

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.

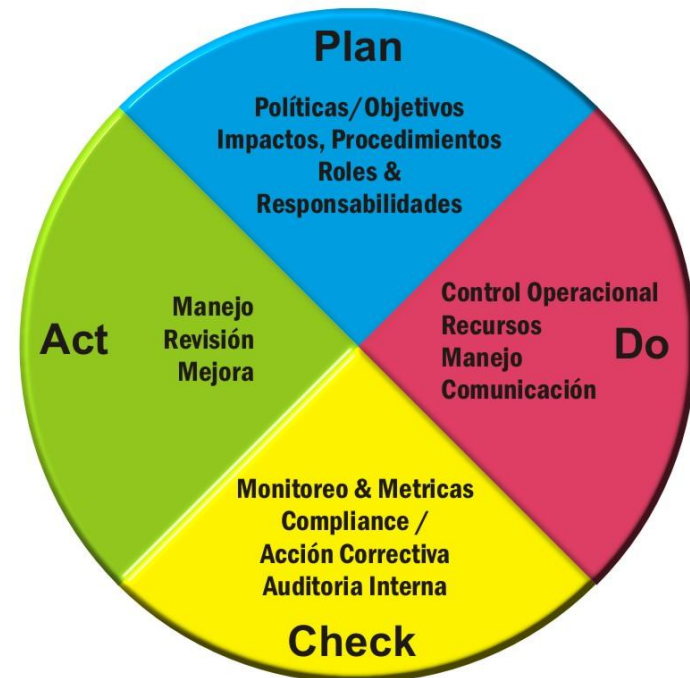
Objetos de Análisis

- Conceptos Teóricos

🐞 ¿Qué es ISO?

🐞 ¿Qué es un SGSI?

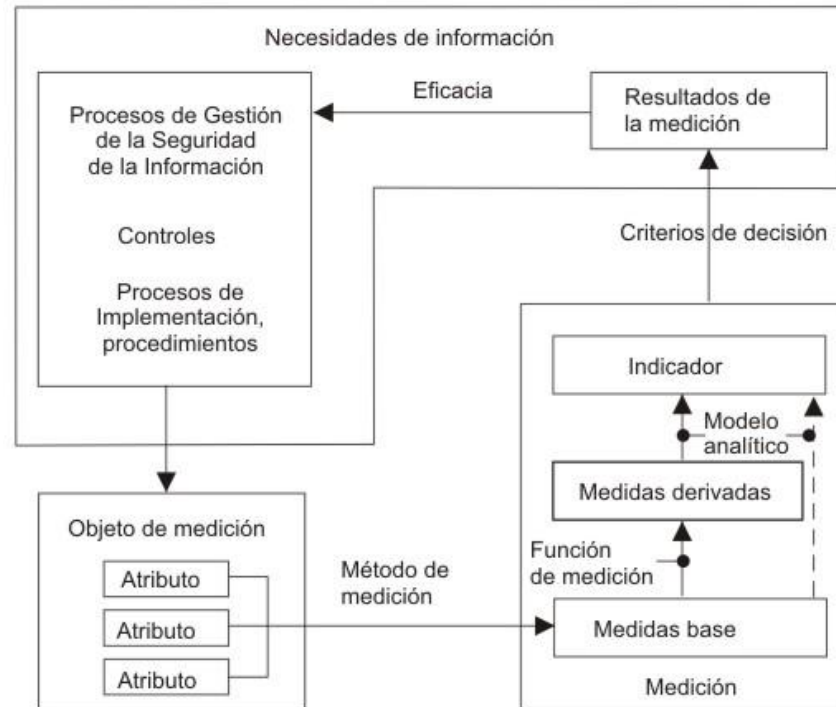
La norma define requerimientos generales y genéricos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI.



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?

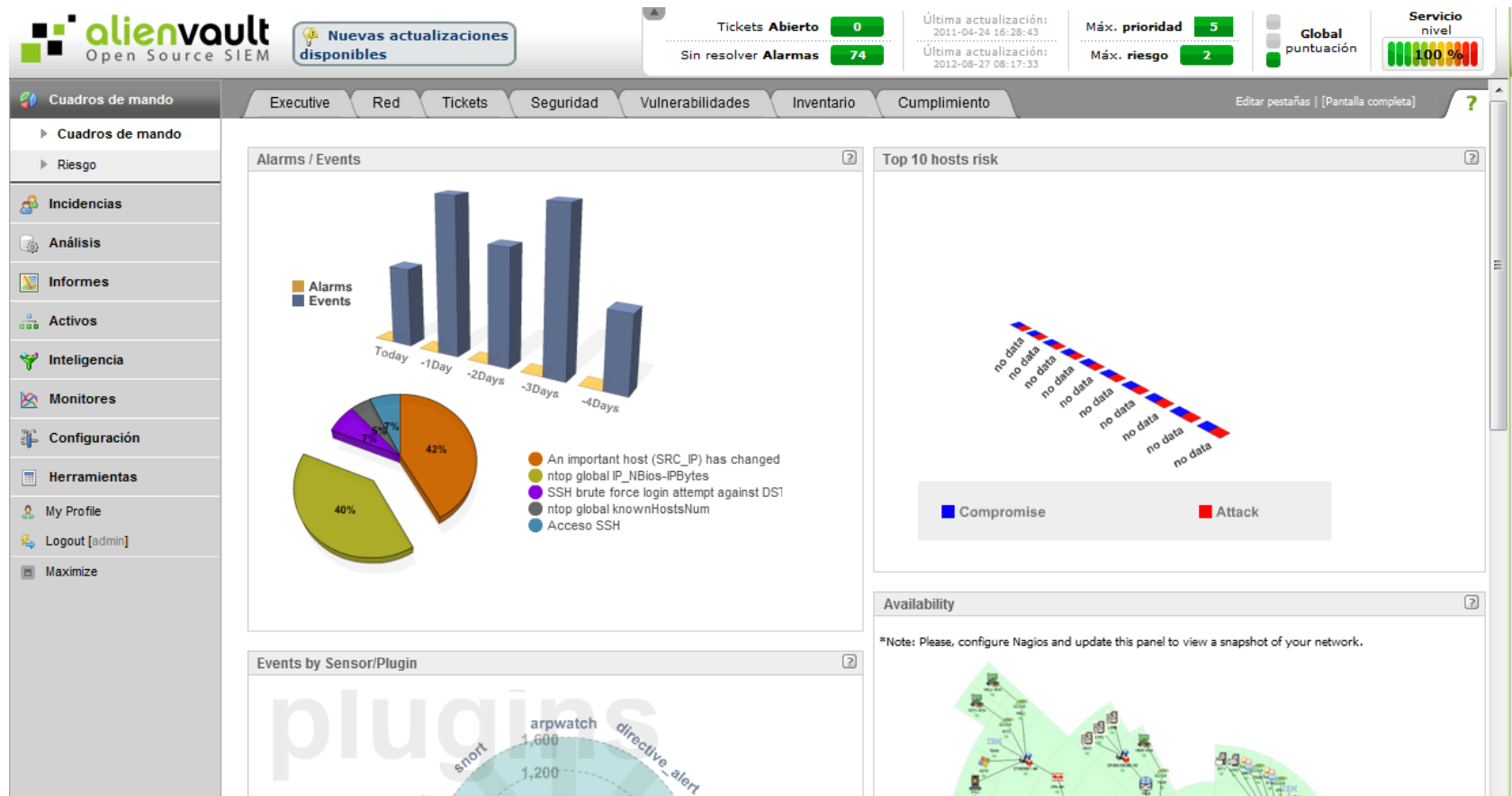
Es un herramienta de monitoreo y compliance gratuita y de código abierto aunque también puede encontrarse versiones comerciales mas completas.

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

Herramientas de Monitoreo y Compliance

- OSSIM

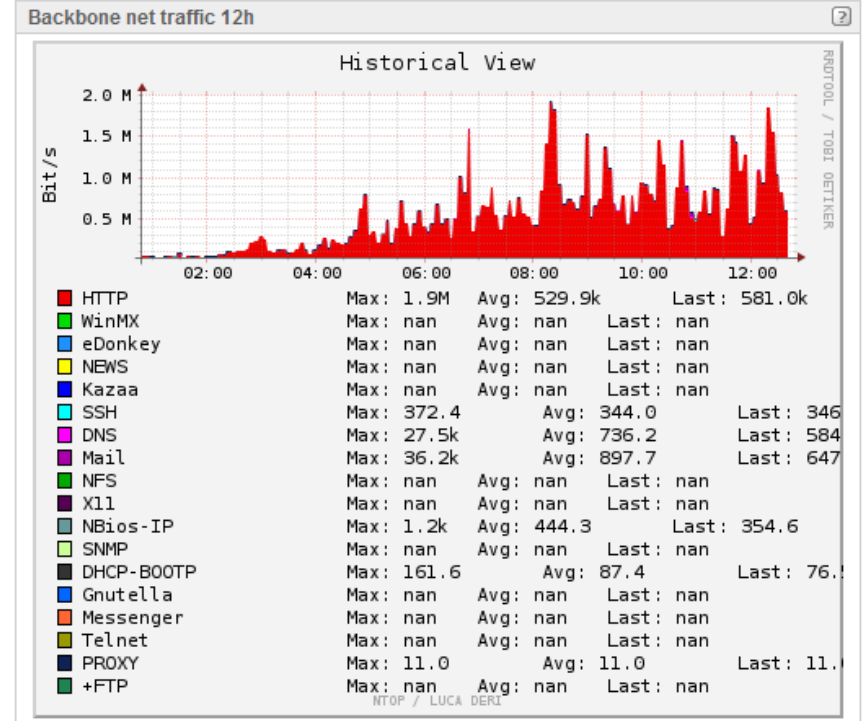
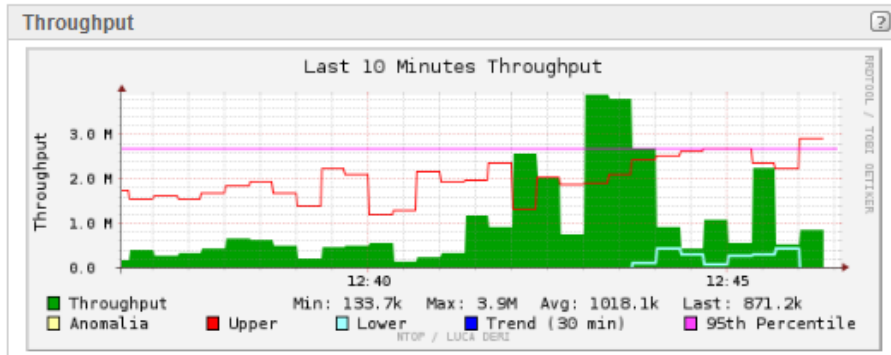
Vista Principal



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

SIEM

Wireless

Anomalías

Estadísticas

Administrar referencias

?

1h

3h

5h

7h

9h

11h

Real Time

Search | Clear

IP

Signature

Payload

Sensor

Orígenes de datos

Riesgo

Más filtros

Selecció del tiempo de frame: 3.1

Today | Last 24 Hours | Last Week | Last two Weeks | Last Month | All

Criterios de búsqueda actuales [...Clear All Criteria...]

META	PAYLOAD	IP	CAPA 4
time >= [09 / 15 / 2012] [any time] ...Clear...	any	any	none

Summary Statistics

Eventos	Sensors	Unique Events	Plugins únicos
Unique addresses: Source Destination	Source Port: TCP UDP	Destination Port: TCP UDP	Unique IP links [FQDN] Eventos únicos por país

Vistas predefinidas

► Displaying events 1-50 of 365 matching your selection. 4,047 total events in database.

☐	Evento	▲ Fecha ▼	Origen	Dest.	Activo S ↔ D	Prio	Rel	Riesgo	L4-PROTO
☐	directive_event: Acceso SSH	2012-09-15 11:47:00	163.10.75.227	opensourcesim	2->2	4	1	0->0	TCP
☐	pam_unix: authentication successful	2012-09-15 11:46:57	opensourcesim	opensourcesim	2->2	1	1	0->0	TCP
☐	directive_event: SSH brute force login attempt against DST_IP	2012-09-15 11:45:56	163.10.75.227:49594	opensourcesim:22	2->2	4	1	0->0	TCP
☐	directive_event: SSH brute force login attempt against DST_IP	2012-09-15 11:45:56	163.10.75.227:49594	opensourcesim:22	2->2	4	1	0->0	TCP
☐	directive_event: SSH brute force login attempt against DST_IP	2012-09-15 11:45:56	163.10.75.227:49594	opensourcesim:22	2->2	4	1	0->0	TCP

Herramientas de Monitoreo y Compliance - OSSIM

Políticas y Acciones

Política

Acciones

Editar Grupos de Políticas

Default Group: Default Group Policy objects

Nuevo

Modificar

Borrar seleccionados

Duplicar seleccionados

Recargar políticas

Habilitar/deshabilitar política

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

Política

Acciones

Editar Grupos de Políticas

Origen *

Destino *

Puertos *

Grupos de plugins *

Sensores *

Rango de Tiempo *

Grupo de políticas *

➔

Consecuencias de la política

Acciones ¿Insertar nueva acción?

2 items selected

Remove all

Add all

⌵ Enviar email por evento en la ip

⌵ Enviar Email

Enviar mail al administrador de la red

OK

Reiniciar

Prioridad *

No cambiar

SIEM *

☒ Sí ☐ No

Califica eventos *

☒ Sí ☐ No

Correlar eventos *

☒ Sí ☐ No 1)

Correlación Cruzada *

☒ Sí ☐ No 1)

Almacenar eventos *

☒ Sí ☐ No 1)

Logger *

☐ Sí ☒ No "Sólo disponible en profesional SIEM"

Sign *

☐ Línea ☒ Bloque

Multinivel

☒ Sí ☐ No

Reenviar alarmas *

☐ Sí ☒ No "Sólo disponible en profesional SIEM"

Reenviar eventos *

☐ Sí ☒ No "Sólo disponible en profesional SIEM"

1) No se aplica a los targets sin base de datos asociada. El valor implícito es siempre No.

Descripción *

Enviar mail al administrador de la red

Activo *

☒ Sí ☐ No

Herramientas de Monitoreo y Compliance

- OSSIM

Directivas de Correlación

- Cuadros de mando
- Incidencias
- Análisis
- Informes
- Activos
- Inteligencia**
 - Política y acciones
 - Directivas de correlación
 - Compliance Mapping
 - Correlación Cruzada
- Monitores
- Configuración
- Herramientas
- My Profile
- Logout [admin]
- Maximize



Categorías actuales [Reiniciar servidor]

- ▶ Genérico [19 directivas] ✓ +
- ▶ Attacks [12 directivas] ✓ +
- ▶ Worms [1 directiva] ✓ +
- ▶ Webattack ✓ +
- ▶ Dos ✓ +
- ▶ Escaneo ✓ +
- ▶ Abnormal ✗ +
- ▶ Red ✓ +
- ▶ Troyanos ✓ +
- ▶ Otros [1 directiva] ✓ +
- ▶ Usuario ✗ +
- ▶ Alienvault Worms [8 directivas] ✓ +
- ▶ Alienvault Attacks [9 directivas] ✓ +
- ▶ Alienvault Misc ✓ +
- ▶ Alienvault Scada [2 directivas] ✓ +



Categorías actuales [Reiniciar servidor]

- ▶ Genérico [19 directivas] ✓ +
- ▼ Attacks [12 directivas] ✓ +

Eliminar	Identificación del	Nombre
✗	3001	Acceso SSH
✗	3010	Successful Attack: Reverse Shell Access to the System
✗	3011	POP3 Bruteforce against SRC_IP
✗	3012	FTP Bruteforce against SRC_IP
✗	3013	Command execution against webserver on DST_IP
✗	3014	File /etc/passwd access on DST_IP
✗	3015	SQL injection attempt against DST_IP
✗	3016	attack against DST_IP (Symantec Remote Management RTVScan Exploit)
✗	3017	sa account bruteforce against SRC_IP (SQL)

Herramientas de Monitoreo y Compliance

- OSSIM

Compliance mapping

Cuadros de mando

Incidencias

Análisis

Informes

Activos

Inteligencia

Política y acciones

Directivas de correlación

Compliance Mapping

Correlación Cruzada

Monitores

Configuración

Herramientas

My Profile

Logout [admin]

Maximize

A.10.8 Exchange of information

A.10.9 Electronic commerce services

A.10.10 Monitoring

A.11.1 Business requirement for access control

A.11.2 User access management

A.11.3 User responsibilities

A.11.4 Network access control

Controles de seguridad	Aplica	Implementado	Justificación	Plugins
A.11.4.1 Policy on use of network services	Excluidos	✗		
A.11.4.2 User authentication for external connections	Seleccionados	✓		1 Ref.
A.11.4.3 Equipment identification in networks	Seleccionados	✗		14 Ref.
A.11.4.4 Remote diagnostic and configuration port protection	Seleccionados	✗		
A.11.4.5 Segregation in networks	Excluidos	✗		
A.11.4.6 Network connection control	Seleccionados	✗		29 Ref.
A.11.4.7 Network routing control	Seleccionados	✗		17 Ref.

A.11.5 Operating system access control

A.11.6 Application and information access control

A.11.7 Mobile computing and teleworking

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

Alarmas

Informe

☒ Filtros, Acciones y Opciones

(0-50 de 103) [Siguiente 50 ->](#) [Últimos ->>](#)

Desagrupados | **Agrupados**

#	Alarma	Riesgo	Sensor	Desde	Últimos	Origen	Destino	Estado	Acción			
sábado 15-sep-2012 [Eliminar]												
☒ 1	Acceso SSH (1 eventos)	0	opensourcesim.alienvault	2012-09-15 11:19:12	2012-09-15 12:19:12	163.10.75.227:ANY	opensourcesim.alienvault:ANY	abierta				
#	Identificación del	Alarma	Riesgo	Fecha	Origen	Destino	Nivel de correlación					
1	185943	Acceso SSH	0	2012-09-15 12:19:12	163.10.75.227:ANY	opensourcesim.alienvault:ANY	1					
Resumen de Alarmas [Eventos Totales: 1 - Direcciones IP Destino Únicas: 1 - Tipos únicos: 1 - Puertos Destino Únicos: 1] - [Visualizar alarma]												
1 Total eventos que coinciden después de la regla de nivel más alto, antes de timeout.					Ver/Editar definición actual directiva							
☒ 2	SSH brute force login attempt against opensourcesim.alienvault (1 eventos)	0	opensourcesim.alienvault	2012-09-15 12:19:03	2012-09-15 12:19:03	163.10.75.227:ANY	opensourcesim.alienvault:ssh	abierta				
☒ 3	SSH brute force login attempt against opensourcesim.alienvault	0	opensourcesim.alienvault	2012-09-15 12:19:03	2012-09-15 12:19:03	163.10.75.227:50985	opensourcesim.alienvault:ssh	abierta				

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

The screenshot displays the OpenNMS Web Console interface. At the top, the OpenNMS logo is on the left, and the 'Web Console' header on the right shows the user 'admin (Notices Off)' with a 'Log out' link and the timestamp '17/08/2012 14:22 ART'. A navigation bar below the header contains links: Node List, Search, Outages, Path Outages, Dashboard, Events, Alarms, Notifications, Assets, Reports, Charts, Surveillance, Distributed Map, Map, Add Node, Admin, and Support.

The main content area is titled 'Home' and features several widgets:

- Nodes with Outages:** Lists nodes with active outages, including '163.10.25.4 (4 months)', 'www.fcv.unlp.edu.ar (4 months)', and 'tesis.fcv.unlp.edu.ar (8 months)'.
- Quick Search:** A search form with fields for 'Node ID:', 'Node label like:', 'TCP/IP Address like:', and 'Providing service:'. Each field has a 'Search' button. The 'Providing service:' dropdown is currently set to 'DHCP'.
- Availability Over the Past 24 Hours:** A table showing the availability status of various categories.
- Notification:** A section for managing notifications, showing 'You: No outstanding notices (Check)' and 'All: No outstanding notices (Check)'. It also includes a link to the 'On-Call Schedule'.
- Resource Graphs:** A section for resource graphs, currently showing '-- Choose A Node --'.
- KSC Reports:** A section for KSC reports, currently showing 'No KSC reports defined'.

The 'Availability Over the Past 24 Hours' table is as follows:

Categories	Outages	Availability
Network Interfaces	0 of 9	100.000%
Web Servers	1 of 5	80.000%
Email Servers	0 of 3	100.000%
DNS and DHCP Servers	2 of 2	0.000%
Database Servers	1 of 3	66.667%
JMX Servers	0 of 0	100.000%
Other Servers	0 of 9	100.000%
Total	Outages	Availability
Overall Service Availability	5 of 33	84.848%

Herramientas de Monitoreo y Compliance

- OpenNMS

Detalle de servicios de un host determinado

Node: mail.sievm.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.sievm.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...				

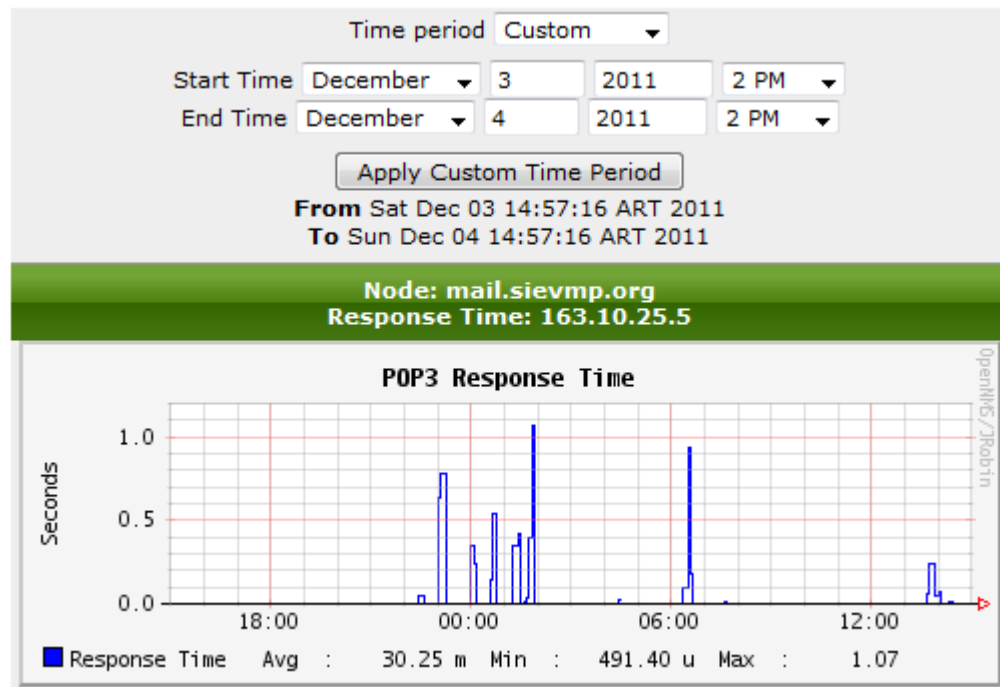
Recent Outages

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

Estadísticas de eventos ocurridos



Herramientas de Monitoreo y Compliance

- OpenNMS

Caídas

Home / Outages / List

Results: (1-20 of 150)

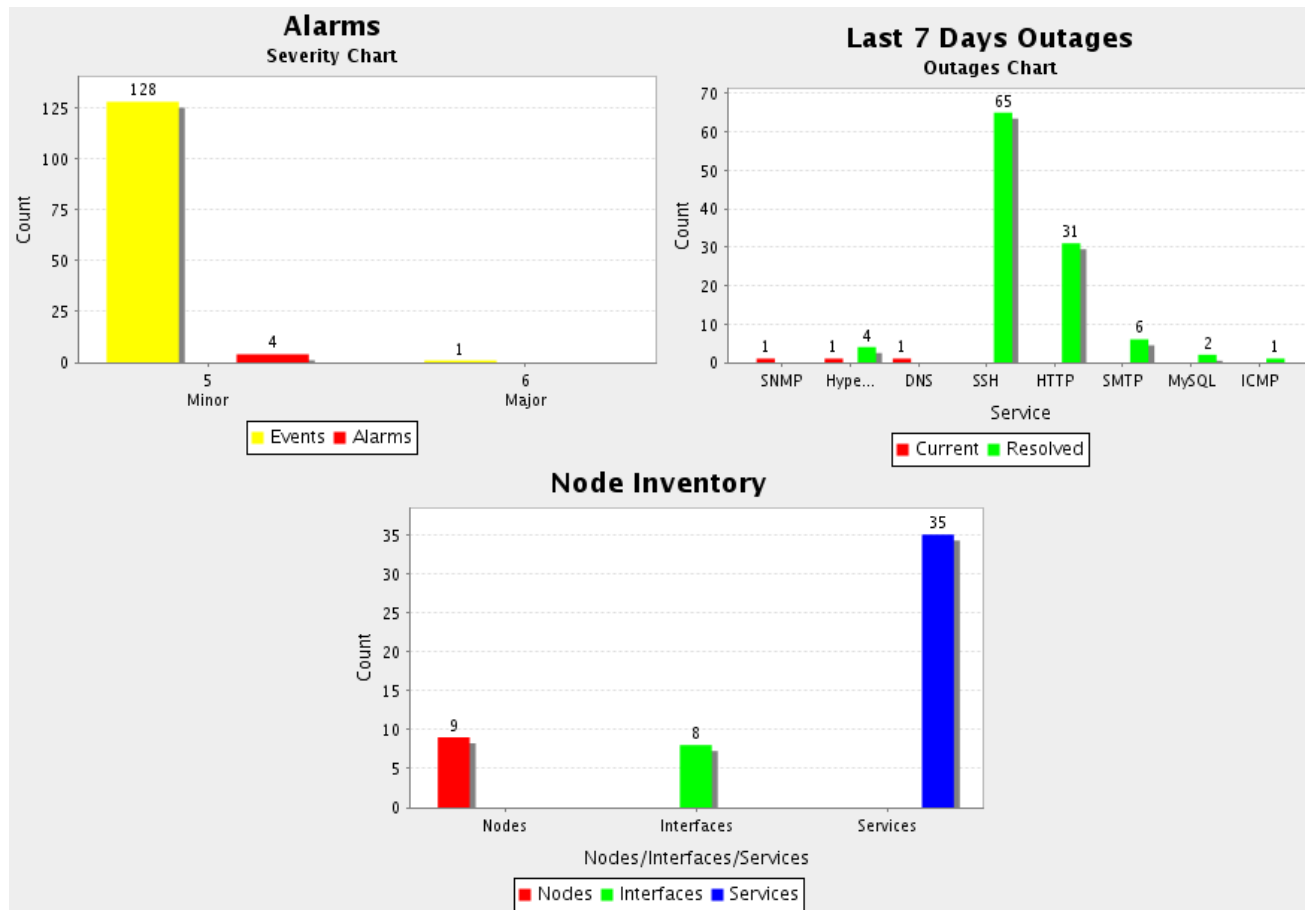
Outage type:

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

Estadísticas de eventos de la red



Herramientas de Monitoreo y Compliance

- OpenNMS

Conclusiones

Ventajas

- 🐜 Descubrimientos dinámico 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 días. 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

HYPERIC HQ

Recent Alerts: (There have been no alerts in the last 2 hours.)

Welcome, HQSign OutScreencastsHelp

DashboardResourcesAnalyzeAdministration

Search Resources

Resource NamePlatforms

Saved Charts

No charts to display

Recently Added

No resources to display

Availability Summary

Resource Type	Availability
No resources to display, please click the icon above to add resources to portlet.	

Add content to this column:

Select Portlet

Auto-Discovery

Resource Name	Status	Changes
Informatica-PC - Microsoft Windows 7	modified	fqdn changed, IP set changed, server set changed

Add to InventorySkip Checked Resources

Favorite Resources

Resource Name	Resource Type	Availability	Alerts
No resources to display, please click the icon above to add resources to portlet.			

Updated: 7:19 PM

Recent Alerts

Date / Time	Alert Name	Resource Name	Fixed	Ack
No recent alerts to display				

FIXEDACKNOWLEDGE

Updated: 7:19 PM

Control Actions

Recent Control Actions

No resources to display

Quick Control Frequency

No resources to display

Herramientas de Monitoreo y Compliance

- HypericHQ

Servicios de un activo

Browse > tesis.fcv.unlp.edu.ar		
Description: Debian 6.0.3	Owner: HQ Administrator (hqadmin) - Change...	
Default Gateway : 163.10.25.1	Vendor : Debian	Vendor Version : 6.0.3
IP Address : 163.10.25.7	Primary DNS : 163.10.25.2	CPU Speed : 2266 MHz
OS Version : 2.6.32-5-amd64	RAM : 2048 MB	Architecture : x86_64

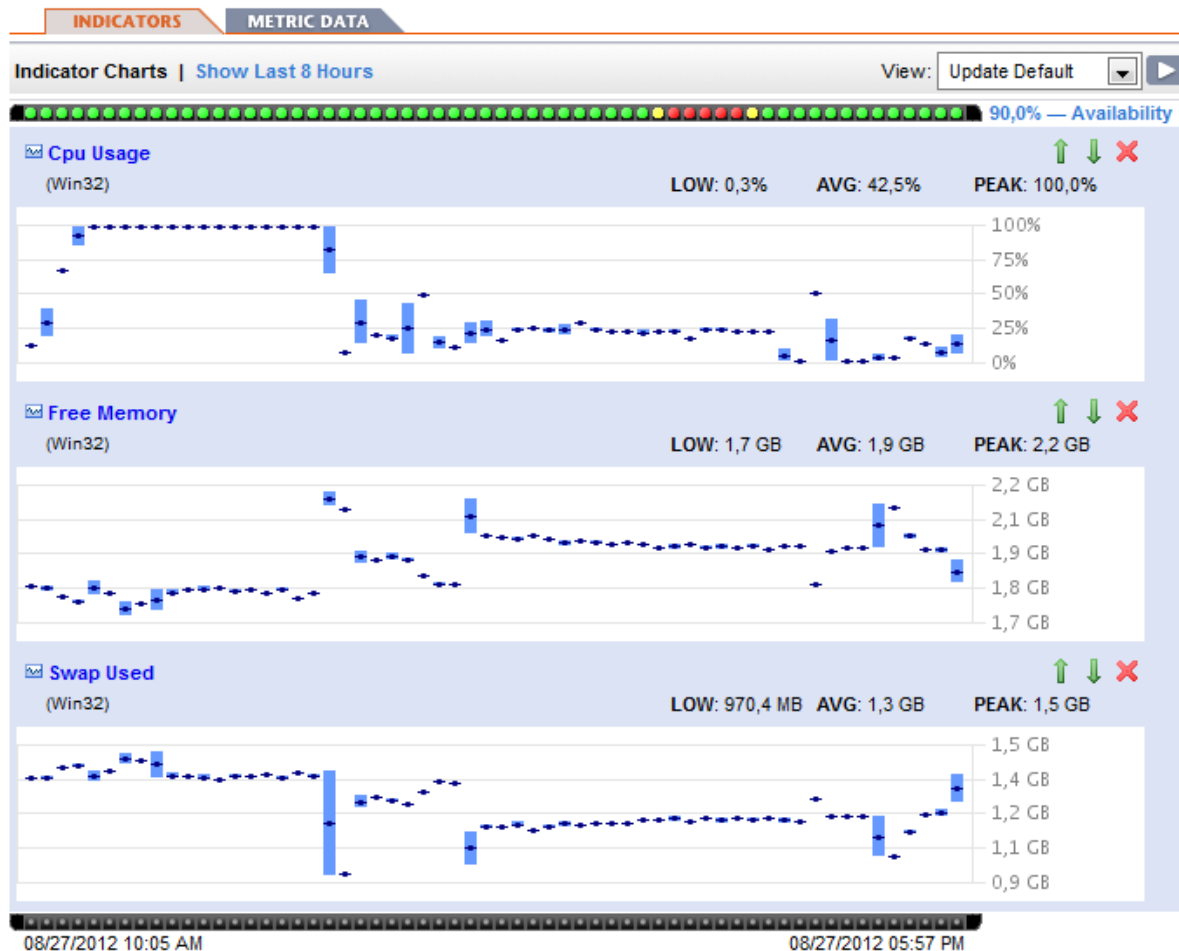
Disponibilidad de sus servicios

RESOURCES		
☐	Platform Services Health	Avail
☐	FileServer Mount	✓
☐	NetworkServer Interface	✓
☐	tesis.fcv.unlp.edu.ar Linux CPU 1 (2266Mhz Intel Xeon)	✓
☐	tesis.fcv.unlp.edu.ar Linux sshd Process	✓
☐	Deployed Servers Health	Avail
☐	tesis.fcv.unlp.edu.ar HQ ActiveMQ Embedded 5.3	✓
☐	tesis.fcv.unlp.edu.ar HQ Agent 4.6	✓
☐	tesis.fcv.unlp.edu.ar HQ PostgreSQL 8.2	✓
☐	tesis.fcv.unlp.edu.ar HQ Tomcat 6.0	✓
Select Resources above & click button to view metrics		
View Metrics		

Herramientas de Monitoreo y Compliance

- HypericHQ

Indicadores de un activo



Herramientas de Monitoreo y Compliance - HypericHQ

Definición de alerta - Reglas

Condition Set

*** If Condition:** ☒ Metric: 

 ☒ is  (absolute value)

☐ value changes

☐ Inventory Property:  value changes

☐ Events/Logs Level:  and match substring (optional, 150 chars max):

☐ Config changed and match file name (optional, 150 chars max):

*** Enable Action(s):** ☒ Each time conditions are met

☐ Once every times conditions are met within a time period of 

☒ Generate one alert and then disable alert definition until fixed

Herramientas de Monitoreo y Compliance

- HypericHQ

Definición de alerta - Esquemas de notificaciones y definición de Plantilla

Step 2 - Create Escalation Scheme Actions:

Create an Action for this escalation	Action Details
Email Notify HQ Users Then continue	Action: Email Notify: hqadmin,

An escalation scheme allows you to order alert notifications and actions. It can be applied to one or more alert definitions.

Step 1 - Create New Escalation Scheme for Prueba:

*** Name:**

Description:

If the alert is acknowledged:

☒ Allow user to pause escalation for

☐ Continue escalation without pausing

If the alert state has changed:

☒ Notify previously notified users of the change

☐ Notify entire escalation chain of the change

If alert is not fixed when escalation ends:

☒ Stop escalation execution

☐ Repeat escalation actions

Herramientas de Monitoreo y Compliance

- HypericHQ

Centro de Alertas y Eventos

Alert Center

AlertsDefinition

Alert Filter

Show:
☐ Not Fixed
☐ In Escalation
☒ All

Minimum priority:
! Low

In the last:
day

Group:
-- All Groups --

Resource Alerts

PreviousPage 1Next

☐	Date	Alert Definition	Resource	Platform	Fixed	Ack	Priority
☒	04/12/11 19:56	Prueba	tesis.fcv.unlp.edu.ar	tesis.fcv.unlp.edu.ar	No		High

FIXED**ACKNOWLEDGE**

Click the icon to acknowledge an alert

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 herramienta 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

Gestor Documental

- Nuevo Documento
- Biblioteca
 - Lectura Obligada (1)
 - Biblioteca Documental

Ficha del documento | **Obligada lectura** | **Documentos relacionados**

Datos del Documento

ID: Nombre:

Estado: Código: Versión:

Instrucciones Técnicas:

Fecha Creación:

Fecha Caducidad:

Fecha Aprobación:

Versión	Autor	Fecha de Aprobación	Aprobado	Aprobador
0.0	Carlos Torres	2012-09-03	☐	

Modificar datos del fichero "Cableado Estructurado"

Nombre:

Versión:

Autor:

Fecha de Aprobación:

Aprobado: ☒

Aprobador:

Herramientas de Monitoreo y Compliance

- SecuriaSGSI

Análisis y Gestión de Riesgos

Configuración
+
Análisis
=
Cálculo del Riesgo

Análisis de Riesgos	
[-]	Configuración
	Editar Dimensiones
	Escenarios
	Controles
	Vulnerabilidades
	Niveles de Riesgo
	Probabilidad
[-]	Análisis
	Actividad/Proceso de Negocio
	Activos
	Amenazas
	Test Inicial
	Cálculo Riesgo Intrínseco
	Cálculo Riesgo Efectivo
	Declaración de Aplicabilidad (SOA)
	Plan de Acción
	Cálculo Riesgo Residual
	Selección de Controles

Herramientas de Monitoreo y Compliance

- SecuriaSGSI

Activos

Datos del Activo		Dependencias de "Procedimiento"		Cálculo del Impacto del Activo	
Nombre	Procedimiento			Fecha:	01 - 09 - 2012
Descripción	Impacto	0	Categoría	ACTIVOS DATOS/INFORMACI...	
El procedimiento que indica como realizar la prueba y completar el formulario de informes					
Responsable:	Carlos Torres		Cargo del Responsable:	Responsable de Calidad	
Actividad o Proceso:	Emisión de informes				
✓ Aplicar			✕ Eliminar		

Herramientas de Monitoreo y Compliance

- SecuriaSGSI

Test Inicial

Datos del Control

Grupo del Control:

Control de acceso

Subgrupo del Control:

Gestión de acceso de usuario

Identificador:

11.2

☒ ¿Aplica?

Nombre:

Documento de Política de Seguridad de la Información

Estado Actual:

GESTIONADO

Justificación Selección/Exclusión:

Todos los usuarios deben acceder con usuario y contraseña para obtener información del servidor principal.

Guardar

Preguntas para el Control

Pregunta	Respuesta
¿Establece un marco para la definición de los objetivos globales de seguridad?	No
¿Establece las directrices y principios de seguridad más importantes para la Dirección?	No
¿Se ha considerado, para su elaboración, los riesgos a los que está expuesta la organización?	Si
¿Existe un documento de política de seguridad disponible para todos los usuarios aprobado por Dirección?	Si.

Informe Test Inicial

Nueva Pregunta

Anterior Control

Siguiente Control

Herramientas de Monitoreo y Compliance

- SecuriaSGSI

Riesgo intrínseco

Cálculo del Riesgo Intrínseco			
Amenaza	Categoría	Probabilid...	
Incendios, Riadas, terremotos, rayos	D	2	^
Incendios, Riadas, terremotos, rayos	SW	3	
Incendios, Riadas, terremotos, rayos	HW	3	
Incendios, Riadas, terremotos, rayos	COM	3	
Incendios, Riadas, terremotos, rayos	U	3	
Incendios, Riadas, terremotos, rayos	OR	3	
Incendios, Riadas, terremotos, rayos	S	3	
Desastres debidos a la actividad humana	D	3	
Desastres debidos a la actividad humana	SW	3	
Desastres debidos a la actividad humana	HW	3	
Desastres debidos a la actividad humana	COM	3	
Desastres debidos a la actividad humana	U	3	
Desastres debidos a la actividad humana	OR	3	
Desastres debidos a la actividad humana	S	3	
Contaminación electromagnética	HW	3	
Contaminación electromagnética	COM	3	
Avería de origen físico o lógico	SW	3	
Avería de origen físico o lógico	HW	4	
Avería de origen físico o lógico	COM	3	
Corte del suministro eléctrico	HW	3	
Corte del suministro eléctrico	COM	3	v

 Amenazas Por Categorías

 Cálculo del Riesgo Intrínseco

 Cálculo del 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

Gestor de Incidencias y No Conformidades

- Incidencias
 - Nueva Incidencia
 - Nuevas Incidencias de Seguridad
 - Incidencias Técnicas
- No Conformidades
 - Nueva No Conformidad
 - No Conformidades

Nueva Incidencia

Notificador: Fecha:

Asunto: Hora:

Estado: Prioridad:

Tipo:

Descripción de la incidencia:

Se detectó que el personal ingresó el día Sabado a las oficinas gracias a la alarma, pero no se logueó en el sistema de RFid.

Causa:

El sensor de la puerta no está funcionando.

Herramientas de Monitoreo y Compliance

- SecuriaSGSI

Gestión de Incidencias y No conformidades – No conformidades

Control de Eficacia

Control de eficacia y cierre de la acción

Fecha: 12/10/2012

Responsable del control: Matias Almeida

Método de control y plazo:
Se controla que los permisos hayan funcionado correctamente para todos los usuarios de la organización.

Método de control realizado: ☒

Revisión por el responsable de sistema

Ha sido revisada: ☒ Ha sido eficaz: ☒

✓ Aceptar

✗ Cancelar

✓ Aplicar

Fecha de implantación

Fecha: 01/09/2012

Cerrar No Conformidad

Implantada	Revisada
☐	☐

Herramientas de Monitoreo y Compliance

- SecuriaSGSI

Mejora continua – Nueva acción

Nueva Acción

ID Accion:

Tipo: **Preventiva**  Fecha: 

Asunto:

Acción:

Se reemplaza el sistema de cámaras. Las cámaras anteriores grababan a una resolución máxima de 320x200px en blanco y negro. El nuevo equipo instalado tiene la capacidad de grabar en 640x480 a color y realizar zoom por demanda.

Responsable de implantación:  Plazo:

Promotor de la acción:  Coste (Euros):

 Aceptar  Limpiar

Herramientas de Monitoreo y Compliance

- SecuriaSGSI

Mejora continua – control de eficacia

The screenshot shows a software window titled "Control de Eficacia" with a standard Windows-style title bar (minimize, maximize, close buttons). The window contains a form for recording control effectiveness. The form has a title "Control de eficacia y cierre de la acción" and several input fields and checkboxes. The "Fecha" field is set to "10/10/2012". The "Responsable del control" dropdown menu is set to "Federico Frags". The "Método de control y plazo" section contains a text box with the description: "Se realizaron unas pruebas para medir los niveles de sensibilidad de la cámara. Se probó el zoom on demanda y la calidad de grabación." The "Método de control realizado" checkbox is checked. The "Revisión por el responsable de sistema" section has two checkboxes: "Ha sido revisada:" and "Ha sido eficaz:", both of which are checked. At the bottom of the window, there are three buttons: "Aceptar" (with a green checkmark icon), "Cancelar" (with a red X icon), and "Aplicar" (with a green checkmark icon).

Control de Eficacia

Control de eficacia y cierre de la acción

Fecha: 10/10/2012

Responsable del control: Federico Frags

Método de control y plazo:

Se realizaron unas pruebas para medir los niveles de sensibilidad de la cámara. Se probó el zoom on demanda y la calidad de grabación.

Método de control realizado: ☒

Revisión por el responsable de sistema

Ha sido revisada: ☒ Ha sido eficaz: ☒

Aceptar Cancelar Aplicar

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:

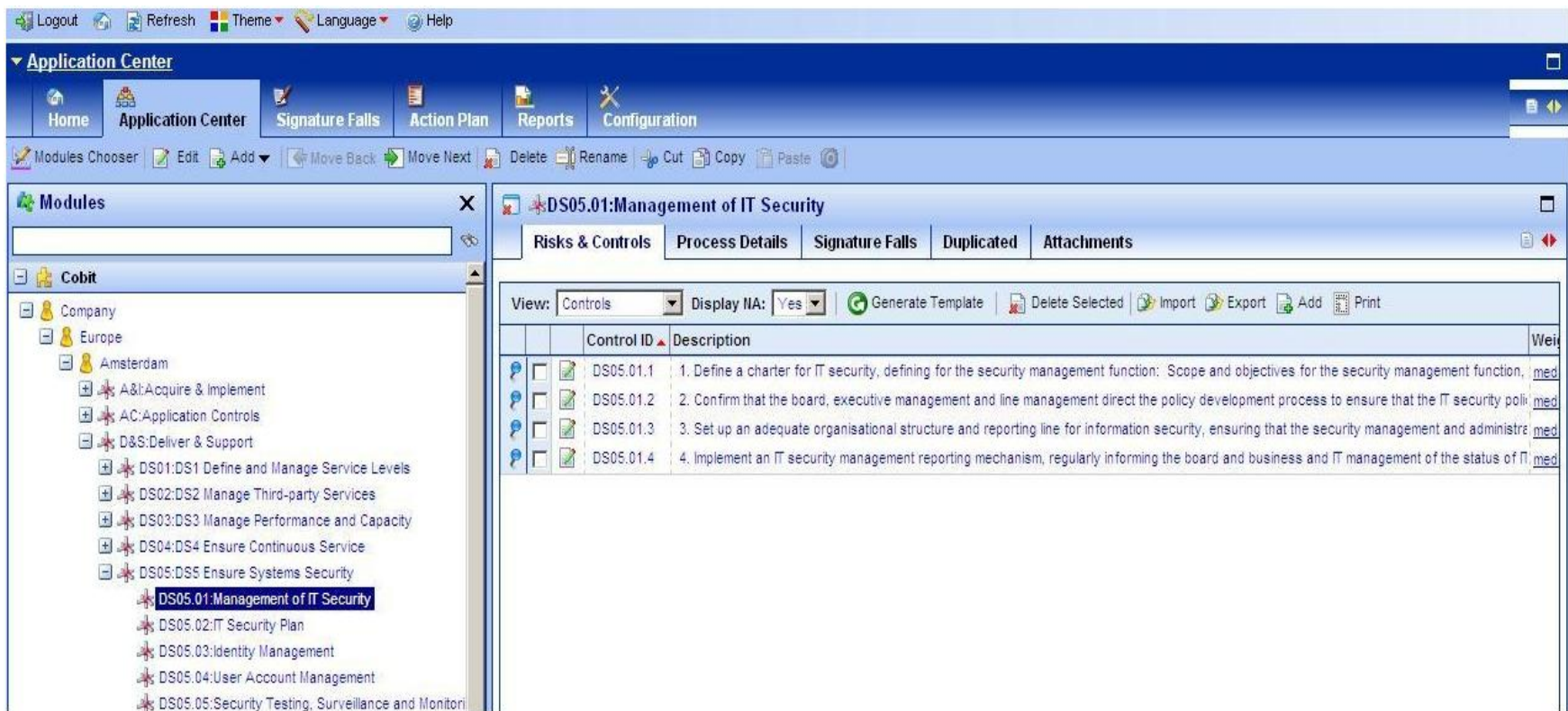
- 🐞 Documentación y Pérdida / Asesoramiento del Riesgo
- 🐞 Eventos de Pérdida / Incidentes de Seguridad
- 🐞 Indicadores claves de Riesgo / Métricas de Riesgo
- 🐞 Firma
- 🐞 Reportes
- 🐞 Dashboard
- 🐞 Plan de acción
- 🐞 Configuración del sistema

Herramientas de Monitoreo y Compliance

- Easy2Comply



Centro de aplicación



Herramientas de Monitoreo y Compliance

- Easy2Comply

Detalles de un control

A.11.4.5: Maintenance ports are secured to avoid abuse. — Webpage Dialog

General Details **Testing** Additional Occurrences Attachments

General Details **Test Plan**

Test Plan

Tester:

Test Start Date:

Test Occasions: Test Frequency:

Sample Size:

Required Documents:

Test Procedure

Check if all ports in the report are matching the organization requirement and not allow communication for non-Business use.

Criteria

Positive Compliance:

Large Extent Compliance:

Small Extent Compliance:

Save Close Print

Herramientas de Monitoreo y Compliance

- Easy2Comply

Plan de acción

A.11.4.R-1 : Penetration of malicious source to sensitive information by exploiting technology weaknesses in access control...

General Details **Qualitative Assessment** Risk Classifications Additional Occurrences Attachm

Inherent

Impact * Likelihood *

Tolerance

Impact * Likelihood *

Risk Square

Impact:	Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood					
Rare					
Unlikely					
Possible					15.00
Likely					
Almost Certain					

Summary

Inherent 15

Residual Risk Level 7.09

Save Close Print

Herramientas de Monitoreo y Compliance

- Easy2Comply

Incidentes de seguridad

Security Incident : Laptop theft -- Webpage Dialog

Documentation Investigation Loss Estimation Conclusions Action Plan Attachments

Description General Details Additional Details Attached Controls

Event Description

The CTO's laptop left in the end of the day at his room, on the table.

The laptop was locked logically but he wasn't locked by a physical security lock.

Also the door was unlocked.

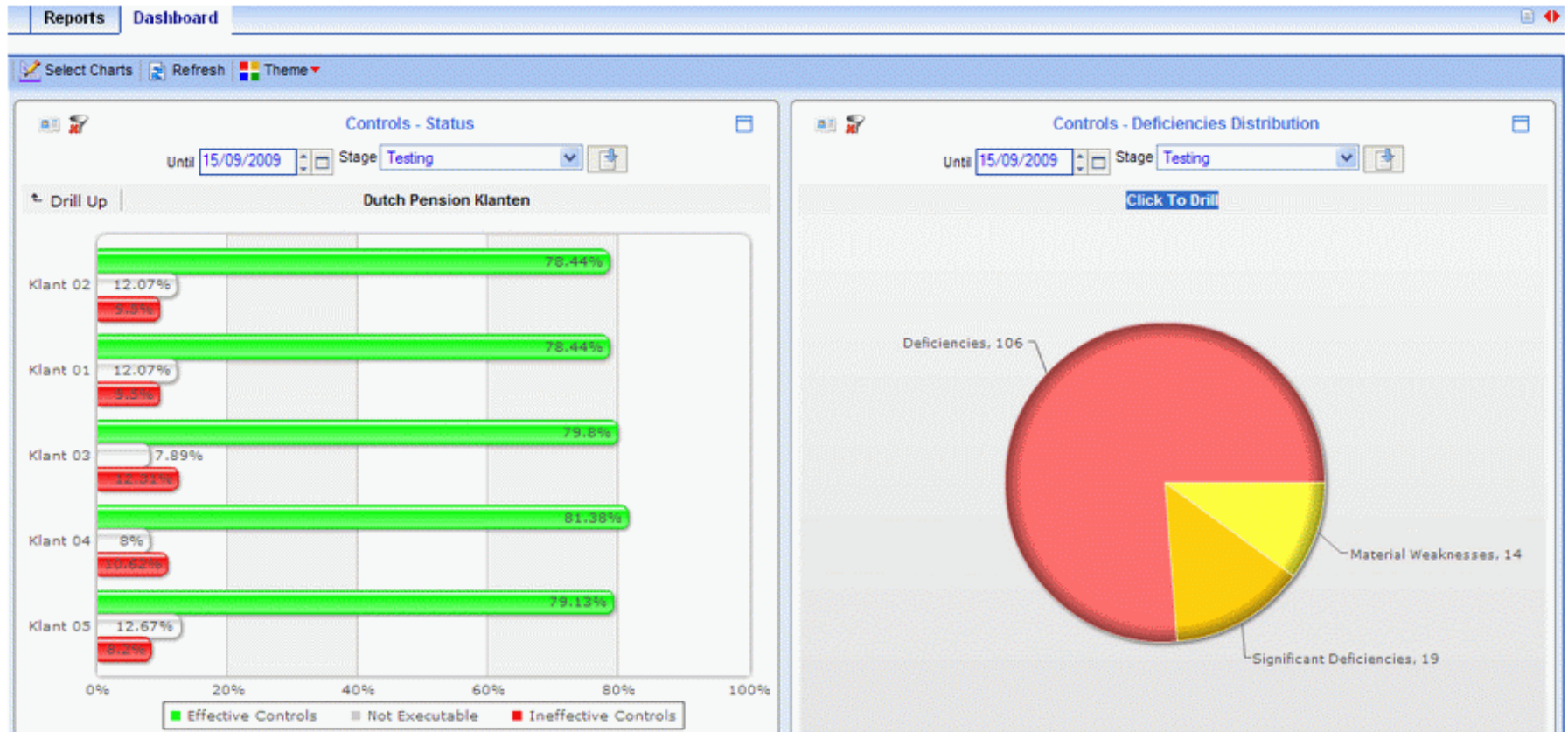
Event Description in Stages

	Number	Description	Date	Time
	1	The CTO finishes his work;	01/09/2009	16:00
	2	The CTO locks his personal laptop, logically only.	01/09/2009	16:00
	3	The CTO leaves the office, with the computer on his desk.	01/09/2009	16:00
	4	The CTO remembered that he forgot to lock the office and calls his se	01/09/2009	16:30
	5	The secretary didn't find the copy of the key for the office, so she left it	01/09/2009	17:00

Save Close Print

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 herramientas 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 dirección	-	-	-	-	-
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 construirlos
- 🐜 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?

