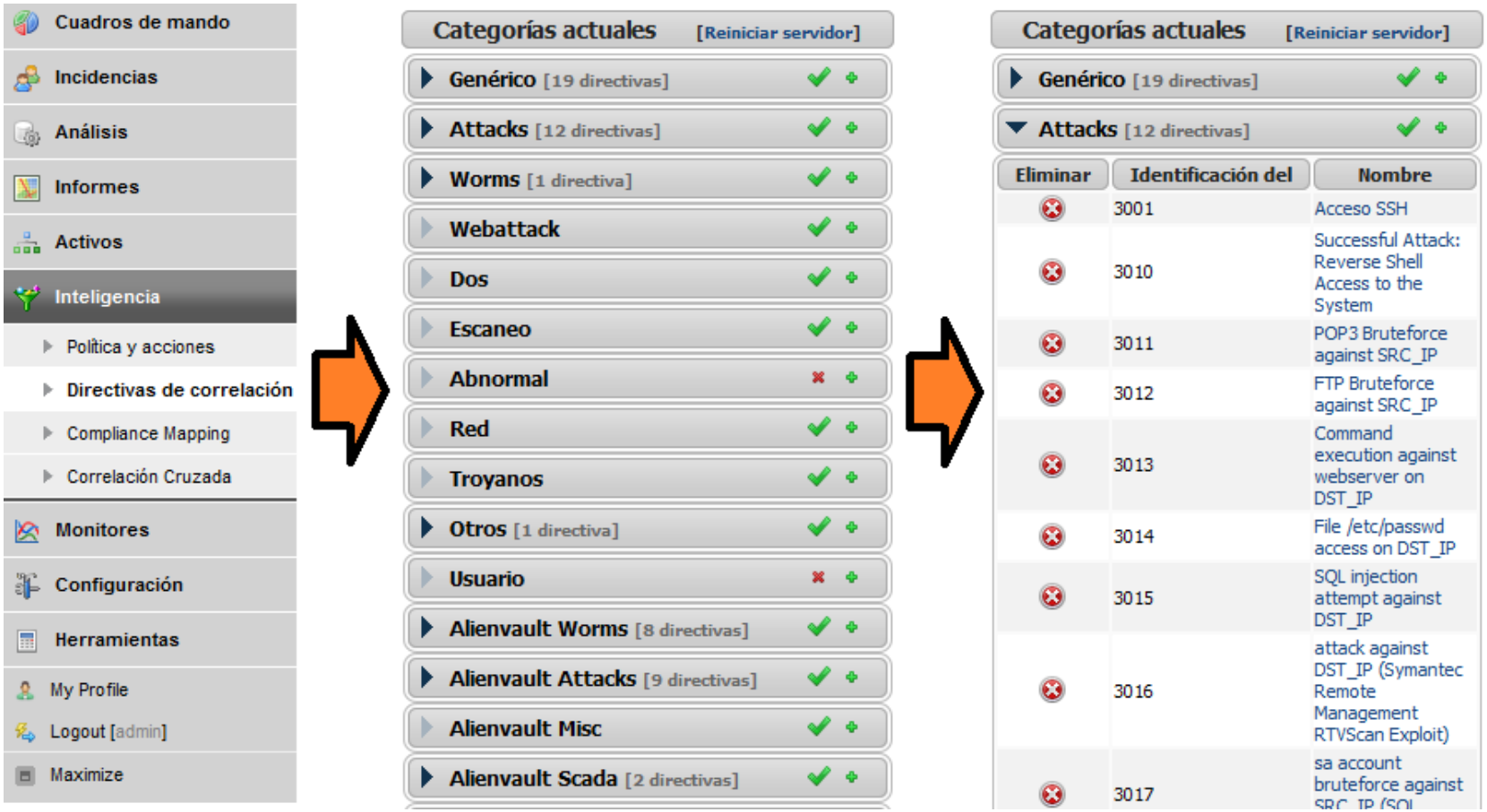
Herramientas de Monitoreo y Compliance - OSSIM

Políticas y acciones



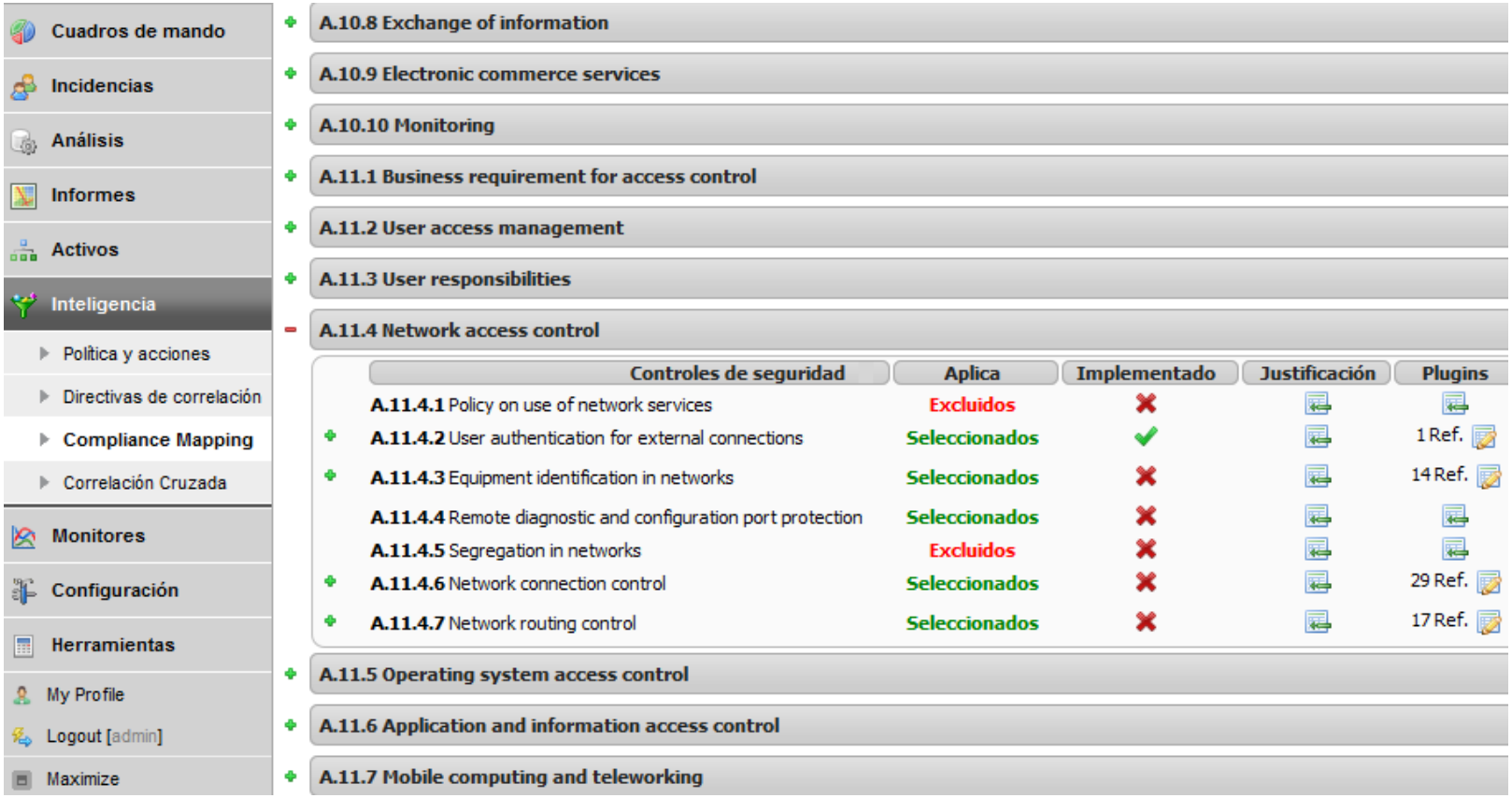
Herramientas de Monitoreo y Compliance - OSSIM

Directivas de Correlación



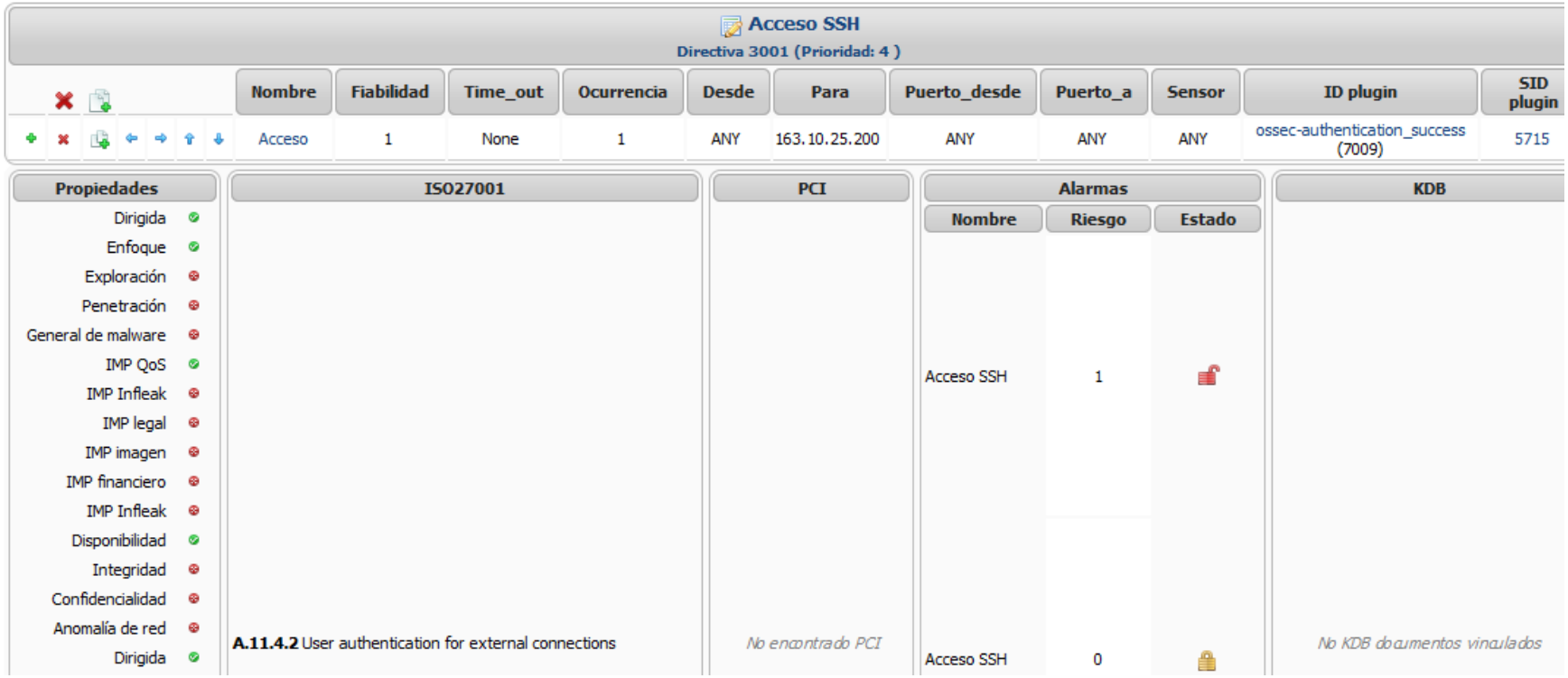
Herramientas de Monitoreo y Compliance - OSSIM

Compliance mapping



Herramientas de Monitoreo y Compliance - OSSIM

Directivas de Correlación



Acceso SSH

Directiva 3001 (Prioridad: 4)

Nombre	Fiabilidad	Time_out	Ocurrencia	Desde	Para	Puerto_desde	Puerto_a	Sensor	ID plugin	SID plugin
Acceso	1	None	1	ANY	163.10.25.200	ANY	ANY	ANY	ossec-authentication_success (7009)	5715

Propiedades	
Dirigida	✓
Enfoque	✓
Exploración	✗
Penetración	✗
General de malware	✗
IMP QoS	✓
IMP Infleak	✗
IMP legal	✗
IMP imagen	✗
IMP financiero	✗
IMP Infleak	✗
Disponibilidad	✓
Integridad	✗
Confidencialidad	✗
Anomalía de red	✗
Dirigida	✓

ISO27001

A.11.4.2 User authentication for external connections

PCI

No encontrado PCI

Alarmas

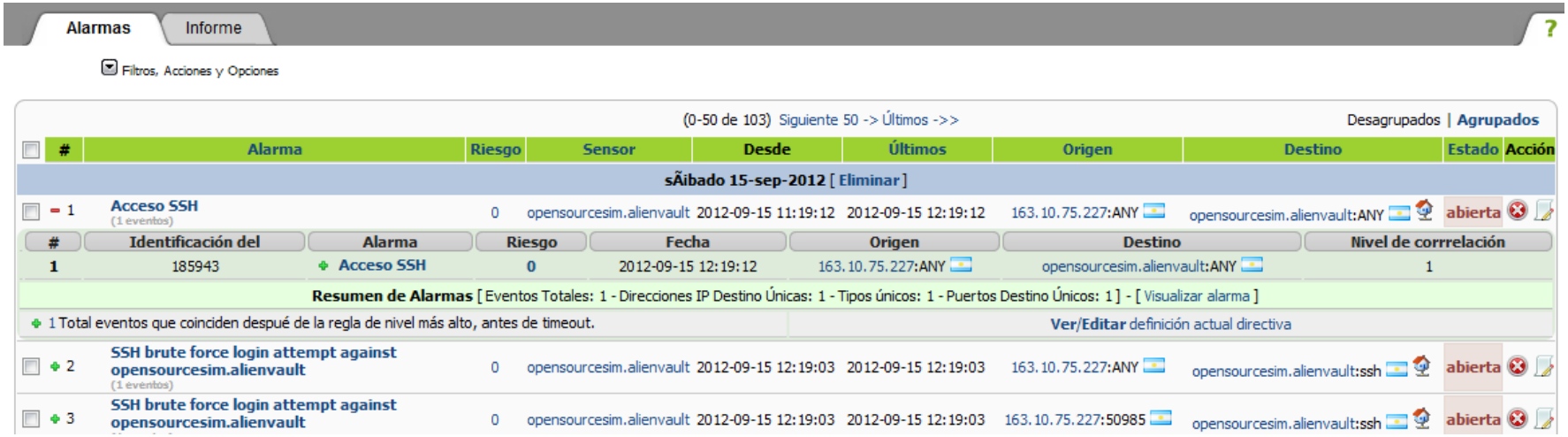
Nombre	Riesgo	Estado
Acceso SSH	1	
Acceso SSH	0	

KDB

No KDB documentos vinculados

Herramientas de Monitoreo y Compliance - OSSIM

Alarmas



Herramientas de Monitoreo y Compliance - OSSIM

Conclusiones

Ventajas

- Análisis de eventos de la red
- Gran cantidad de plugins
- Visualización del riesgo
- Manejo de los controles la norma ISO

Limitaciones

- Complejidad de uso
- No provee manejo de gestión de la norma ISO

Herramientas de Monitoreo y Compliance - OpenNMS

¿Que es OpenNMS?

Es una herramienta unicamente de monitoreo y es completamente gratuita. Realiza descubrimientos de hosts sin importar en que subredes se encuentren. Está orientada mayormente a servicios.

- Descubre hosts en distintas subredes/VLANS
- Permite la importación de activos desde otras fuentes
- Permite diagramar una topologia de red
- Analiza los servicios disponibles de cada host encontrado
- Realiza estadisticas de eventos ocurridos discriminados por protocolo
- Notificaciones programadas
- Reportes

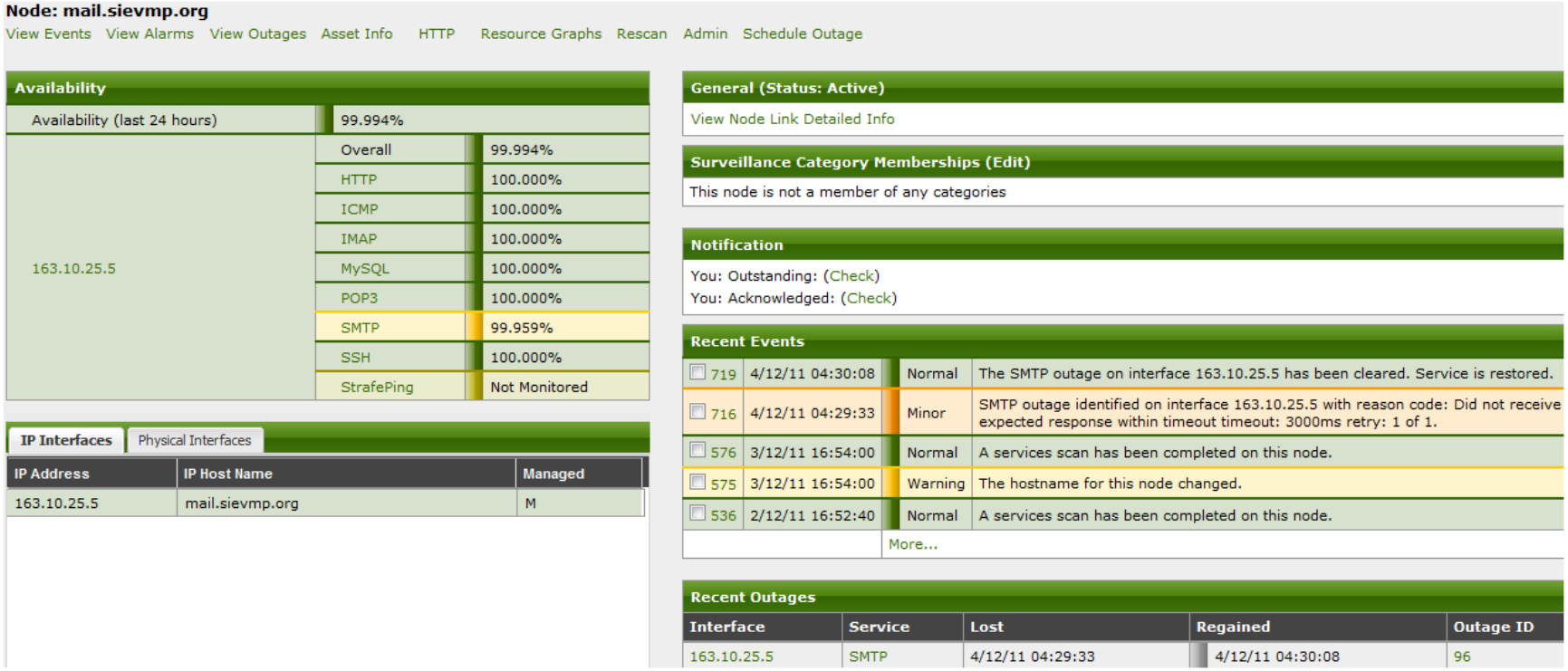
Herramientas de Monitoreo y Compliance - OpenNMS

Vistazo principal

OpenNMS Copyright © 2002-2011 The OpenNMS Group, Inc. OpenNMS® is a registered trademark of The OpenNMS Group, Inc.

Herramientas de Monitoreo y Compliance - OpenNMS

Detalle de servicios de un host determinado



Node: mail.sievmp.org

View Events | View Alarms | View Outages | Asset Info | HTTP | Resource Graphs | Rescan | Admin | Schedule Outage

Availability

Availability (last 24 hours)		99.994%
163.10.25.5	Overall	99.994%
	HTTP	100.000%
	ICMP	100.000%
	IMAP	100.000%
	MySQL	100.000%
	POP3	100.000%
	SMTP	99.959%
	SSH	100.000%
	StrafePing	Not Monitored

IP Interfaces | Physical Interfaces

IP Address	IP Host Name	Managed
163.10.25.5	mail.sievmp.org	M

General (Status: Active)

View Node Link Detailed Info

Surveillance Category Memberships (Edit)

This node is not a member of any categories

Notification

You: Outstanding: (Check)
You: Acknowledged: (Check)

Recent Events

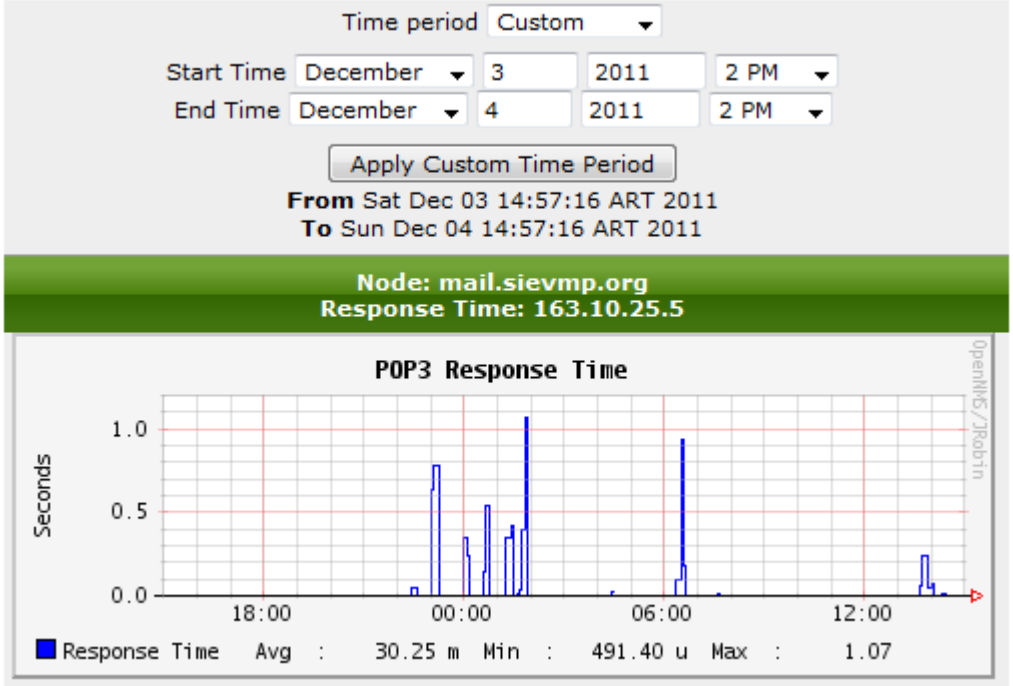
719	4/12/11 04:30:08	Normal	The SMTP outage on interface 163.10.25.5 has been cleared. Service is restored.
716	4/12/11 04:29:33	Minor	SMTP outage identified on interface 163.10.25.5 with reason code: Did not receive expected response within timeout timeout: 3000ms retry: 1 of 1.
576	3/12/11 16:54:00	Normal	A services scan has been completed on this node.
575	3/12/11 16:54:00	Warning	The hostname for this node changed.
536	2/12/11 16:52:40	Normal	A services scan has been completed on this node.
		More...	

Recent Outages

Interface	Service	Lost	Regained	Outage ID
163.10.25.5	SMTP	4/12/11 04:29:33	4/12/11 04:30:08	96

Herramientas de Monitoreo y Compliance - OpenNMS

Estadisticas de eventos ocurridos



Herramientas de Monitoreo y Compliance - OpenNMS

Caídas

Home / Outages / List
Results: (1-20 of 150)

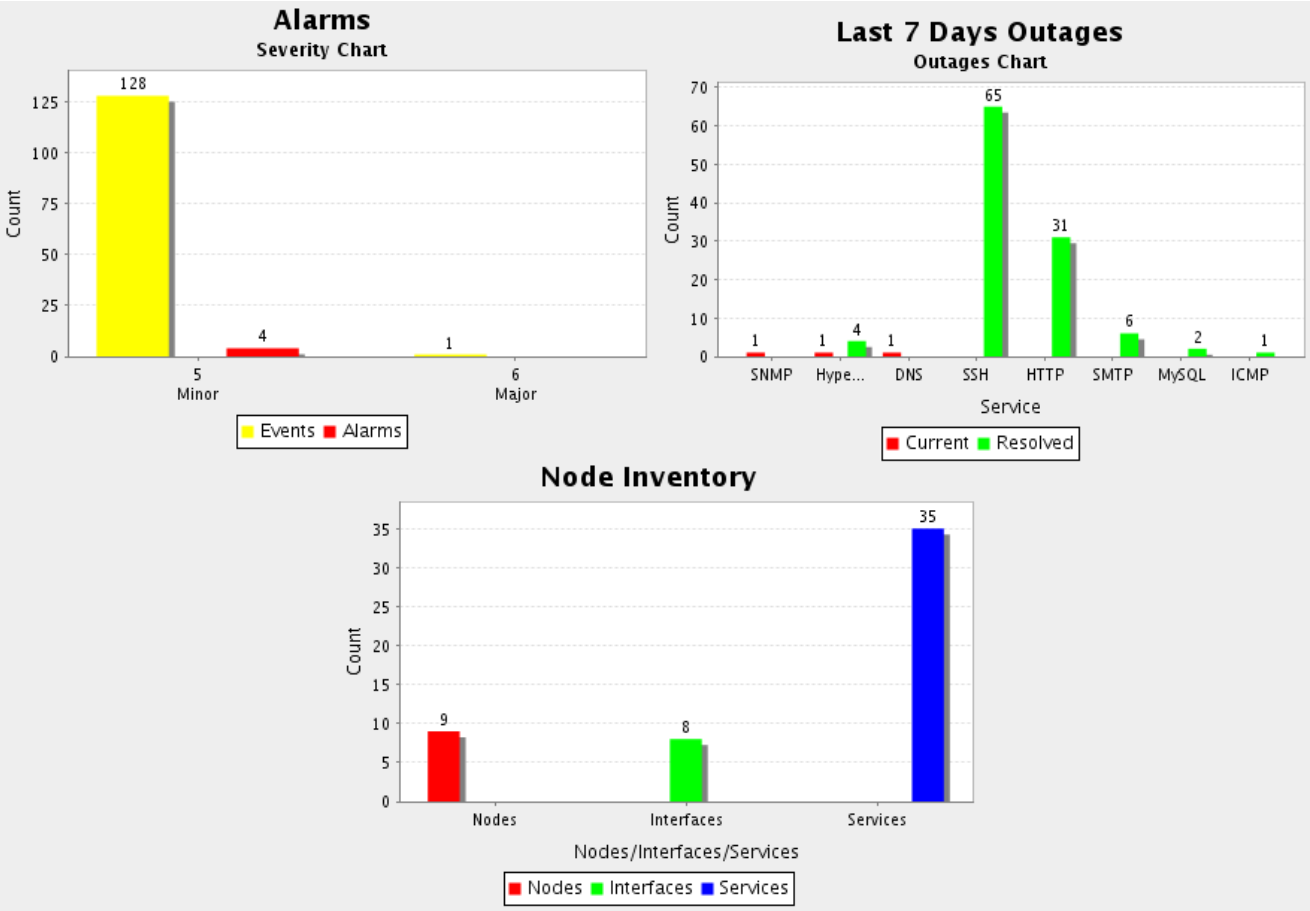
1 2 3 4 5 Next Last

Outage type: Both Current & Resolved
Current
Resolved
Both Current & Resolved

ID	Node	Interface	Service	Down	Up
153	163.10.25.4 [+] [-]	163.10.25.4 [+] [-]	DNS [+] [-]	29/04/12 14:48:22 [<] [>]	DOWN
152	www.fcv.unlp.edu.ar [+] [-]	163.10.25.2 [+] [-]	HTTP [+] [-]	29/04/12 14:48:18 [<] [>]	DOWN
151	www.fcv.unlp.edu.ar [+] [-]	163.10.25.2 [+] [-]	MySQL [+] [-]	29/04/12 14:48:07 [<] [>]	DOWN
150	tesis.fcv.unlp.edu.ar [+] [-]	163.10.25.7 [+] [-]	HypericAgent [+] [-]	10/12/11 14:21:30 [<] [>]	DOWN
149	tesis.fcv.unlp.edu.ar [+] [-]	163.10.25.7 [+] [-]	SSH [+] [-]	10/12/11 14:04:50 [<] [>]	10/12/11 14:21:24 [<] [>]
148	tesis.fcv.unlp.edu.ar [+] [-]	163.10.25.7 [+] [-]	SSH [+] [-]	10/12/11 13:39:02 [<] [>]	10/12/11 13:39:34 [<] [>]
147	www.fcv.unlp.edu.ar [+] [-]	163.10.25.2 [+] [-]	DNS [+] [-]	09/12/11 17:01:53 [<] [>]	DOWN
146	tesis.fcv.unlp.edu.ar [+] [-]	163.10.25.7 [+] [-]	SSH [+] [-]	08/12/11 16:30:59 [<] [>]	08/12/11 16:32:41 [<] [>]
145	www.fcv.unlp.edu.ar [+] [-]	163.10.25.2 [+] [-]	HTTP [+] [-]	07/12/11 10:58:59 [<] [>]	07/12/11 10:59:30 [<] [>]

Herramientas de Monitoreo y Compliance - OpenNMS

Estadisticas de eventos de la red



Herramientas de Monitoreo y Compliance - OpenNMS

Conclusiones

Ventajas

- Descubrimientos dinamico de activos
- Importación de activos desde una fuente externa

Limitaciones

- Carencia de controles y manejo de gestión de la norma ISO
- No analiza comunicaciones entre los hosts

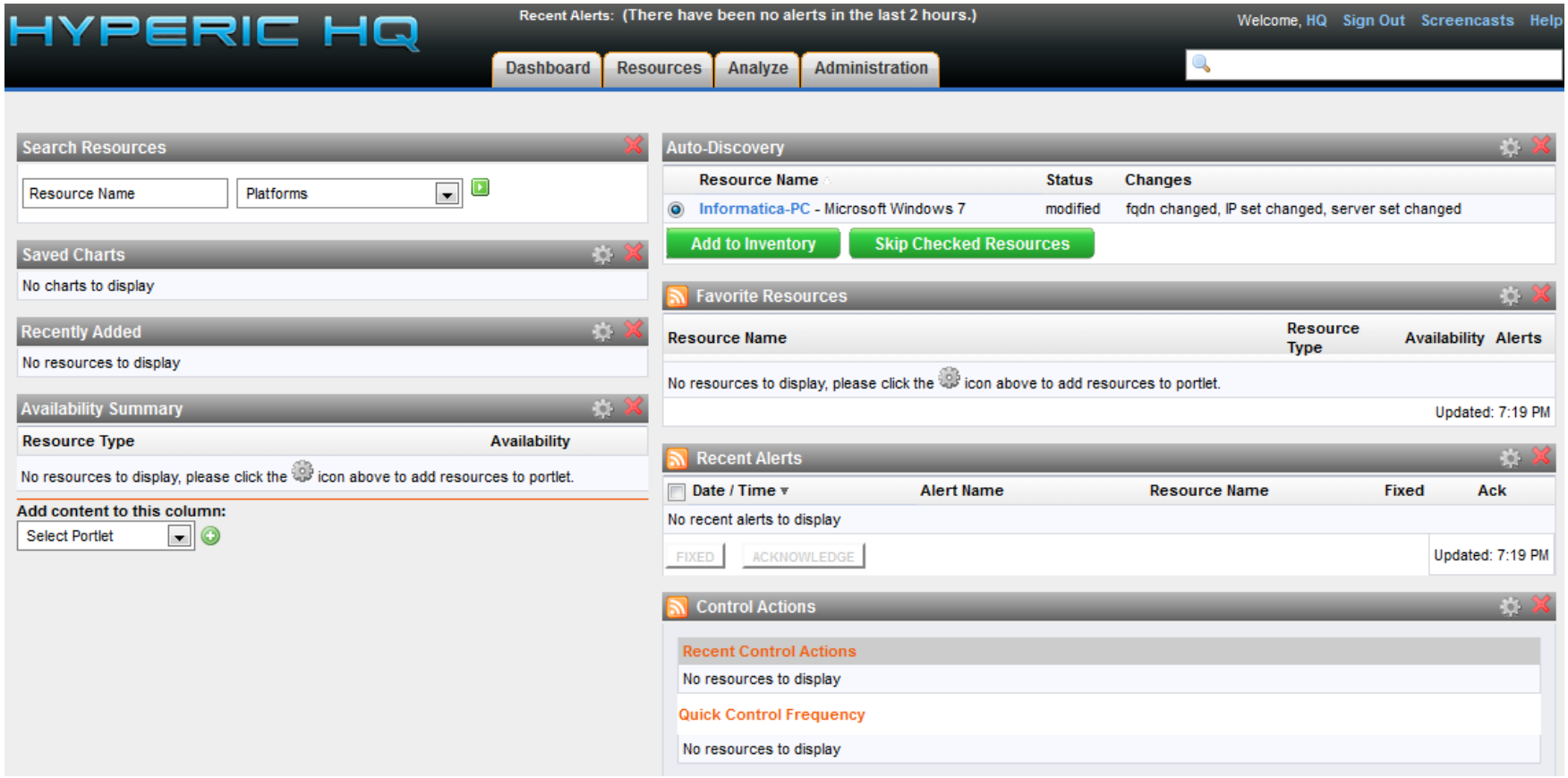
Herramientas de Monitoreo y Compliance - HypericHQ

¿Que es HypericHQ?

Es una herramienta comercial de monitoreo que ofrece una versión de prueba por 30 dias. Está basado en un esquema cliente-servidor donde cada agente es instalado en los activos de la red para que esta herramienta pueda descubrirlos automaticamente junto a sus servicios.

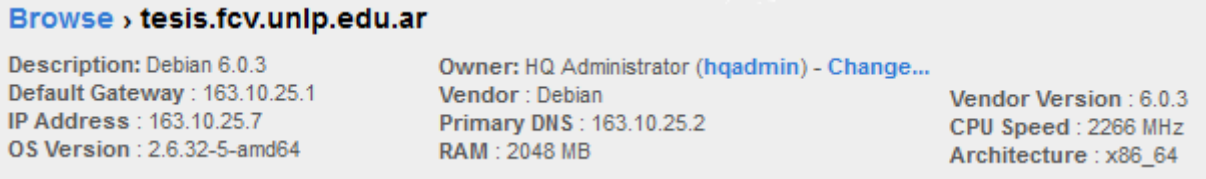
- Centraliza información de cada activo a traves de un dashboard web personalizable
- Realiza un inventario de activos con su correspondiente Hardware y Software además de su estado actual y metricas en tiempo real.
- Define alertas, condiciones, y acciones a ejecutar en base a metricas definidas, como las notificaciones
- Posee un panel de control que discrimina entre eventos del sistema y eventos ocurridos en un activo

Herramientas de Monitoreo y Compliance - HypericHQ

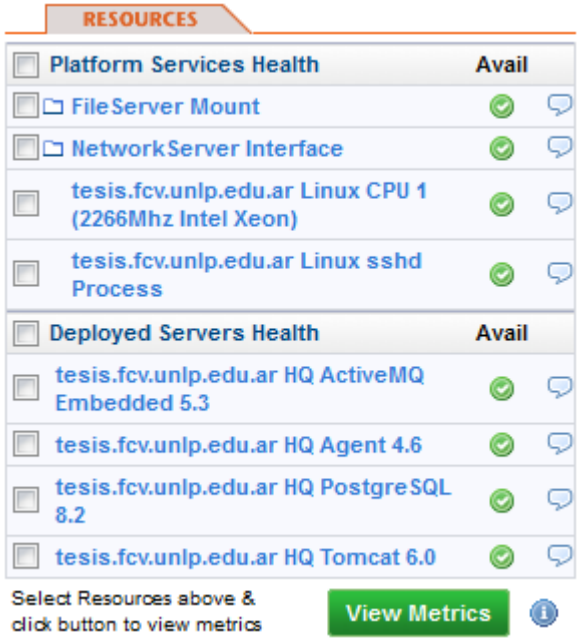


Herramientas de Monitoreo y Compliance - HypericHQ

Servicios de un activo

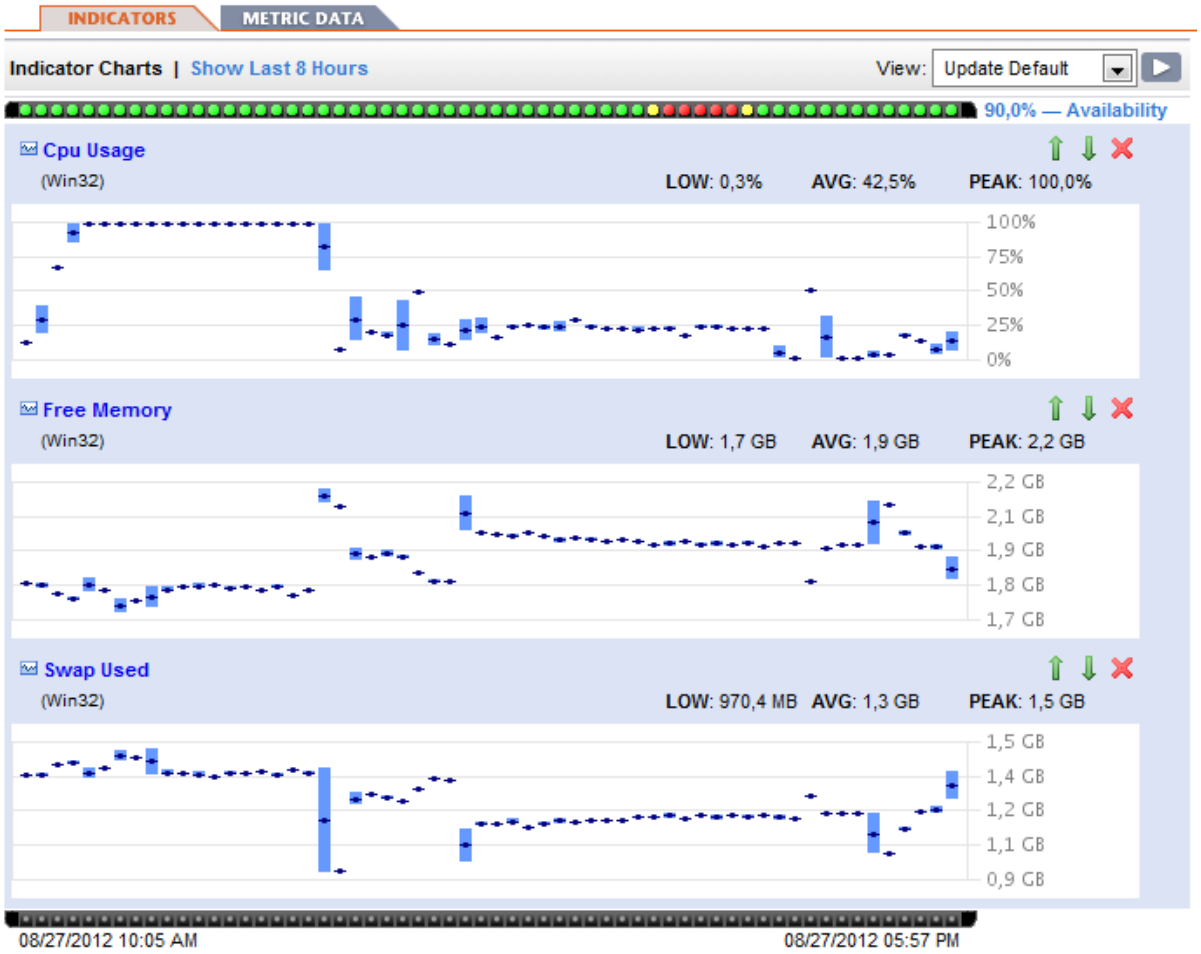


Disponiblidad de sus servicios



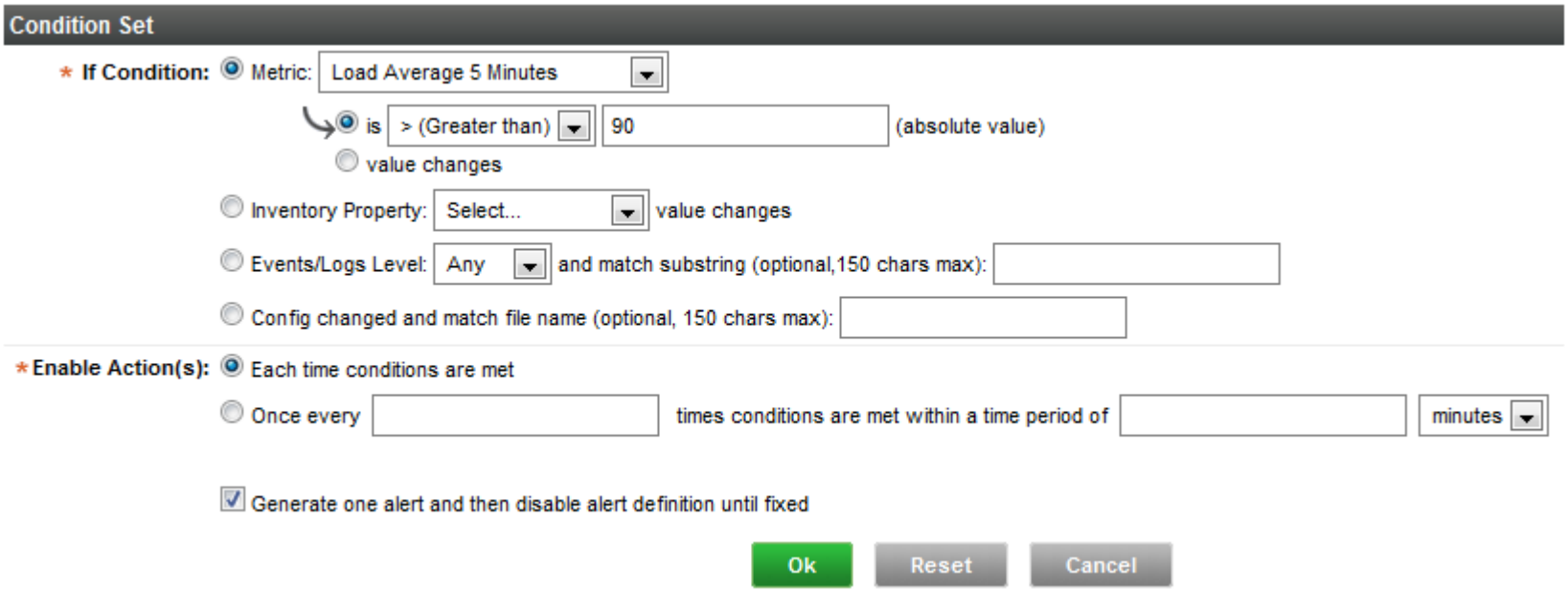
Herramientas de Monitoreo y Compliance - HypericHQ

Indicadores de un activo



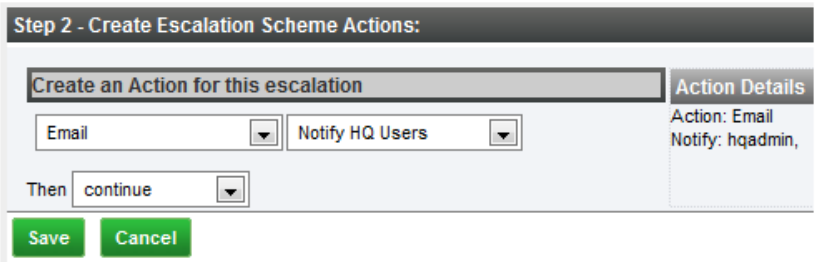
Herramientas de Monitoreo y Compliance - HypericHQ

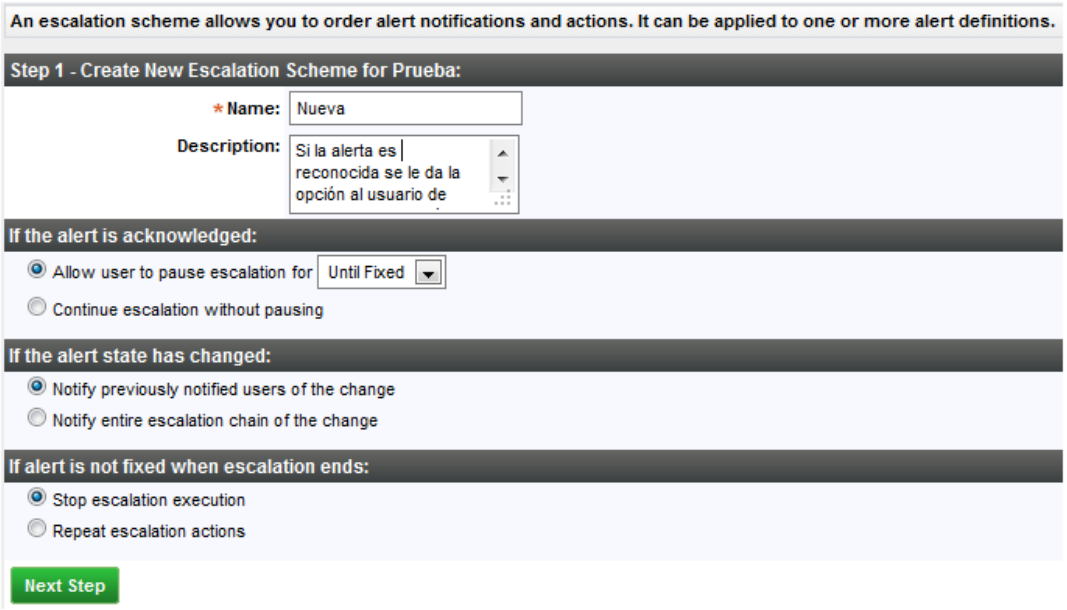
Definición de alerta - Reglas



Herramientas de Monitoreo y Compliance - HypericHQ

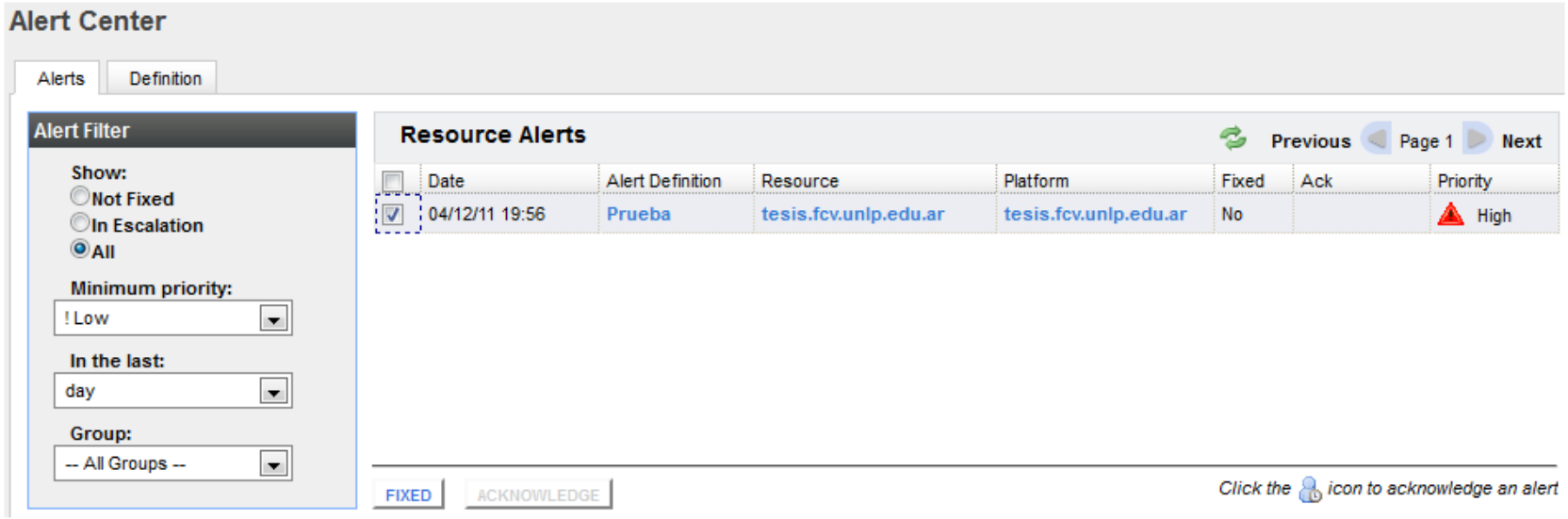
Definición de alerta - Esquemas de notificaciones y definición de Plantilla





Herramientas de Monitoreo y Compliance - HypericHQ

Centro de Alertas y Eventos



Herramientas de Monitoreo y Compliance - HypericHQ

Conclusiones

Ventajas

- Acceso de información completa por medio del agente lo que posibilita un mayor control sobre el activo
- Manejo de esquemas de alertas

Limitaciones

- Configuración sujeta a la ip estática del agente
- Monitoreo solo del activo y no de la red
- No posee manejo de la norma ISO 27001

Herramientas de Monitoreo y Compliance - SecuriaSGSI

¿Que es SecuriaSGSI?

Es una heramienta de compliance totalmente gratuita y de código cerrado. Se basa en un esquema cliente-servidor. A través de cuatro módulos principales realiza un seguimiento de la implementación de la norma 27001, puesta en funcionamiento, mantenimiento y mejora continua de un SGSI.

Herramientas de Monitoreo y Compliance - SecuriaSGSI

¿Como funciona SecuriaSGSI?

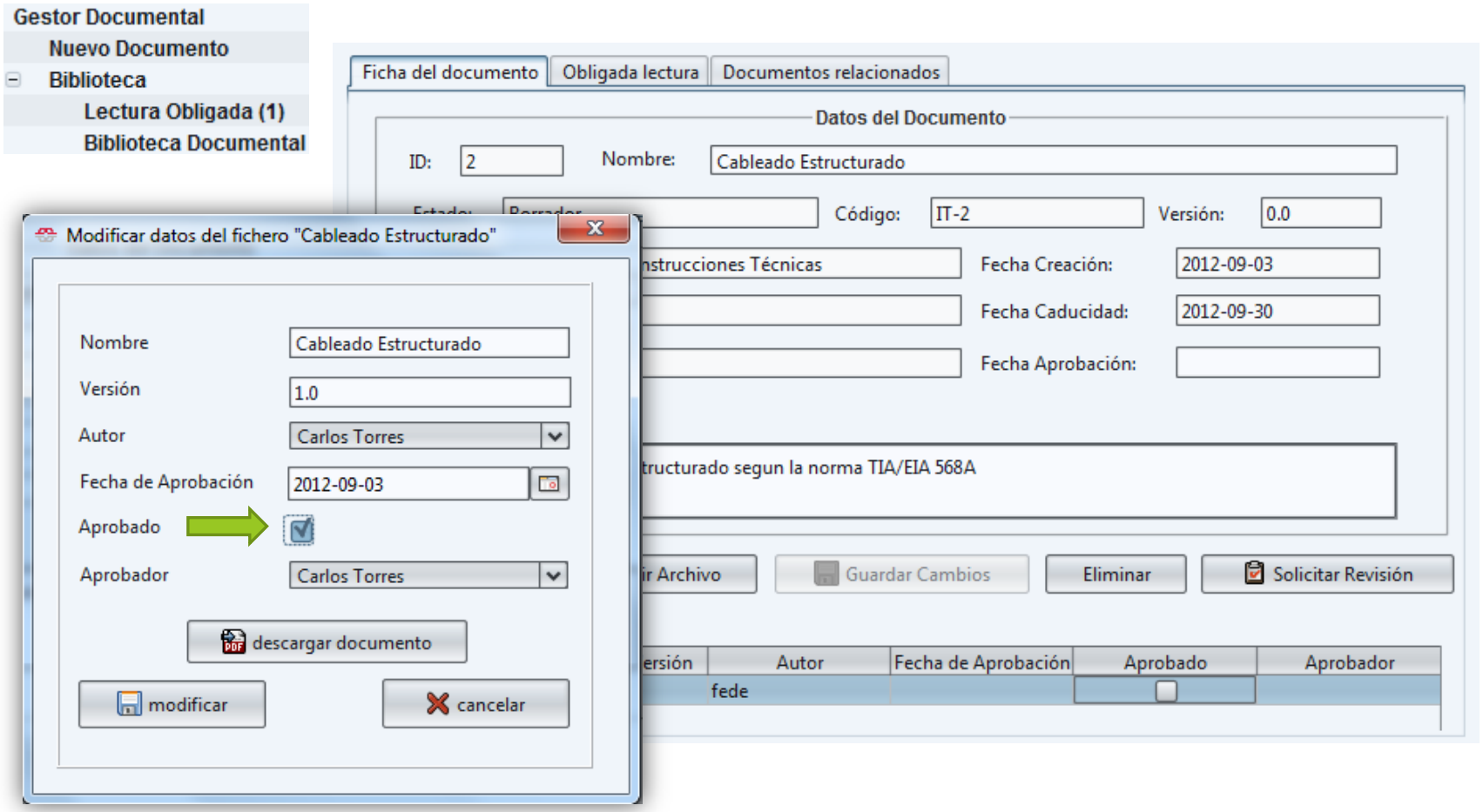
Sistema Administración

- Creación del sistema SGSI
- Definición de usuarios y roles
  - Perfiles de usuario (Rble. Sistema, Rble. Técnico, Usr. Genérico)
  - Aprobadores
  - Responsables de riesgo

Sistema Cliente

Herramientas de Monitoreo y Compliance - SecuriaSGSI

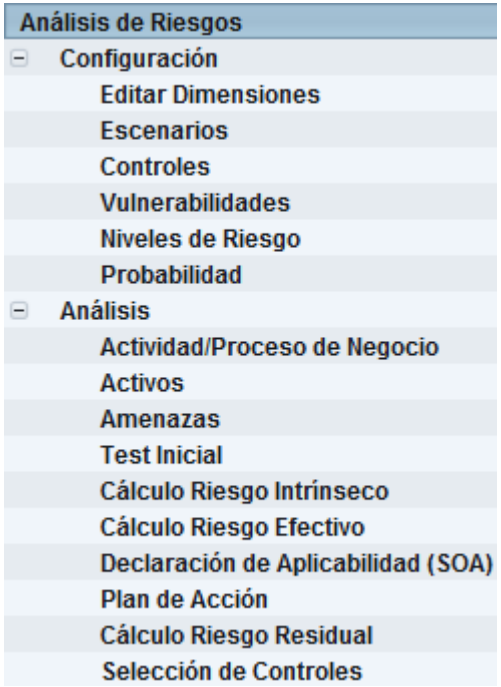
Gestión Documental – Creación de documento



Herramientas de Monitoreo y Compliance - SecuriaSGSI

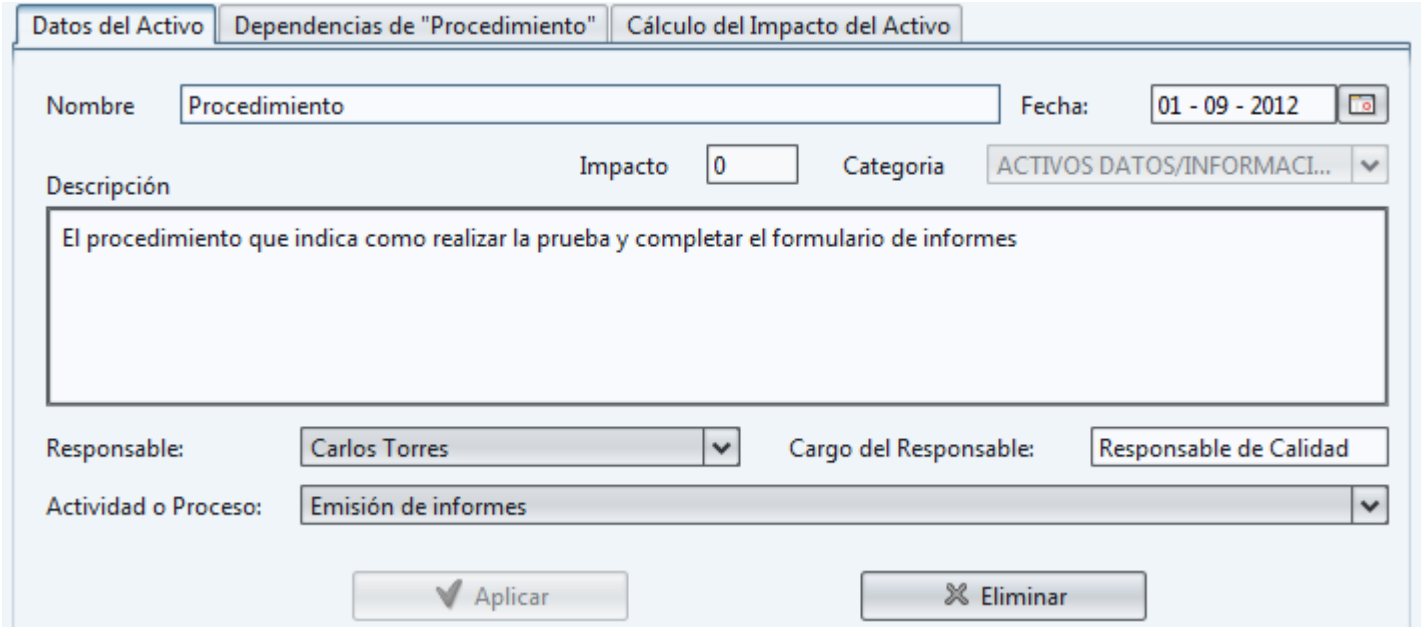
Análisis y Gestión de Riesgos

Configuración
+
Análisis
=
Cálculo del Riesgo



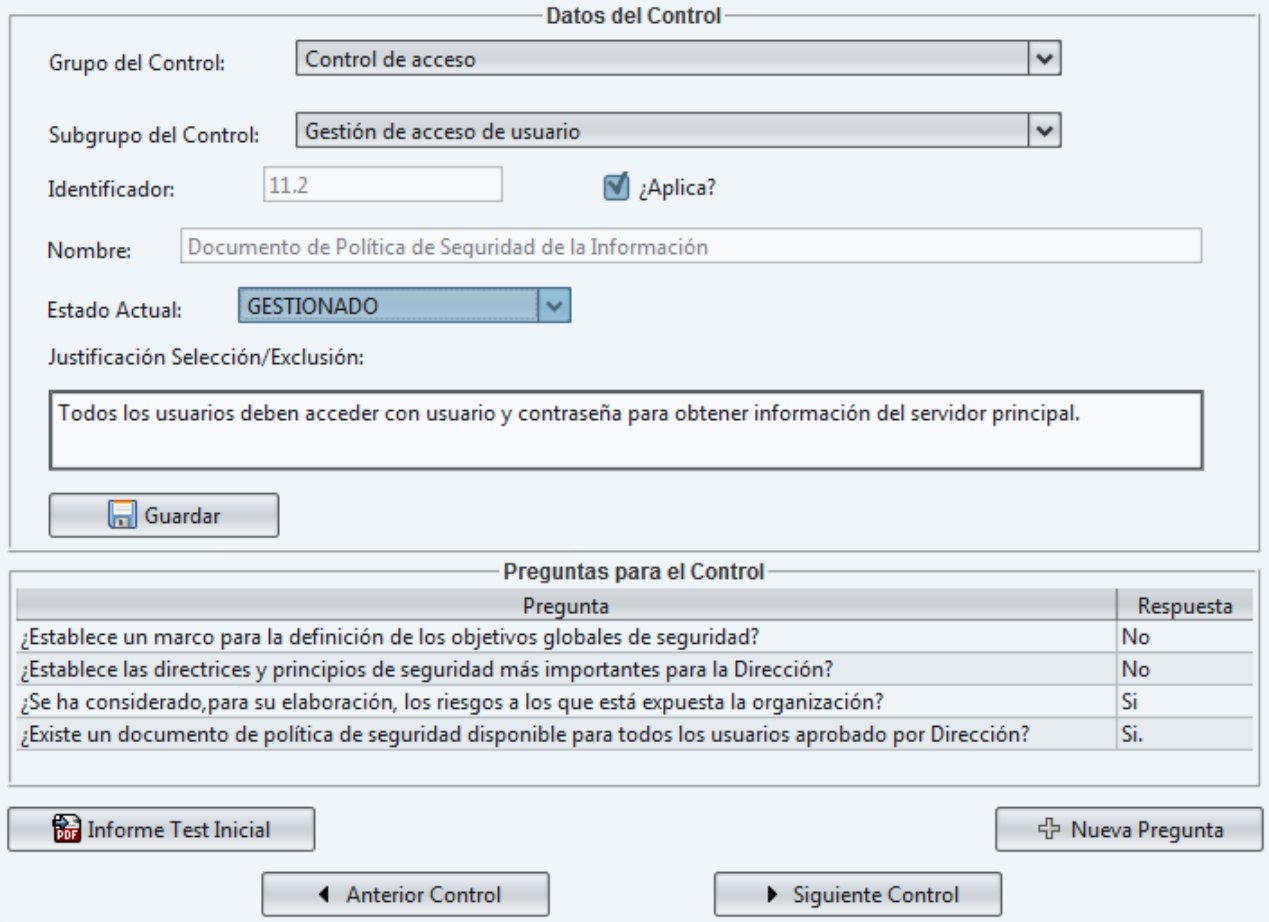
Herramientas de Monitoreo y Compliance - SecuriaSGSI

Activos



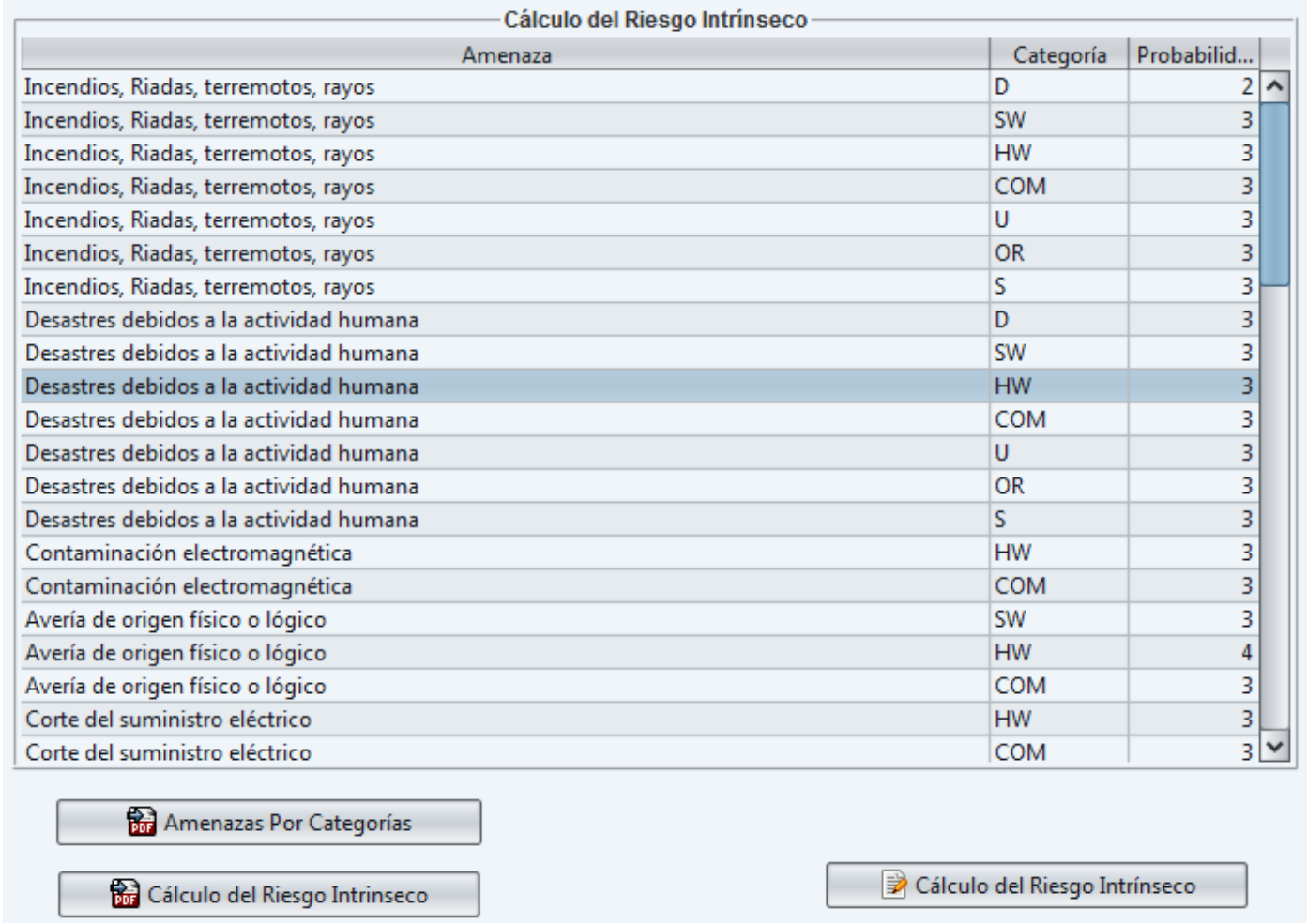
Herramientas de Monitoreo y Compliance - SecuriaSGSI

Test Inicial



Herramientas de Monitoreo y Compliance - SecuriaSGSI

Riesgo intrínseco



Herramientas de Monitoreo y Compliance - SecuriaSGSI

Riesgo intrínseco

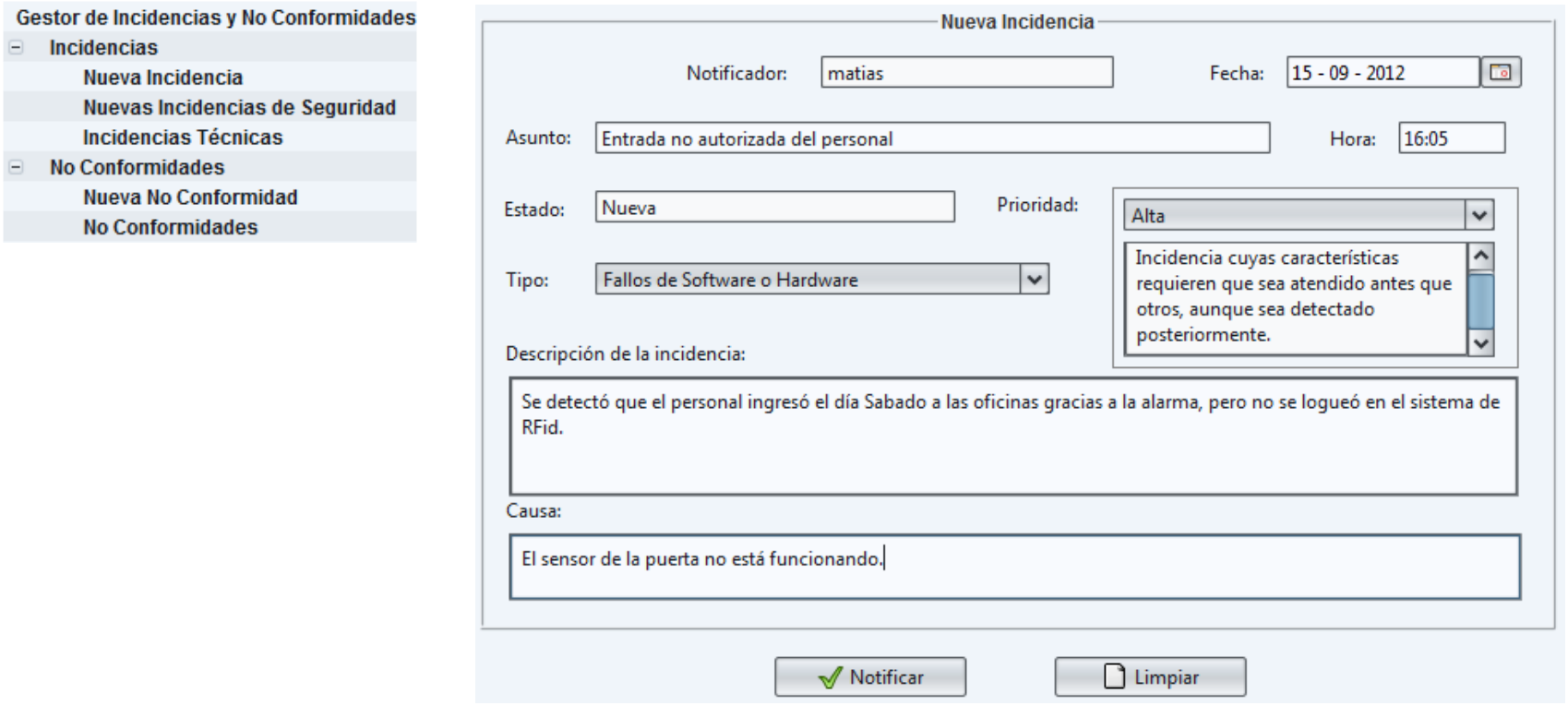
Categoría	Activo	C1	C2	D1	D2	D3	I1	I2
D	Procedimiento	1	3	2	3	5	2	5
D	Procedimiento	1	3	2	3	5	2	5
D	Procedimiento	1	3	2	3	5	2	5
D	Procedimiento	1	3	2	3	5	2	5

Amenaza	P	C	D	I
Desastres debidos a la actividad humana	3	☐	☑	☐
Difusión de software dañino	3	☐	☑	☐
Divulgación de información	3	☑	☐	☐
Errores de los usuarios	3	☑	☑	☑

C1	C2	D1	D2	D3	I1	I2
0	0	6	9	15	0	0
0	0	6	9	15	0	0
3	9	0	0	0	0	0
3	9	6	9	15	6	15

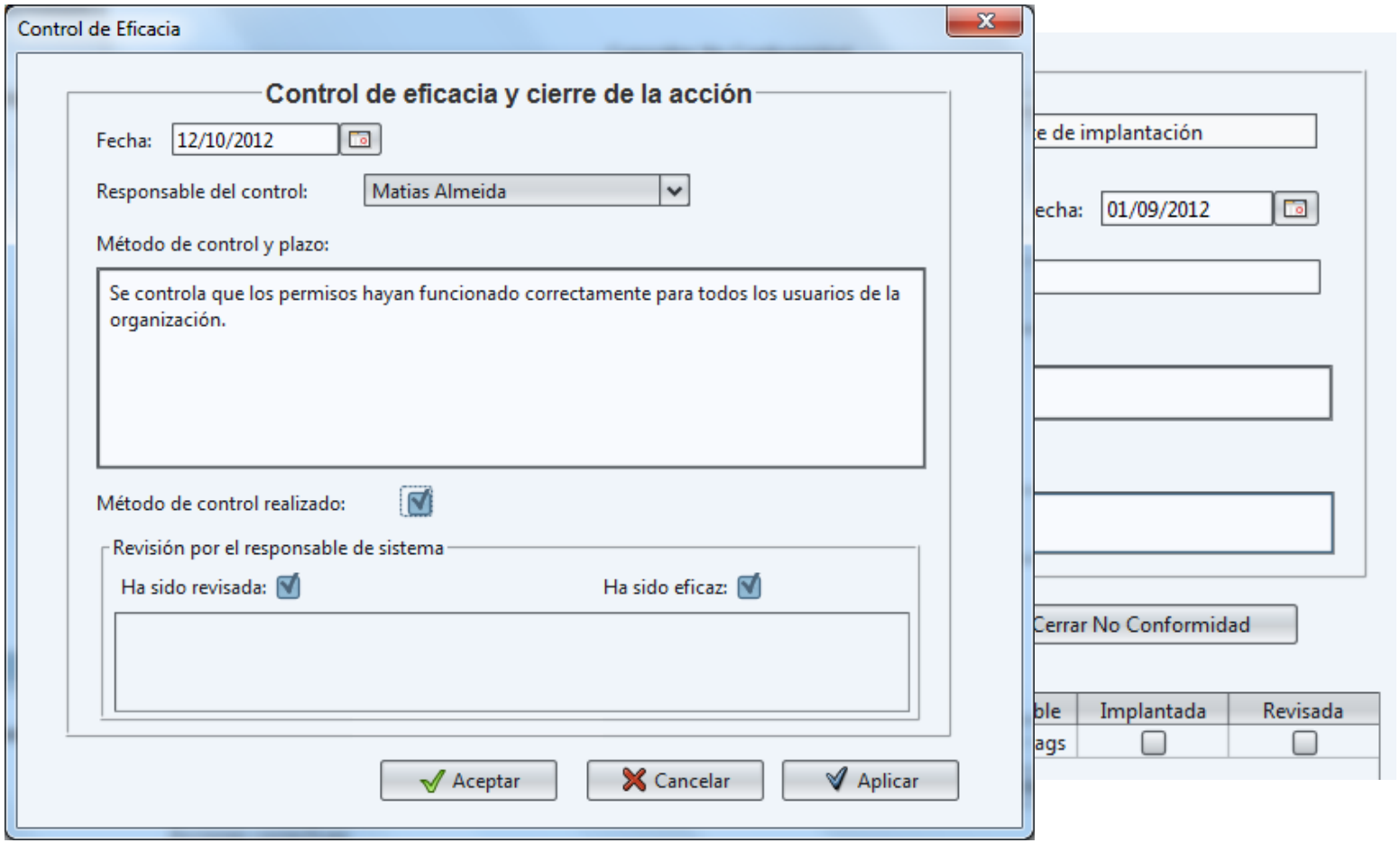
Herramientas de Monitoreo y Compliance - SecuriaSGSI

Gestión de Incidencias y No conformidades - Incidencias



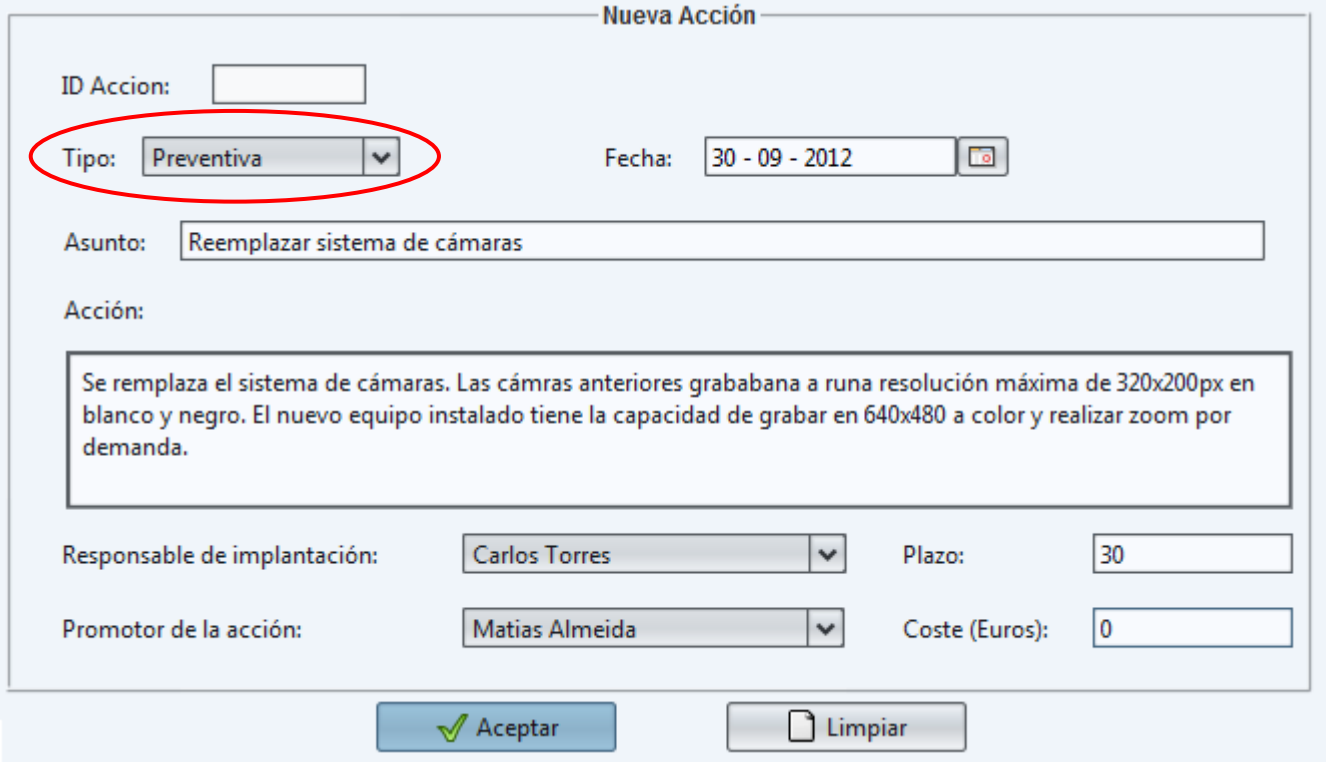
Herramientas de Monitoreo y Compliance - SecuriaSGSI

Gestión de Incidencias y No conformidades – No conformidades



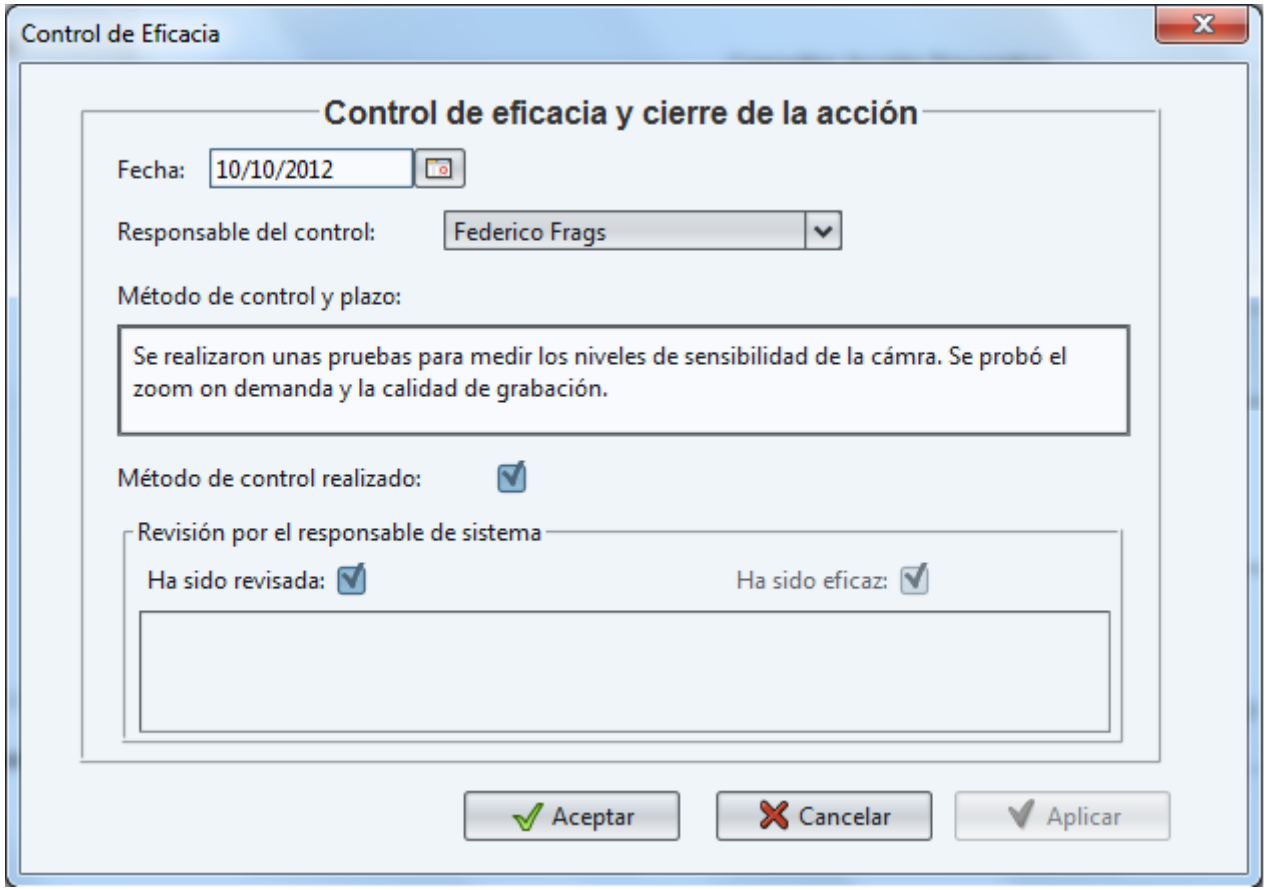
Herramientas de Monitoreo y Compliance - SecuriaSGSI

Mejora continua – Nueva acción



Herramientas de Monitoreo y Compliance - SecuriaSGSI

Mejora continua – control de eficacia



Herramientas de Monitoreo y Compliance - SecuriaSGSI

Conclusiones

Ventajas

- Muy completa en el manejo de la norma
- A partir de una incidencia puede generarse una no conformidad
- A partir de una no conformidad se puede definir una acción correctiva y luego medir su eficacia

Limitaciones

- Definición confusa entre Grupos y Perfiles.
- La notificaciones no son automáticas
- Bugs del sistema

Herramientas de Monitoreo y Compliance - Easy2Comply

¿Que es Easy2Comply?

Es una herramienta comercial y de código cerrado que está compuesta por cinco productos diferentes que manejan un control interno, el riesgo, IT-GRC, auditorías y herramientas de compliance. Es altamente configurable y puede adaptarse a cualquier organización y a cualquier norma.

Herramientas de Monitoreo y Compliance - Easy2Comply

¿Como funciona Easy2Comply?

Es un sistema cliente-servidor accedido a traves de un usuario y contraseña

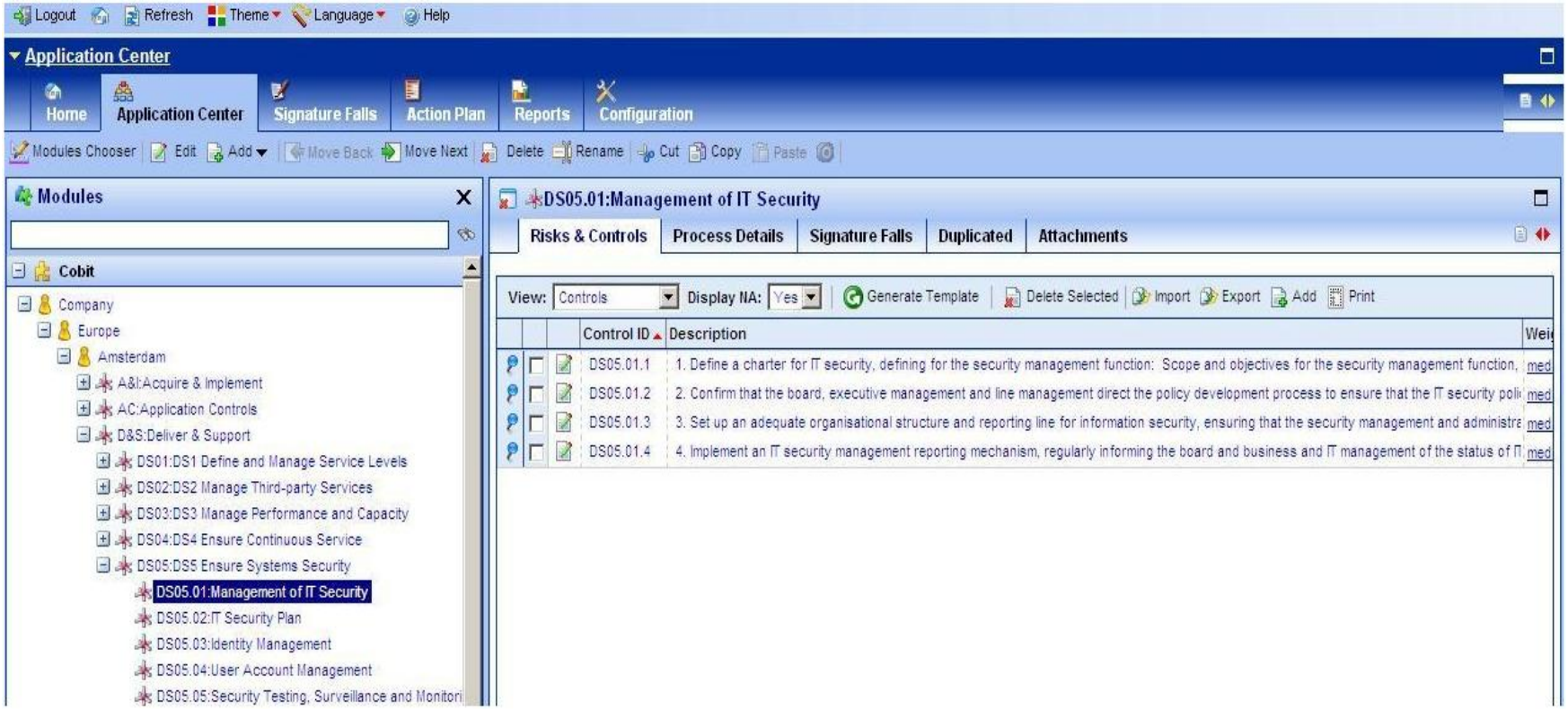
El panel principal o dashboard contiene los siguientes items:

- Documentación y Pérdida / Asesoramiento del Riesgo
- Eventos de Pérdida / Incidentes de Seguridad
- Indicadores claves de Riesgo / Métricas de Riesgo
- Firma
- Reportes
- Dashboard
- Plan de acción
- Configuración del sistema

Herramientas de Monitoreo y Compliance - Easy2Comply

Herramientas de Monitoreo y Compliance - Easy2Comply

Centro de aplicación

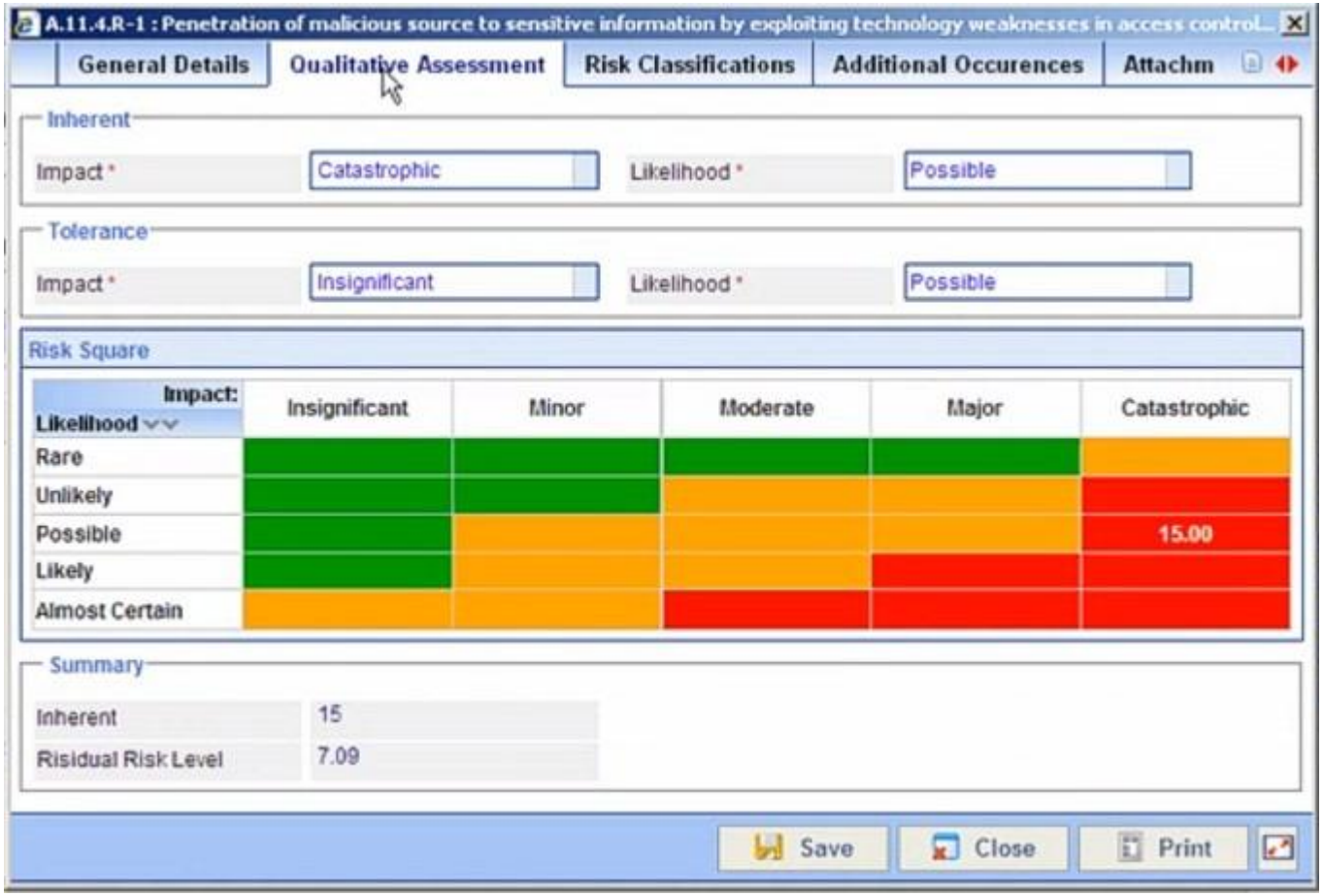


Herramientas de Monitoreo y Compliance - Easy2Comply

Detalles de un control

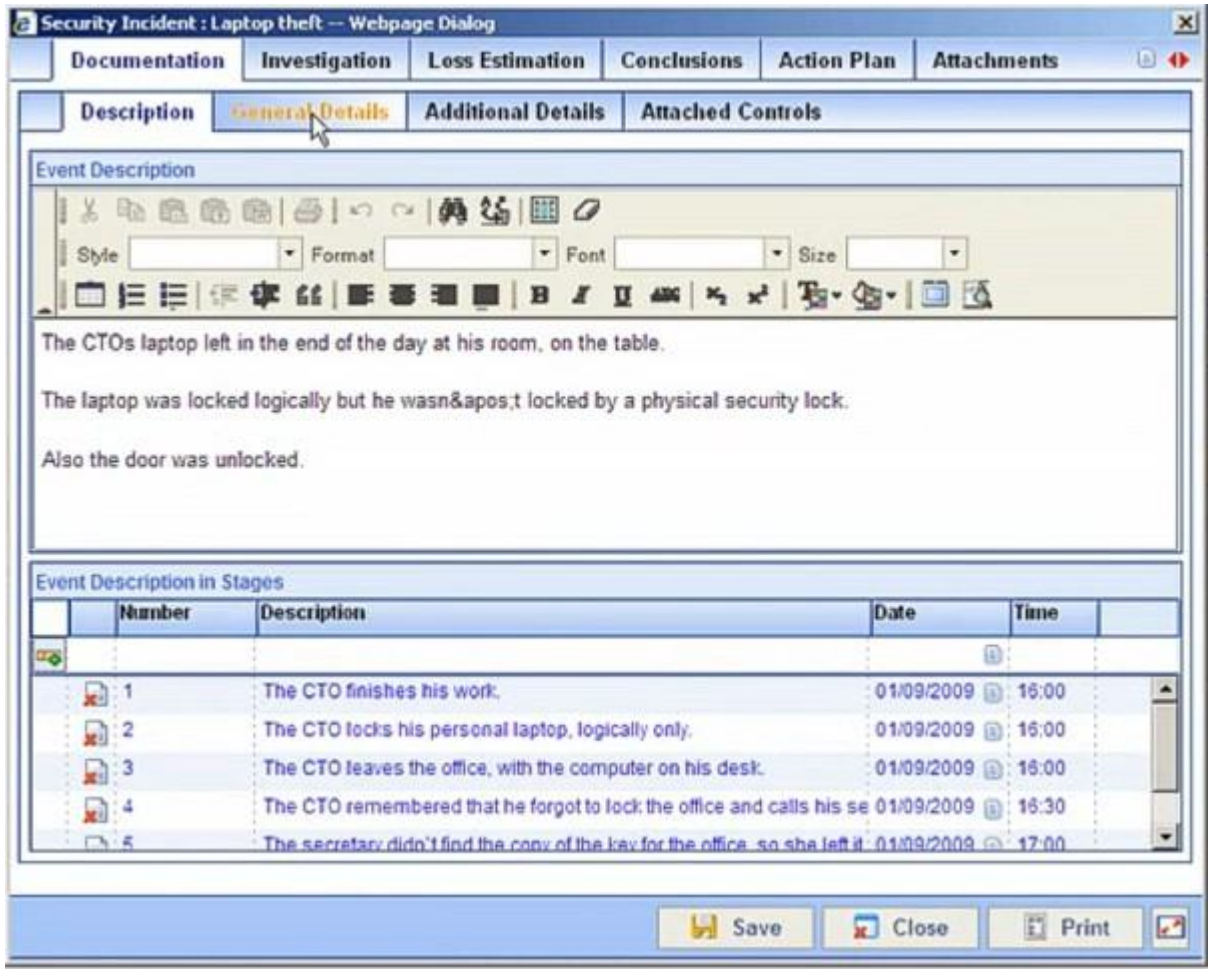
Herramientas de Monitoreo y Compliance - Easy2Comply

Plan de acción

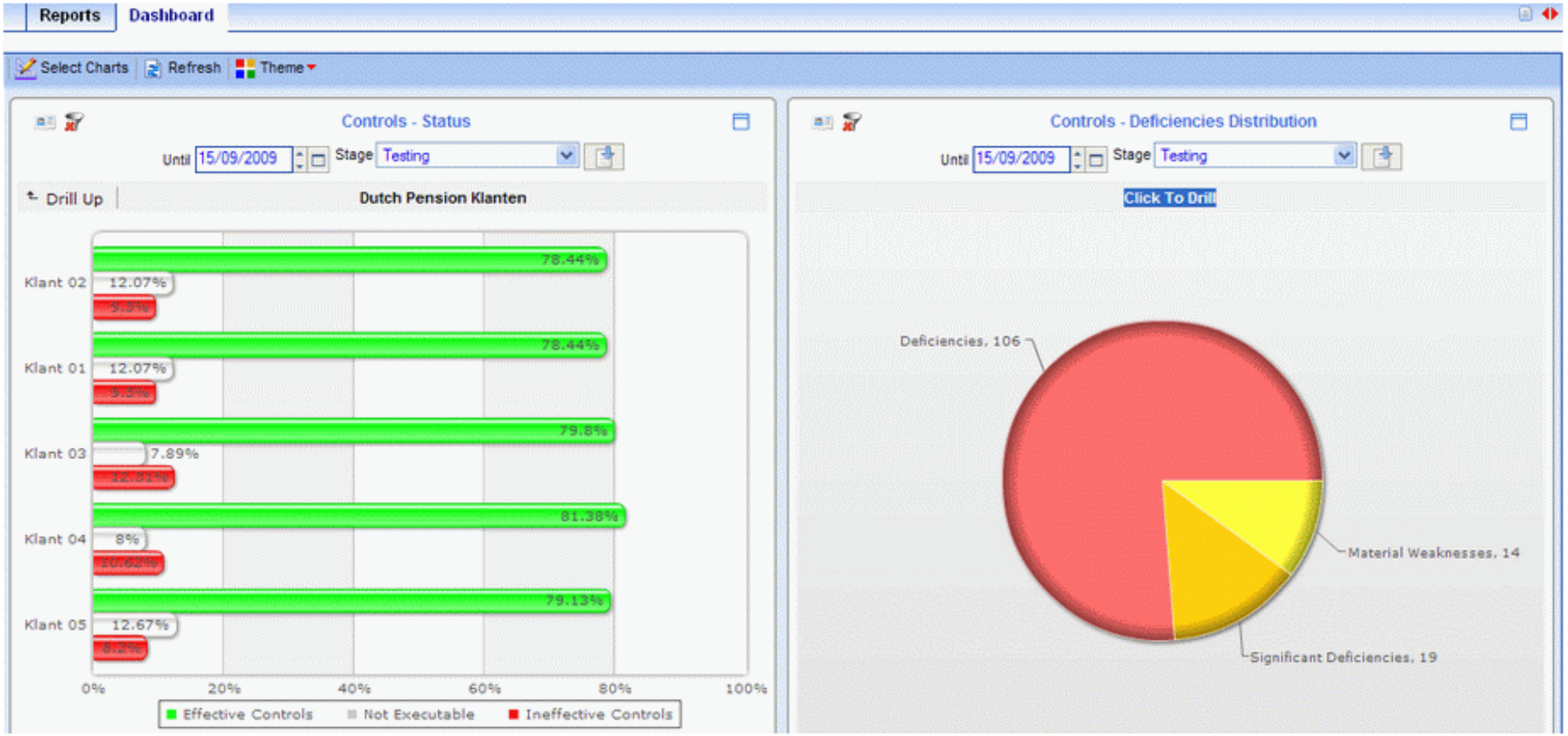


Herramientas de Monitoreo y Compliance - Easy2Comply

Incidentes de seguridad



Herramientas de Monitoreo y Compliance - Easy2Comply



Herramientas de Monitoreo y Compliance - Easy2Comply

Conclusiones

Ventajas

- Herramienta altamente personalizable a los requerimientos de la organizacion
- Adaptacion a cualquier norma ISO/IEC
- Seguimiento de revisiones segun calendario

Limitaciones

- No tiene monitorización a nivel de activos ni de red

Conclusiones

- Cuadro comparativo y checklist

Analisis comparativo de las herramientas

Características	OSSIM	OpenNMS	HypericHQ	Easy2Comply	SecuriaSGSI
Manejo de Activos	✔	✔	✔	✔	✔
Tratamiento de Riesgos	✔	✖	✖	✔	✔
Gestión de Documentación	✖	✖	✖	✔	✔
Compliance Checklist	✔	✖	✖	✔	✔
Monitoreo	✔	✔	✔	✖	✖
Plan de Pruebas	✖	✖	✖	✔	✔
% Cumplimiento	66 %	33 %	33 %	83 %	83 %

Conclusiones

- Herramientas e ISO 27001

Análisis de cumplimiento de las herrmientas segun las secciones de la norma ISO27001

Sección ISO27001	OSSIM	OpenNMS	HypericHQ	Easy2Comply	SecuriaSGSI
4 SGSI	-	-	-	-	-
4.2 Establecer el SGSI	✔	✔	✔	✔	✔
4.3 Documentacion	✖	✖	✖	✔	✔
4.3.1 General	✖	✖	✖	✔	✔
4.3.2 Control de documentos	✖	✖	✖	✔	✔
4.3.3 Control de Registros	✖	✖	✖	✖	✖
5 Responsabilidad de la direccón	-	-	-	-	-
6 Auditorias Internas	✔	✖	✖	✔	✔
7 Revisión gerencial del SGSI	✔	✔	✔	✔	✔
7.2 Insumo de la revisión	✔	✔	✔	✔	✔
7.3 Resultado de la revisión	✔	✖	✖	✔	✔
8 Mejora del SGSI	-	-	-	-	-
8.2 Acción correctiva	✖	✖	✖	✖	✔
8.3 Acción preventiva	✔	✔	✔	✖	✔

Conclusiones

- Especificación de requerimientos

Características deseadas

- Manejo de Activos
- Tratamiento de Riesgos
- Gestion de Documentación
- Compliance Checklist
- Monitoreo
- Plan de Pruebas

Conclusiones
- Aportes 27004

Aportes de la ISO 27004

- Propone el programa de medición
- Define un modelo y una estructura de medición
- Da recomendaciones para construírlos
- Anexo A - Provee un template para registrar los datos recolectados durante la ejecución del programa
- Anexo B - Provee ejemplos del template anterior

Conclusiones
- Aportes de la Tesis

Resumiendo…

- Queda una síntesis de la norma 27001 y 27004
- Explicitamos los aportes de la 27004
- Comparación de herramientas de Monitoreo y Compliance
- Aplicabilidad de las herramientas investigadas a cada una de las secciones de la norma
- Especificación de requerimientos para una futura implementación

FIN

¿Preguntas?