UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

TESINA DE LICENCIATURA

Título: Impacto de la ISO 27000 en organizaciones: Estudio comparativo de herramientas para la implementación de un SGSI.

Autores: Federico Martín Pantaleone – Matías Nicolás Silva
Director: Lic. F. Javier Díaz
Codirector: Lic. Paula Venosa
Asesor profesional: N/A
Carrera: Licenciatura en Sistemas

Resumen

El objetivo del siguiente trabajo es realizar un análisis de herramientas de cumplimiento respecto de la norma ISO/IEC 27001:2005 observando las características que éstas presentan y unificarlas para más adelante plasmarlas en requerimientos de lo que sería un sistema ideal de gestión para la norma en cuestión. Para ello primero se realiza un estudio de la norma previamente mencionada y la norma IRAM-ISO/IEC 27004:2011, la cual sirve de apoyo para implementar el programa de medición del SGSI con el cual podemos medir la eficacia y eficiencia de los controles aplicados. Luego se realiza un estudio comparativo de herramientas de monitoreo y cumplimiento, analizando para cada una de ellas a que requerimientos de la norma ISO/IEC 27001:2005 pueden dar soporte.

Palabras Claves

ISO – SGSI – Monitoreo – Compliance - Seguridad

Conclusiones

- Presentación de aportes que brinda la norma IRAM-ISO/IEC 27004:2001 a la ISO/IEC 27001:2005.
- Cuadro comparativo de herramientas en cuanto al soporte que brindan a los requerimientos de la norma ISO/IEC 27001:2005.
- Especificación de requerimientos para la implementación de un SGSI.

Trabajos Realizados

- Análisis de la norma ISO/IEC 27001:2005.
- Análisis de la norma IRAM-ISO/IEC 27004:2011.
- Análisis de herramientas de monitoreo y compliance
- Estudio de aplicabilidad de las herramientas previamente mencionadas a los requerimientos de la ISO 27001.

Trabajos Futuros

- Implementación de una aplicación o modificación de herramientas existentes para cumplir con los criterios previamente establecidos para un software de gestión de un SGSI.
- Análisis en profundidad de las necesidades de una herramienta que de soporte a la norma IRAM-ISO/IEC 27004:2011.
- Análisis de la ISO/IEC 27006:2007, que establece los requerimientos para los auditores y SGSI, y su relación con las herramientas existentes. Posibilidad de desarrollo de una herramienta para dar soporte a una auditoría de un SGSI.

Fecha de la presentación: **Septiembre de 2012**

UNIVERSIDAD NACIONAL DE LA PLATA
Facultad de Informática

IMPACTO DE LA ISO 27000 EN ORGANIZACIONES:
Estudio comparativo de herramientas para la implementación de un SGSI

Tesis presentada para optar al título de Licenciado en Sistemas

Federico Martín Pantaleone
Matias Nicolas Silva

Director de tesis: Lic. F. Javier Diaz
Co-director: Lic. Paula Venosa

La Plata, 30 de Junio de 2012.

Resumen

Agradecimientos

En primer lugar quisieramos agradecer profundamente a nuestras familias, quienes nos dieron la posibilidad y el apoyo necesario para poder estudiar lo que nos gusta.

También quisieramos agradecer la invalorable ayuda de nuestros compañeros de carrera con quienes compartimos grandes momentos asi como también a nuestros profesores por enseñarnos día a día.

Por último, pero no menos importante, a la Facultad de Informática y a la UNLP.

Índice

Índice de figuras

Índice de cuadros

Capitulo 1

1 Objetivos

El objetivo del siguiente trabajo es realizar una comparación de herramientas de cumplimiento respecto de la norma ISO/IEC 27001:2005, observando las características que éstas presentan, unificándolas, para más adelante plasmarlas en requerimientos de lo que sería un sistema ideal de gestión para la norma en cuestión. Para ello primero se realiza un análisis de la norma y aquellas normas que sirven de apoyo a ésta, en especial la ISO/IEC 27004:2009 y luego se analizan diversas herramientas existentes.

Las herramientas analizadas son independientes de la organización, debido a que el objetivos de estás es principalmente su ingreso económico. Para ello, las organizaciones deben tener especial cuidado de la información que manejan. Para aquellas organizaciones que trabajan con activos informáticos (hoy día casi el 100 %) es donde se aplica la idea de implantar un SGSI (Sistema de Gestión de Seguridad de la Información)

La organización objetivo es una Organización típica la cual consta de recursos humanos y activos informáticos. Se pretende entrenar a los recursos humanos en la utilización para proteger la sensibilidad de los activos mencionados.

1.1. Motivación

Con el avance de la tecnología, en particular los servicios de redes de datos y de comunicación cada vez se hace más presente la necesidad de armar un sistema de seguridad que nos garantice tranquilidad a la hora de la ocurrencia de algún incidente que atente contra nuestros activos, siendo estos, los más importantes que posibilitan brindar los servicios antes mencionados. Cuando nos referimos a un sistema de seguridad intentamos dar a entender un conjunto de mecanismos que hacen posible tanto la seguridad física como lógica. Aunque a veces se tengan todos los medios para hacer frente a incidentes (por cuestiones de vulnerabilidad en los activos) no siempre se puede lograr que la probabilidad de ocurrencia de éstos sea nula, por ello, debemos controlar el Riesgo mediante un SGSI (Sistema de Gestión de Seguridad de la Información).

1.2. Pasos a seguir

1. Realizar una introduccion a los conceptos de Seguridad de la Información, Amenazas, Vulnerabilidades, Riesgos y SGSI.
2. Analizar y Estudiar el alcance de la norma ISO/IEC 27001:2005.

3. Analizar de los aportes que brinda la ISO/IEC 27004:2009.
4. Analizar las características de herramientas de monitoreo y compliance en cuanto a su capacidad de asistir en la implmementación de un SGSI.
5. Analizar que herramienta/s puede/n aplicarse para la implementación de cada requerimiento de la norma ISO/IEC 27001:2005
6. Plasmar los resultados de los análisis de las herramientas de compliance (de acuerdo a criterios establecidos en base a las herramientas analizadas) en una suerte de "Requerimientos" para lo que sería, una herramienta ideal para e la gestión de la ISO/IEC 27001:2005

Capitulo 2

2 Seguridad de la información y SGSI

La intención de este capítulo es describir los conceptos con los cuales nos encontraremos al momento de analizar e implementar la norma ISO/IEC 27001:2005. Luego de la introducción, se explica la importancia que debe proveerse al manejo de la información en entornos informáticos. Posteriormente se detalla como entran en juego las vulnerabilidades, amenazas y riesgos en estos sistemas de información. Por último se explica el concepto de SGSI.

2.1. Introducción

Se entiende por información a todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita. Existen distintos tipos de información (Impresa, escrita en papel, imágenes, almacenada electrónicamente, transmitida por correo o medios electrónicos, etc.).

La información además de ser un medio principal e importante de comunicación, se lo puede denominar como un activo vital para el éxito y la continuidad en el mercado de cualquier organización. Por ello mismo debemos asegurarnos que dicha información junto con los sistemas que la procesan sean bien resguardados, siendo éste uno de los objetivos principales.

Hoy en día, las organizaciones comenzaron a tomar conciencia, en mayor o menor grado, que tienen un problema que puede afectar al negocio más allá de los límites netamente comerciales u organizacionales.

Es por ello que es muy común escuchar hablar de "seguridad informática", pues bajo este concepto se busca la protección considerada necesaria para suplir esta falencia riesgosa para el negocio y desconocida hasta el momento.

Si bien la información puede ser contenida por nuestros sistemas informáticos, no podemos darle protección a éstos sin analizar a qué información le brinda soporte y cuán importante es dicha información para la organización.

Para gestionar la seguridad de la información, se necesita incorporar un sistema o mecanismo que realice un orden de la información de forma metódica y documentada,

evaluando los riesgos a los que está sometida.

Este mecanismo se basa en la norma ISO/IEC 27001:2005 que se desprende de ISO/IEC 27000:2009 que es un conjunto de estándares desarrollados o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission).

2.2. Importancia de la seguridad de la información

En primer lugar diremos que la seguridad de la información, aplicada en términos de una organización, intenta preservar la confidencialidad, integridad y disponibilidad de los datos. Explicamos brevemente que es cada uno de estos conceptos:

La **confidencialidad**, es garantizar que la información sea accesible sólo a aquellas personas que tienen autorización. Ej:: Un recurso muy utilizado en hoy en dia por los hackers es la *ingeniería social*, donde se engaña a la víctima obligándo a la persona a compartir informacion confidencial haciéndose pasar por una entidad confiable.

La **integridad**, es la capacidad de garantizar que la información no ha sido manipulada, y por ende se mantiene libre de modificaciones no controladas. Ej.: La integridad puede verse comprometida por un usuario que realice modificaciones directamente sobre la base de datos (sin utilizar un sistema que posea control de modificaciones); o por ejemplo un error fisico en un dispositivo de almacenamiento que provoque modificaciones en los bits lo que reflejaría resultados erroneos como podria ser en el caso de dinero donde la introducción de un 0 cambiaría la cifra de $1.000.000 a $10.000.000.

La **disponibilidad**, es garantizar que la información y los recursos de información estén disponibles cada vez que se los requiera. Ej.: La disponibilidad se podria ver afectada por un ataque de denegación de servicio (Denial of Service attack - DoS).

Entonces podemos decir que si nuestra tarea principal es la preservación de la Información, antes de establecer cualquier sistema de protección (ya sea físico o lógico), debemos conocer con qué información cuenta nuestra organización, en que medios se encuentra y cuál es su valor en términos a su confidencialidad, disponibilidad o integridad no sólo en cuanto a lo económico, sino que se debe evaluar en qué medida afecta a la continuidad del negocio, a la imagen de la organización, etc.

Para realizar esta evaluación tenemos que introducirnos un poco en el concepto de análisis de riesgos de la cual se desprenden una serie de pasos a seguir, tales como: su análisis, valoración, tratamiento, aceptación, y gestión.

Es muy importante asumir el riesgo e identificar la fuente del mismo mediante el uso sistemático de la información. La clave está en identificar dichos riesgos, analizando la probabilidad de que ellos realmente ocurran y el daño que podrian causar, y por consiguiente tomando los recaudos necesarios parar reducir el nivel total de riesgo al

que la organización identifica como aceptable.

Una vez aplicado el tratamiento obtendremos un riesgo residual, es decir, un nivel restante de riesgo que puede ser aceptable o no por la organización, lo que hace necesario realizar actividades coordinadas de dirección y control de la organización en relación con dicho residuo.

2.3. Vulnerabilidades, amenazas y riesgos

Cuando hablamos de metodología de trabajo, nos referimos a la documentación a seguir para la evaluación. Podemos crear nuestra propia metodología, o bien, basarnos en las que ya existen (IRAM 17750, Guía 73, Magerit, Octave, etc.)

Durante el proceso de identificación de activos recolectaremos una serie de datos que nos permitirá armar un árbol de dependencias con el tipo de información, el propietario del activo, sectores/personas con acceso, formato de almacenamiento y dependencias de los activos de información.

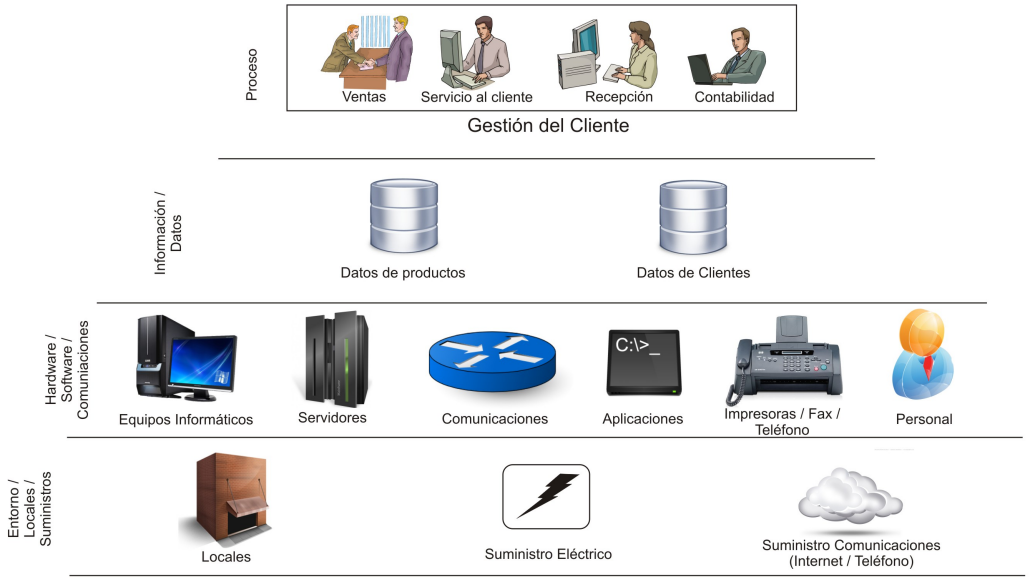

Figura 1: Árbol de Dependencias de Activos

Después de establecer todos los requerimientos para evaluar el riesgo y definir los activos pasamos a realizarle una serie de estudios a cada uno de estos de acuerdo a la metodología empleada. A continuación se detallan lo que se conoce como Valoración de los activos:

En primer lugar, se realiza un **Análisis de impacto**, en la que se estudia la consecuencia que ocasionaría para la organización la concreción de al menos una de las amenazas a la que se encuentra expuesto el activo teniendo en cuenta la disponibilidad, integridad y confidencialidad del mismo. Luego, un **Estudio de las Amenazas**, es decir, todos los posibles eventos que pueden causar un daño sobre el activo mediante la explotación de vulnerabilidades y debido a la posible existencia de ellas se realiza un **Estudio de las Vulnerabilidades** para identificar todas esas debilidades o errores que presentan los activos de información, susceptibles de ser explotados por una amenaza ocasionando un impacto negativo.

Hay varios tipos amenazas que pueden tomar ventaja de varios tipos de vulnerabilidades. La siguiente tabla muestra la relación entre alguno de ellos. Dicha lista no pretende ser completa de ninguna manera, solo muestra un ejemplo de los riesgos que muchas organizaciones podrían tener en cuenta en su programa de gestión de riesgo.

Amenaza	**Puede explotar la Vulnerabilidad**	**Resultado de esta Amenaza**
Virus	Falta de software antivirus	Infección de virus
Hacker	Servicios importantes ejecutándose en el servidor	Acceso no autorizado a información confidencial
Usuarios	Parámetro mal configurado del SO	Mal funcionamiento del sistema
Fuego	Falta de extinguidores de fuego	Daño de las instalaciones, computadoras y riesgo de vida
Empleado	Mecanisimos de control de accesos pobres	Daño a la información critica
Empresario	Mecanisimos de control de accesos pobres SO	Robo de información comercial
Atacante	Aplicaciones pobremente escritas	Conduce a un buffer-overflow
Intruso	Falta de guardia de seguridad	Rotura de ventanas, robo de computadoras y servicios
Empleado	Falta de auditoría	Alteración de los datos de entrada y salida de las aplicaciones de procesamiento
Atacante	Falta de reglas en el firewall	Conduce a un ataque DoS

Cuadro 1: Relación entre Amenazas y Vulnerabilidades

Para evaluar la ocurrencia de las amenazas se realiza un **Cálculo de la proba-**

bilidad de ocurrencia que una amenaza explote las vulnerabilidades de un activo. Este cálculo está directamente relacionado con las vulnerabilidades, las motivaciones, las capacidades y los controles.

Por último se realiza un **Estudio del riesgo** donde se definirá en función de la probabilidad de que una amenaza explote una vulnerabilidad y el impacto de que dicho evento causare a la organización.

Figura 2: Modelo de Interacción del Riesgo

Después de haber concluido con todos los pasos anteriores se debe planificar e implementar todos los controles necesarios sobre los activos en riesgo, a fin de minimizar el mismo y llevarlo a niveles aceptables por la organización. Éstos niveles se encuentran por debajo del definido por la política de la organización en donde el costo de aplicarle mayor controles al activo excede el costo que ocasionara la concreción de la amenaza.

Hay cuatro maneras básicas de tratar el riesgo: *transferirlo*, *rechazarlo*, *reducirlo* o *aceptarlo*.

Hay varios tipos de seguros disponibles a las organizaciones al momento de proteger sus activos. Si una organización decide que el riesgo total o residual son demasiado altos para jugar con ellos pueden comprar un seguro y esto significaría *transferir el riesgo* a la compania de seguros.

Si la organización implementa contramedidas, esto significaría *reducir el riesgo*. Si una organización se niega a conocer sobre los riesgos o simplemente los ignora, esto significaría *rechazar el riesgo*, lo cual puede ser muy peligroso y no recomedable. La ultima apoximación es *aceptar el riesgo*, lo que significaría que la organización comprende el nivel del riesgo al que está haciendo frente y cual es el costo del daño con el que deciden

vivir. Muchas organizaciones aceptarán el riesgo cuando la relación costo-beneficio indique que el costo de la contramedida supera el valor potencial de la pérdida. Por esto la organización no implementará la contramedida y aceptará el riesgo.

Para concluír esta sección, tomemos como ejemplo una organización ficticia que se dedica prestar un servicio de un juego online y que almacena en sus servidores dicho servicio y todos los datos pertinentes a las cuentas de los jugadores, los cuales pagan suscripciones mensuales para acceder al servicio.

Esta organización tiene muchos **activos**, pero nosotros nos enfocaremos en el servidor principal, el cual contiene el servicio que ejecuta el juego. Una **amenaza** para dicho servidor seria que el mismo reciba ataques de denegación de servicio (DoS) con lo cual éste se se saturaría y no podria atender las peticiones de los usuarios legítimos, provocando retrasos en las comunicaciones (lag) o incluso la caída total del servicio. Asociado a esto tenemos **vulnerabilidades**, y un ejemplo muy claro en este caso sería que el servidor no cuente con software Anti-DoS.

La **probabilidad de ocurrencia** claramente no es nula (dependerá del tamaño, seguridad implementada y servicios que organización preste) y debe ser tenida en cuenta por dicha organización. En general las grandes organizaciones protegen sus servidores que estan conectados a internet con diferentes técnicas Anti-DoS.

El **riesgo** que esta organización posee es verse imposibilitada de proveer sus servicios a los jugadores (debido a la concreción de la amenaza), con lo cual deberá (una vez solucionado el problema) recompensar a los jugadores por los dias de baja del servicio.

El **riesgo residual** está relacionado con el riesgo y la amenaza inicial. Es decir, a pesar de implementar medidas de seguridad para prevenir ataques DoS, entre otros, la organización no tiene asegurado en un 100 % de que esto no pueda volver a ocurrir. Entonces el riesgo residual se basa en que nuevamente la organización se vea imposibilitada de proveer sus servicios y tener que recompensar a sus jugadores, pero esta vez el riesgo es mucho menor (es residual).

2.4. Sistema de gestión de seguridad de la información

Cuando hablamos de seguridad de la información dentro de una organización nos referimos, a las medidas tecnológicas de protección y a la supervisión del funcionamiento de las mismas y de sus usuarios.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI.

Éste posee un enfoque basado en procesos donde se comprenden los requisitos de seguridad de la información, se implementan y operan controles para gestionar los riesgos, se realiza un seguimiento y revisión del desempeño y efectividad del SGSI y además se trata que haya una mejora continua a lo largo del tiempo.

Podemos agrupar este tipo de procesos en desarrollo, mantenimiento, revisión y mejora, basándonos en un modelo PDCA donde es un ciclo completo y continuo, es decir, termina y vuelve a empezar. Un SGSI adopta una serie de documentación que se puede estructurar en forma de pirámide de cuatro niveles, donde en el primer nivel se encontraría el manual de seguridad, el más importante, en el que se describen las políticas de seguridad, el alcance, los objetivos, etc. En el segundo nivel tendríamos a los procedimientos de gestión en los que se detallan la planificación, operación y control de los procesos de seguridad, en pocas palabras, se detallan el qué, quién, cuándo y dónde de un proceso. En el tercer nivel tendríamos a los procedimientos operativos que detallan cómo se deben hacer estas tareas. Y en el cuarto y último nivel tendríamos a los registros que son documentos en los que se detallan la salida arrojada por cada uno de los niveles anteriores y el cumplimiento de los mismos.

En la sección donde habla de la norma ISO/IEC 27001:2005, la norma detalla de manera genérica como debe estar formado un SGSI. En un nivel más práctico podremos decir que un SGSI se establece de la siguiente manera.

En primer lugar, la Dirección debe asumir el compromiso del apoyo y decisión ya que durante este proceso va cambiando la cultura y concientización de todos los miembros de la organización, sobre todos, de aquellos que están involucrados directamente con los puntos críticos que deben adaptarse para respetar la norma.

Deben planificarse fechas y responsables para estimar tiempos y caminos críticos entre las tareas a implementar a fin de determinar una estructura formal para el cumplimiento de las mismas en tiempo y forma. Asimismo, como mencionamos anteriormente, se definen el alcance y los límites que va a tener el SGSI (sistema de gestión de seguridad de la información) en función de una serie de características inherentes a la organización, al negocio, a la tecnología, etc.

Es necesario definir una política de seguridad; una especie de "declaración de intenciones" por parte de la Dirección en los que se establezcan criterios de evaluación de riesgos. Se establece además las necesidades de la organización, se determina el nivel de riesgo aceptable y la metodología de evaluación de los riesgos en donde la organización puede optar por alguna aceptada internacionalmente o definir la suya propia.

Se define un inventario de activos de información que los identifique y los clasifique. Cada uno de estos debe incluir, al menos, su descripción, localización y propietario. El propietario debe ser el que defina el nivel de seguridad que requiere su activo, y no necesariamente debe ser el que vaya a gestionarlo. Por ejemplo, una base de datos de una empresa puede ser un activo propiedad del Director de la empresa, mientras que su gestión puede estar a cargo del área de sistemas y sus usuarios pueden ser los comerciales.

También, debe analizarse si estos activos tienen algún valor para la propia organización, identificando amenazas y vulnerabilidades que los afectan. A su vez, se identifican los impactos que provocarían una pérdida de la confidencialidad, la integridad y la

disponibilidad de cada unos de los activos

Una vez identificados estos activos, se debe realizar un análisis de las dependencias existentes entre ellos. Para establecer estas dependencias se pueden hacer preguntas del tipo ¿quién depende de quién? O bien ¿Si ocurre un fallo en un activo X, cuáles otros activos se van a ver perjudicados? El resultado de este análisis arroja un árbol de dependencias de activos como el de la Figura 1.

Teniendo ya armado el árbol de dependencias entre activos se realiza una valoración de los mismos en función de la relevancia que estos tengan para el negocio y el impacto que provocaría que una incidencia sobre el mismo pueda causar a la entidad. Esta valoración se puede hacer de dos tipos: cuantitativa en la que se estima el valor económico del activo o cualitatitiva que se establece en relación a una escala que puede ser con valores numéricos de 0 a 10 o con valores del tipo bajo, medio y alto. Cabe destacar que este tipo de valoración requiere que exista un criterio homogéneo de valoración que permita comparar entre activos y por supuesto basado en los tres pilares básicos (confidencialidad, integridad y disponibilidad). Si tomamos el ejemplo que dimos anteriormente con la base de datos y necesitamos hacer una valoración de ésta, debemos hacernos preguntas del tipo: ¿qué impacto tendría para el negocio que alguien tuviese acceso a la base de datos y pueda modificar ciertos valores críticos?

Es importante mencionar que existen diversos tipos de valoración de activos pero hoy en día el más utilizado por las organizaciones son la entrevista y la encuesta, que consisten en reunir a un grupo selecto del personal de la organización, que posean diferentes roles y que abarquen a todas la áreas que comprenderá el SGSI.

Luego se evalúan los daños resultantes de una posible falla de seguridad y la probabilidad de ocurrencia del mismo. En dicho caso, se estima el nivel de riesgo resultante y se determina si el riesgo es aceptable o requiere tratamiento para ser reducido, eliminado, aceptado o transferido. Según el tratamiento a aplicar se seleccionan controles del Anexo A de la norma ISO/IEC 27001:2005, en la que se deben justificar las exclusiones tenidas en cuenta. Una vez aplicado estos controles queda un riesgo residual que la organización debe asumir y vigilar, ya que (en términos prácticos) por más que aumentemos los controles no se logrará la eliminación del riesgo al 100 %.

Capitulo 3

3 Norma ISO 27001

La intención de este capítulo es introducir brevemente explicando en qué consiste la familia de las ISO 27000, siguiendo por los comienzos históricos de la ISO 2700 y finalmente describiendo el objetivo y requerimientos de la misma.

3.1. La serie 27000

De la misma manera que otros estándares, la 27000 es una familia o serie de estándares. Dentro de esta se encuentran más de 20 estándares. A continuación se describen los más conocidos y utilizados junto con la ISO/IEC 27001:2005:

– ISO/IEC 27000:2009 - *Sistemas de gestión de seguridad de la información - Resumen y vocabulario*

Contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

– ISO/IEC 27001:2005 - *Sistemas de gestión de seguridad de la información - Requerimientos*

Es la norma principal de requerimientos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma mediante la cual el SGSI de una organización es evaluado para lograr su certificación por auditores externos. Dado que ésta fue la sustitución de la BS 7799-2, se establecieron condiciones para realizar la transición de aquellas empresas certificadas en ésta última. En su Anexo A, lista en forma de resumen los objetivos de control y controles que desarrolla la ISO/IEC 17799:2005 (actualmente ISO/IEC 27002:2005), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en esta última, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

– ISO/IEC 27002:2005 - *Código de práctica para la gestión de la seguridad de la información*

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Está hecha en base a la norma BS 7799-1 e ISO/IEC 17799:2005. La norma ISO/IEC 27001:2005 contiene un anexo que resume los controles de ISO/IEC 17799:2005, a diferencia que en la primera los requerimientos son específicos y obligatorios para la organización que

desee certificar.

– ISO/IEC 27003:2010 - *Guía para la implementación de un sistema de gestión de seguridad de la información*

Contiene una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implementación.

– ISO/IEC 27004:2009 - *Manejo de seguridad de la información - Métricas*

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. Dichas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y utilizar) del ciclo PDCA.

– ISO/IEC 27005:2008 - *Gestión del riesgo de la seguridad de la información*

Consiste en una guía para la gestión del riesgo de la seguridad de la información y es un apoyo para la ISO/IEC 27001:2005 y la implementación de un SGSI. La segunda edición fue lanzada en Mayo del 2011.

– ISO/IEC 27006:2007 - *Requerimientos para los auditores y certificación de sistemas de gestión de la seguridad de la información*

Es una guía para los auditores en el proceso de certificar o registrar los SGSI de otras organizaciones. Su alcance es especificar requerimientos generales que una entidad de terceras-partes realizando la certificación/registro de un SGSI tiene que cumplir, si se la reconoce como competente y confiable para la certificación/registro certificación de un SGSI.

3.2. Historia de la ISO 27001

En el año 1901, la única entidad de normalización a nivel mundial era la BSI (British Standards Institution, equivalente a la organización AENOR española). BSI ha publicado importantes normas tales como:

BS 5750 en 1979 (ahora es la ISO 9000)
BS 7750 en 1992 (ahora es la ISO 14001)

La norma BS7799 de BSI aparece por primera vez en 1995, con el objetivo de preparar a cualquier empresa (británica o no) en la certificación de la gestión de la seguridad de su información por medio de una auditoría realizada por un auditor acreditado y externo. El gobierno del Reino Unido recomendó como parte de su Ley de Protección de

la Información que las compañías británicas utilizasen BS7799 como método de cumplimiento de la Ley.

La primera parte de la norma (BS7799-1) es una guía de buenas prácticas, para la que no se establece un modelo de certificación. Es la segunda parte (BS7799-2) la que se audita y certifica en aquellas empresas solicitantes que hayan desarrollado un SGSI (Sistema de Gestión de Seguridad de la Información) según el conocido modelo PDCA (acrónimo inglés de Plan-Do-Check-Act: Planificar-Hacer-Verificar-Actuar), ya presentado en otros estándares como ISO9000, y que asegura la adaptación continua de la seguridad a los requisitos siempre cambiantes de la empresa y su entorno.

Figura 3: Ciclo PDCA

Las dos partes de la norma BS7799 se revisaron en 1999 y la primera parte (BS7799-1) se adopta por ISO, sin cambios sustanciales, como ISO17799 en el año 2000, bien recibida por más de 80.000 empresas. En 2005, y con más de 1700 empresas certificadas en BS7799-2, el esquema SGSI de la norma se publica por ISO bajo la norma ISO/IEC 27001:2005, junto a la primera revisión formal realizada en ese mismo año de ISO17799.

En Marzo de 2006, posteriormente a la publicación de la ISO/IEC 27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información. Ésta es la base de la ISO27005.

3.3. ISO 27001

La norma ISO/IEC 27001:2005 define requerimientos generales y genéricos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI. También presenta un anexo con controles, con los cuales una organización debe cumplir com mínimo.

A continuación describiremos paso a paso los requerimientos indicados en la norma ISO/IEC 27001:2005.

La norma se basa en el ciclo PDCA para planear todas sus actividades. Lo primero que menciona la norma es el SGSI haciendo una breve introduccón del mismo.

La norma está preparada para que el SGSI trabaje conjunta y consistentemente con un sistema ya existente que cumpla con la norma ISO/IEC 9001:2000 y/o ISO/IEC 14001:2004.

La norma especifica los requerimientos para implementar controles de seguridad personalizados para una organización o parte de ella.

Los requerimientos son genéricos, de manera tal de que una organiación de cualquier tipo, tramaño y naturaleza pueda adaptarse facilmente.

Todos los requerimientos de la norma son obligatorios. Sin embargo hay ocasiones donde estos requerimientos no pueden cumplirse, en tal caso una omisión de un requerimiento deberá justificarse y proporcionar evidencia de que los riesgos asociados han sido aceptados por las personas responsables.

La misma se divide en cinco partes principales: SGSI, Responsabilidad de la dirección, Auditorías internas, Revisión general del SGSI y Mejora del SGSI.

3.3.1. SGSI

Requerimientos Generales

Aquí se indican los lineamientos que debe tener un SGSI para establercerlo, implementarlo, operarlo, monitorearlo, mantenerlo y mejorarlo continuamente.

Establecer el SGSI (PLAN)

Definir el alcance, política y límites del SGSI en terminos de las características del negocio, la organización, su ubicación y tecnologías

- Definir el enfoque de evaluación del riesgo, proveyendo una metodología para el cálculo del riesgo
- Identificar los riesgos junto con las amenazas y vulnerabilidades y el impacto que tendría sobre los activos la la explotación de éstas vulnerabilidades

- Analizar y evaluar el riesgo comercial teniendo en cuenta la integridad, confidencialidad y disponibilidad
- Calcular los niveles de riesgo actuales
- Determinar la aceptabilidad del riesgo
- Identificar y evaluar las acciones para el tratamiento de los riesgos para evitarlos, reducirlos, eliminarlos, transferirlos
- Seleccionar objetivos de control para el tratamiento de riesgos, teniendo en cuenta el criterio para aceptar los riesgos

  En el Anexo A hay un conjunto de controles mínimos a ser aplicados. La organización puede incluír sus propios controles
- Obtener la aprobarción de la genrencia para los riesgos residuales propuestos
- Obtener la aprobación de la generencia para implementar y operar el SGSI
- Preparar un Enunciado de Aplicabilidad que indique los objetivos de control y controles objetivos de control y controles a ser implmementados y excusión de los mismos (si aplica)

Implementar el SGSI (DO)

- Formular un plan de tratamiento de riesgos
- Implementar un plan de tratamiento de riesgos
- Implementar los controles indicados en el punto anterior
- Definir como medir la efectividad de los controles o grupo de controles seleccionados Ésto está explicado en mayor detalle en la norma ISO/IEC 27004:2011
- Implementar los programas de capacitación y conocimiento
- Manejar las operaciones del SGSI
- Manejar recursos para el SGSI
- Implementar los procedimientos y otros controles necesarios para dar respuesta a incidentes de seguridad

Monitorear y revisar el SGSI (CHECK)

- Ejecutar procedimientos de monitoreo y revisión, y otros controles para identificar incidentes, amenazas y violaciones de seguridad y determinar si las acciones tomadas son efectivas para resolver incidentes de seguridad.
- Realizar revisiones regulares del SGSI y controles de seguridad, teniendo en cuenta los resultados de auditorías, incidentes, mediciones de seguridad, sugerencias y retroalmientación de las partes interesadas.
- Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad. Ésto está explicado en mayor detalle en la norma ISO/IEC 27004:2011.
- Revisar las evaluaciones del riesgo en un lapso de tiempo determinado y revisar riesgos residuales y niveles de aceptación del mismo.

- Realizar auditorías internas del SGSI a intervalos planeados

Mantener y mejorar el SGSI (ACT)

- Implementar las mejoras idenficadas en el SGSI
- Tomar las acciones correctivas y preventivas y aplicar una acción
- Comunicar los resultados a las partes interesadas con el nivel de detalle apropiado.
- Asegurar que las mejoras loguren los objetivos señalados

Requerimientos de documentación

- Política y objetivos del SGSI
- Alcance del SGSI
- Procedimiento de control y soporte del SGSI
- Descripción de la metodología de evaluación del riesgo
- Reporte de evaluación del riesgo
- Plan de tratamiento del riesgo
- Procedimientos necesarios para asegurar la planeación, operación y control de sus procesos
- Registros requeridos por la norma y enunciado de aplicabilidad

Control de los documentos

- Aprobar la idoneidad de los documentos previa emisión
- Revisar y actualizar los documentos conforme sea necesario
- Asegurar que el detalle de la revisión y estado actual de los documentos esté disponible
- Asegurar que las versiones mas reciestes estén disponibles
- Asegurarse que los documentos se mantengan legibles y facilmente identificables
- Asegurar el ciclo de un documento: vigente, obsoleto y eliminado
- Asegurar que se identifiquen los documentos de origen externo
- Asegurar que se controle la distribución de documentos
- Evitar el uso indebido de documentos externos
- Aplicar una identificación apropiada si se van a retener por algún propósito

Control de registros

Los registros deben ser protegidos y controlados de la misma manera en la que se mantienen los documentos generales del SGSI. Se deben documentar e implementar los controles necesarios para la identificación, almacenaje, protección, recuperación, tiempos de retención y disposición de los registros. Se deben mantener registros del desempeño del proceso e incidencias de seguridad.

3.3.2. Responsabilidad de la dirección

Compromiso de la dirección

Se debe presentar evidencia del compromiso de la gerencia con establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI.

- Establecer una política SGSI
- Asegurar que se establescan objetivos y planes
- Establecer roles y responsabilidades para la seguridad de la información
- Comunicar a la organización la importancia de lograr los objetivos de seguridad
- Proporcionar los recursos suficientes para operar el SGSI
- Decidir el criterio para la aceptación del riesgo y niveles de riesgo aceptables
- Asegurar que se realicen las auditorías internas y revisiones gerenciales

Gestión de los recursos

Provision de los recursos

La organización debe determinar y proporcionar los recursos necesarios para:

- Operar el SGSI
- Asegurar que los procedimientos de seguridad respalden los requerimientos comerciales
- Gestionar requerimientos legales y obligaciones de seguridad
- Llevar a cabo revisiones cuando sean necesarias
- Mejorar la efectividad del SGSI

Capacitación, Conocimiento y Seguridad

Asegurar que todo el personal a quien se le asignó responsabilidades sea competente para realizar las tareas requeridas

- Determinar las capadidades de acuerdo a los roles dentro del SGSI
- Proporcionar las capacitaciones pertinentes o emplear personal competente
- Evaluar la efectividad de las acciones tomadas
- Mantener registros de capacitación, capacidades, experiencias y calificaciones

3.3.3. Auditorías Internas

Se deben realizar auditorías internas a intervalos de tiempo planeados para analizar si los objetivos de control, controles, procesos y procedimientos:

- Cumplen con los requerimientos de la norma
- Cumplen con los requerimientos de seguridad de la información
- Se implementan de manera efectiva y se realiza conforme a lo esperado

3.3.4. Revisión gerencial del SGSI

Se debe realizar una revisión por la dirección al menos una vez al año.

Insumos de la revisión

La revisión por la dirección debería utilizar los siguientes datos:

- Resultados de auditorías y revisiones del SGSI
- Retroalimentación de las partes interesadas
- Técnicas, productos o procedimientos para mejorar el desempeño y efectividad
- Estado de acciones correctivas y preventivas
- Vulnerabilidades y/o Amenazas no tratadas en evaluaciones de riesgo previas
- Resultados de mediciones de efectividad
- Acciones de seguimiento de revisiones previas
- Recomendaciones para la mejora

Resultado de la revisión

Se debe incluír cualquier resultado, decisión y acción relacionada con lo siguiente:

- Mejora de la efectividad del SGSI
- Actualización de la evaluación del riesgo y el plan de tratamiento de riesgo
- Modificación de procedimientos y controles que afectan la seguridad de la información
- Necesidades de recursos
- Mejora de como se mide la efectividad de los controles

3.3.5. Mejora del SGSI

Acción correctiva

Se deben eliminar las causas de las no conformidades para evitar la recurrencia. Se deben definir los requerimientos para:

- Identificar las no conformidades
- Determinar las cusas de las mismas

- Evaluar la necesidad de acciones para evitar la recurrencia
- Determinar la acción correctiva necesaria
- Registrar los resultados de la acción tomada
- Revisar la acción correctiva tomada

Acción preventiva

Se debe determinar la acción para eliminar la causa de las no conformidades potenciales para evitar su ocurrencia. Se deben definir los requerimientos para:

- Identificar las no conformidades potenciales y su causa
- Evaluar la necesidad de acciones para evitar la recurrencia
- Determinar e implementar la acción preventiva necesaria
- Registrar los resultados de la acción tomada
- Revisar la acción preventiva tomada

El Anexo A indica los controles mínimos requeridos por la norma.

Capitulo 4

4 Norma ISO 27004

El objetivo de este capítulo es describir como está compuesta la norma IRAM-ISO/IEC 27004 para dejar en evidencia los aportes que realiza a la ISO/IEC 27001:2005.

4.1. Introducción

La norma ISO/IEC 27001:2005 impone ciertos controles a cumplir para poder certificar. Al leer la norma IRAM-ISO/IEC 27004:2011 veremos que siempre dice "se recomienda que..." debido a que se trata de un documento de apoyo y, a pesar de que las actividades de las cuales habla deben ser llevadas a cabo, la manera de hacerlo dependerá de la organización, su tamaño y de sus necesidades particulares.

Ésta norma versa sobre el programa de medición y para esto se maneja en torno a recomendaciones para que la organización, en especial, la alta dirección y los responsables de las mediciones puedan efectuar dicho programa de manera eficaz. El programa de medición se realiza para poder determinar el nivel de cumplimiento y efectividad de los controles requeridos por la ISO/IEC 27001:2005 con los cuales se trabaja durante el ciclo PDCA.

4.2. Programa y modelo de medición

El programa de medición consiste en varias etapas. La norma IRAM-ISO/IEC 27004:2011 sirve de guía para la implementación de este programa y provee una definición para cada uno de los pasos.

Como se mencionó anteriormente, este programa sirve para medir la eficacia de los controles implementados. Para esto la norma identifica a todo lo que puede ser medido como "Objetos". Los objetos de medición pueden incluir procesos, procedimientos, proyectos, aplicaciones y sistemas de información y recursos planificados o implementados.

Para realizar el programa de medición, la norma define un modelo de medición como se puede ver a continuación:

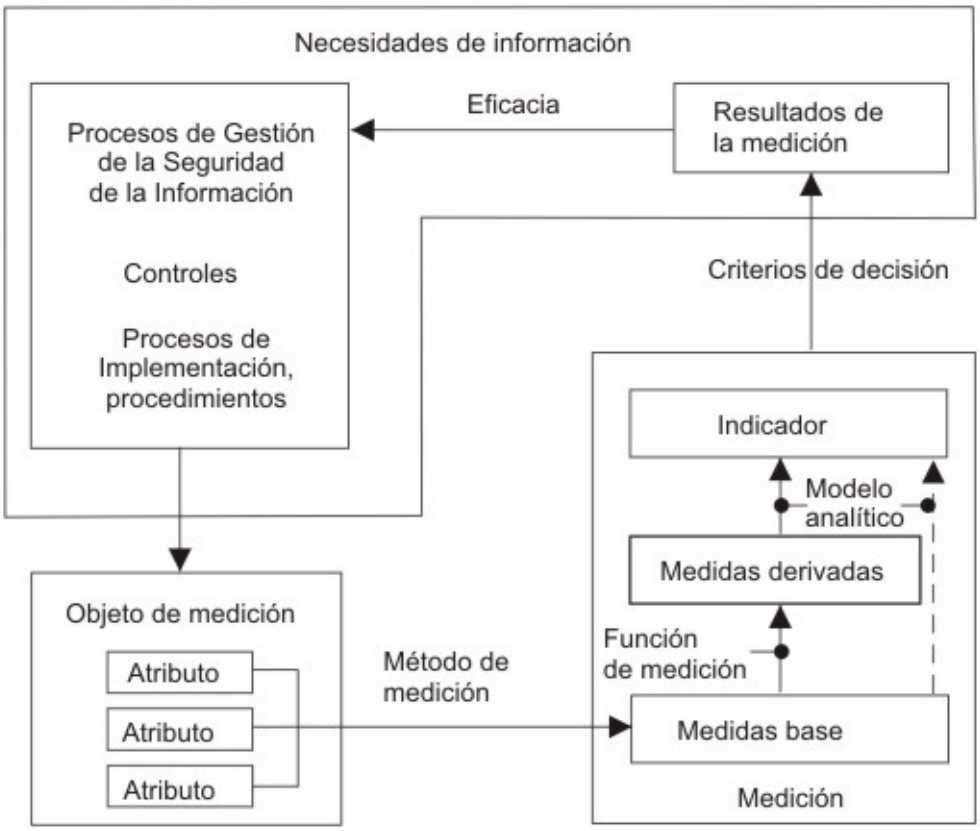

Figura 4: Modelo de medición

El modelo de medición de seguridad de la información es una estructura que vincula una necesidad de información con los objetos de medición relevantes y sus atributos. A continuación se detallarán los elementos individuales del modelo.

Un **Objeto de Medición** puede tener varios atributos, pero puede que solo alguno de ellos tenga valores útiles para ser asignados a una medida base. Un atributo puede ser asignado a varias mediciones diferentes.

Un **Método de Medición** es un conjunto de operaciones para medir los atributos de un objeto de forma cuantitativa. La operación puede consistir en contar ocurrencias u observar el paso del tiempo.

Una **Medida Base** es la primer medida que se obtiene de la medición de los atributos de un objeto de medición.

Una **Medida Derivada** es una combinación de dos o más Medidas Base.

Por ejemplo: Si medimos personal que debe firmar un convenio, tendremos dos medidas base una con a) el total del personal que debe firmarlo y otra con, b) el personal que ya lo firmó. Una medida

derivada podría ser b) dividido a) con los cual nos daría el grado de avance en la firma del convenio.

Una **Función de Medición** es un cálculo utilizado para combinar Medidas Base de manera de crear una Medida Derivada. Ésta puede promediar, asignar ponderación o asignar valores cualitativos a las Medidas Base.

Un **Indicador** es una medida que provee una estimación o valoración de atributos. Éste se obtiene aplicando un modelo analítico a las Medidas Base y/o Derivadas y combinándolos con los criterios de decisión.

Los **Criterios de Decisión** se utilizan para determinar la necesidad de una acción así como también para determinar el nivel de confiabilidad de los resultados medidos.

El **Resultado de la Medición** se basa interpretando los indicadores aplicados.

La norma recomienda que, para los primeros programas de medición se comience con los objetivos más críticos de la organización. Éstos pueden ampliarse a medida que el SGSI vaya evolucionando y de acuerdo a las partes interesadas. Asimismo recomienda hacer un filtro con los resultados más sobresalientes. El hecho de informar un gran número de resultados puede afectar la habilidad de quienes toman las decisiones.

Otra de las cosas a tener en cuenta es que debemos intentar medir todos los atributos de un objeto, aunque algunos de ellos puedan resultar más costosos que otros. Sin embargo, hay atributos que no se pueden medir, por ende, estos atributos no son útiles.

4.3. La estructura de medición

La estructura de medición son los pasos a seguir para poder implementar el programa de medición de acuerdo al modelo explicado previamente en la sección 4.2. En ésta estructura intervienen varios participantes: cliente y revisor de la medición, propietario, recolector y comunicador de la información.

A continuación se detallarán cada uno de los pasos involucrados en la Estructura de Medición:

Selección de la medida
Como primer paso debemos seleccionar una medida, que será objeto de análisis. Para la selección de dicha medida debemos tener en cuenta los siguientes factores:

- Facilidad para la recolección de datos
- Disponibilidad de los recursos humanos
- Disponibilidad de las herramientas

- Número de indicadores correspondientes
- Facilidad de interpretación
- Número de usuarios de los resultados
- Costo de la recolección, gestión y análisis de los datos

Método de Medición

Se debe establecer un método de medición para cada medida base. Esto se logra a través de la transformación de los atributos de dicho objeto para poder cuantificarlos.

El método de medición puede ser subjetivo u objetivo. Los métodos subjetivos se basan en la cuantificación en la cual está involucrado el juicio humano. Los métodos objetivos utilizan cuantificación basada en reglas numéricas que puede implementarse por medios humanos o automáticos.

El valor obtenido de la medición debe poseer un cierto nivel de confianza, ya que este va a ser asignado a una medida base.

Es importante que el método de medición sea consistente a través del tiempo para que dos medidas tomadas en diferentes momentos puedan ser comparables

Función de medición

Ésta función se aplica a dos o más Medidas Base, con lo cual obtenemos la Medida Derivada. Transforma los valores de una o más Medidas Base para aplicarlos en una Medida Derivada.

Una función de medición puede ser un cálculo tal como un promedio de Medidas Base, ponderaciones de valores asignados a las Medidas Base, asignación de valores cualitativos, etc.

Modelo analítico

El modelo analítico se debería aplicar a una Medida Base y/o Derivada para transformar sus valores y asignarlos a un Indicador.

El objetivo del modelo analítico es seleccionar las medidas más relevantes para poder producir una salida significativa para partes interesadas.

Es recomendable que se tengan en cuenta los Criterios de Decisión que serán aplicados a los Indicadores.

Indicadores

Para obtener los Indicadores debemos aplicar los Criterios de Decisión a los valores correspondientes a las Medidas Derivadas.

Para cada uno de los Indicadores a ser presentados al cliente se debería establecer un formato de presentación, donde se visualizarán las medidas y se detallarán los Indicadores. Dicho formato consta de la información a incluir en el mismo, especificando los métodos y herramientas utilizados e indicando como y donde se almacenan los datos, etc.

Criterios de Decisión

Los Criterios de Decisión definirán rangos aceptables para la organización para cada una de las mediciones, a través del análisis de éstos criterios podemos ver el cumplimiento o no de los objetos medidos.

La idea de los mismos es poder medir el cumplimiento y rendimiento de los controles a través del establecimiento de metas dadas por la alta dirección. No obstante, la alta dirección puede no definir las metas hasta tanto no se recolecten los datos iniciales.

Luego de eso se debe definir los Criterios de Decisión e hitos de implementación que sean realistas para la organización. Estos hitos serán luego controlados en la Revisión por la Dirección (punto obligatorio indicado en el cap. 7 de la ISO/IEC 27001:2005).

Es importante definir y documentar los Criterios de Decisión correspondientes a cada Indicador basados en los objetivos de la seguridad de la información para proveer una guía de acción a las partes interesadas.

El análisis de medidas históricas seleccionadas permitirá establecer Criterios de Decisión más realistas ya que darán una idea del rendimiento que ha existido previamente.

Por último se recomienda que la especificación de la estructura de medición incluya como mínimo lo siguiente:

- El propósito de la medición y el objetivo de control
- El objeto de medición
- Los datos a recolectar y utilizar
- Los procesos para la recolección y análisis de los datos
- Los procesos para informar los resultados de las mediciones
- Los roles y las responsabilidades de las partes interesadas
- Un ciclo para revisar las mediciones

Todo esto se encuentra en mayor detalle en el Anexo A donde se pueden ver cada uno de los puntos a incluir y la explicación de los mismos.

En el Anexo B tenemos ejemplos de estructuras de medición aplicadas para medir los procesos y de controles de un SGSI que requiere la ISO/IEC 27001:2005.

4.4. Aportes de la norma

La norma ISO/IEC 27001:2005, en la sección 4.2.2 d) requiere que se defina como medir los controles para poder analizar su efectividad y eficiencia para determinar en qué grado dichos controles cumplen su objetivo. Para esto, la norma IRAM-ISO/IEC 27004:2011 propone lo que denomina como el “programa de medición” y proveyendo una guía con sugerencias para su correcta implementación.

Para ello primero presenta los grupos de personas que harán uso de la información desde los analistas, pasando por los recolectores hasta los usuarios finales de los resulta-

dos. Luego, define un modelo genérico de medición para poder implementar el programa de medición en el cual vemos al programa dividido en áreas o pasos.

Más adelante se hará hincapié en cada uno de los pasos dando recomendaciones para su implementación.

En el Anexo A provee un template con los datos necesarios a registrar durante todas las etapas del programa de medición y en el Anexo B ejemplos de dicho programa aplicado a procesos y controles requeridos en la ISO/IEC 27001:2005.

En la norma siempre hace hincapié que el programa de medición puede ser adaptado a las necesidades de cada organización ya sea grande o pequeña y de su actividad principal siendo que el objeto de la norma apunta a un SGSI de cualquier tipo de organización.

La norma da muchas recomendaciones para facilitar la implementación del programa de medición, entre ellas:

- Como recolectar y analizar la medición
- Como comunicar los resultados a las partes interesadas
- Como analizar los resultados y transformarlos en acciones
- Como adaptar los resultados de acuerdo al receptor de la información
- Como realizar las revisiones periódicas por parte de la alta dirección
- Como realizar el seguimiento, control, revisión en cuanto a los resultados
- Como planificar la implementación de mejoras
- etc.

Capitulo 5

5 Herramientas de Monitoreo y Compliance

En este capítulo se realizará una reseña de las herramientas existentes en el mercado para certificar y/o complementar en la certificación ISO/IEC 27001:2005.

Estas herramientas pueden ser gratuitas y otras comerciales, y en algunos casos son de código abierto. En ciertos casos una misma herramienta puede proveer una versión gratuita y otra comercial, siendo que la versión comercial incluye mas funcionalidades.

Como se explicó anteriormente, uno de los focos principales de la ISO/IEC 27001:2005 es la seguridad de activos informáticos. Éstos son particularmente vulnerables en redes informáticas. Por ende hablamos de herramientas de monitoreo, las cuales analizan el trafico de red para que, junto con herramientas de compliance, podamos cubrir aquellos puntos requeridos por la norma. Lo ideal es tener una herramienta de compliance junto con una de monitoreo para lograr una mayor efectividad.

A pesar de esto, la variedad de herramientas de este tipo no es muy grande actualmente, en comparación otras herramientas informáticas existentes.

5.1. OSSIM

OSSIM es una herramienta de Monitoreo y Compliance gratuita y de codigo abierto. También ofrece una versión comercial con algunas funcionalidades extras.

Con respecto al monitoreo, éste está compuesto por herramientas (plugins) que ejercen un control de disponibilidad de los servicios ofrecidos por cada host de la red, ya sean Switches, Routers, Servidores o simplemente una PC; por aquellas que chequean el tráfico de entrada y salida de determinados hosts discriminando a su vez el mismo por protocolo y puerto. También analiza el tráfico entre los hosts de la LAN y entre ellos y la WAN.

Con respecto al Compliance, OSSIM tiene soporte para ISO/IEC 27001:2005 como para PCI-DSS. Gracias a las herramientas provistas permite analizar y registrar el nivel de cumplimiento (Compliance Level) actual del SGSI de la organización. Tiene opciones para manejar el nivel de riesgo de la red así como también administración de políticas, directivas que resultan en acciones. Además posee reportes con gráficos que indican las áreas fuertes y vulnerables de la red o del sistema.

¿Cómo funciona OSSIM?

Naturalmente en una red los host se comunican unos a otros para enviar y recibir información. A estas comunicaciones, que implican envío de paquetes, las veremos cómo eventos. Estos eventos pueden verse como el resultado de comunicaciones de un host a otro por la naturalidad de la red o bien como intento de accesos de un host a múltiples host en un período corto de tiempo.

Hay varios factores que analizar al momento de decidir si el establecimiento de una comunicación de un host con otro/s es algo rutinario o un potencial ataque.

OSSIM maneja diferentes conceptos para tratar los eventos que ocurren en la red, analizarlos, priorizarlos y, de acuerdo al riesgo que generan y a las políticas generadas por el administrador, llevar a cabo acciones para evitar inconvenientes con los activos. Lo que sigue a continuación se ve a modo de resumen en el panel superior del sistema en todo momento.

Figura 5: OSSIM - Panel de riesgo

Prioridad La prioridad está relacionada con las amenazas y refleja la importancia de un ataque en particular y no tiene nada que ver con un host o entorno específico. Sólo mide la importancia relativa del ataque en sí.
Rango: 0 - 5
Valor por defecto: 1
Nota: Más alto significa más prioridad.

Ejemplo: Un servidor Unix ejecutando un Samba es atacado por el gusano Sasser. Aparte del hecho de que el ataque no tendrá un impacto en el entorno dado (ya que afecta solo a un proceso de Windows), tiene el potencial de explotar un hueco de seguridad y por dicha razón es considerado alto.

Factibilidad En general, en el entorno de un sistema de gestión de seguridad, utilizaríamos el término "probabilidad". Dado que es difícil determinar cuan probable es que se exponga una red a cierta vulnerabilidades, se consideró que la palabra más apropiada para el IDS en cuestión es "factibilidad".

Rango: 0 - 10

Valor por defecto: 1

Nota: Más alto significa más factible.

Ejemplo: Si un host se conecta a 5 hosts diferentes en la misma subred usando el puerto 445, puede ser un comportamiento normal (poco confiable desde el punto de vista de un IDS). Si se conecta a 15 hosts sería sospechoso. Con 500 conexiones a hosts diferentes en menos de una hora el ataque se volvería mas y mas factible.

Valor del activo Se asigna tanto a los hosts Fuente como Destino y representa la importancia del host para la empresa

Rango: 0 - 5

Valor por defecto: 1 (también se utiliza para los host que no están definidos en la BD de activos)

Nota: Más alto significa más importancia.

Ejemplo: Un servidor de BD puede tener un valor de activo de 5, un servidor de pruebas de desarrollo un valor de 2 y un host desconocido en Internet que causa un evento portscan tendrá un valor de 1.

Alarma Basado en la Prioridad del Evento (0-5), Factibilidad del Evento (0-10) y el Valor del Activo (0-5), se calcula el Valor del Riesgo (0-10) y al haber valores mayores o iguales a 1 se generan Alertas.

Riesgo El Riesgo es calculado en base a la siguiente fórmula:

Riesgo = (Prioridad * Factibilidad * Activo) / 25

Políticas y Acciones Las Políticas son definidas para ver qué acción se tomará con los eventos.

Figura 6: OSSIM - Listado de políticas

Se definen políticas para definir que se hará con los eventos que llegan al Servidor OSSIM:

- Correlación (ej.: verificar contra las directivas)
- Reenvío (ej.: una copia es enviada al almacenamiento forense)
- Acciones (ej.: enviar un email, ejecutar scripts o tickets)
- Descartar (ej.: el último filtro posible antes de guardar el evento en la BD, aunque es recomendado filtrar los eventos lo más cercano a la fuente como sea posible.

Al crear una nueva política tenemos las siguientes opciones que el sistema utilizará de filtro al ocurrir algún evento:

- Activos Fuente y Destino (Hosts, Redes, ANY...)
- Puertos
- Grupo de Plugins
- Sensores (se pueden instalar más de uno en la red)
- Rango de Tiempo
- Consecuencias de la políticas (acciones a ejecutarse)

Por otra parte tenemos las **Directivas de Correlación**, el **Compliance Mapping** y las **Alarmas**.

Dentro del **Compliance Mapping** están los objetivos de control de la norma ISO/IEC 27001:2005. Para cada uno de ellos tenemos diversas opciones como "Aplica", donde podemos indicar si dentro de nuestra organización dicho control aplica o no (y si no aplica, aclarando el por qué en el campo "Justificación"). También podemos marcar si dicho control está implementado (ya sea por una Política, una Directiva de Correlación, u otra medida que exceda a OSSIM pero que pueda ser justificada por escrito). Por último está el botón "Plugins" donde asociamos el plugin que se relaciona con el objetivo de control. Es decir, si estamos trabajando sobre un objetivo de control de accesos, buscaremos cuales plugins de control de acceso se corresponden.

Figura 7: OSSIM - Compliance checklist

Con respecto a las **Directivas de Correlación**, se encuentra integrado por políticas de acceso que se pueden definir a partir de una serie de plugins que controlan

determinados servicios. Estos accesos controlados (directivas) por alguna política definida pueden desencadenar una acción, ya sea el envío de un mail de alerta de acceso no autorizado o bien la aplicación de otra política, como por ejemplo, insertar una regla en el firewall al estilo de un IPS (Intrusion Prevention System).

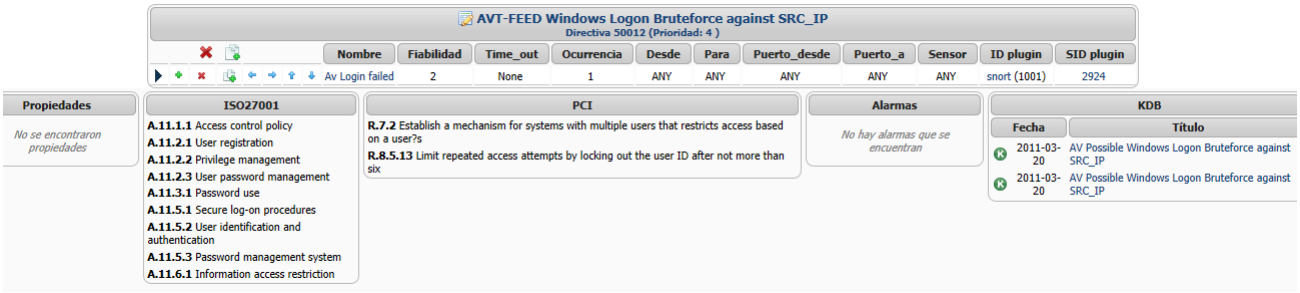

Figura 8: OSSIM - Directivas de correlación

Además las Directivas de Correlación sirven para crear nuevos eventos a partir de algunos eventos.

Analicemos el siguiente ejemplo: Si alguien se equivocó su contraseña 10 veces probablemente sea un ataque o un usuario que olvidó su contraseña. Ahora, si ocurrieron 1000 intentos en 2 minutos con seguridad es un ataque de fuerza bruta.

También podrías encuestar a un Router para ver el nivel de carga de su procesador, ya que el mismo suele incrementarse notablemente durante Ataques de Denegación de Servicio (DOS).

Y en realidad el control de accesos físicos SI se puede implementar con OSSIM siempre y cuando el dispositivo lector de tarjetas (ubicado en las puertas) venga con una forma de conectarse a la red y guardar Logs. Dicha información (Logs) podríamos enviarlos a OSSIM y de ahí realizar correlaciones.

Las **Alarmas** se generan a partir de los tickets abiertos o a partir de las Directivas de Correlación. Cuando se detecta que se cumple una de las reglas definidas en Directivas de Correlación se genera una alarma de acuerdo al evento específico.

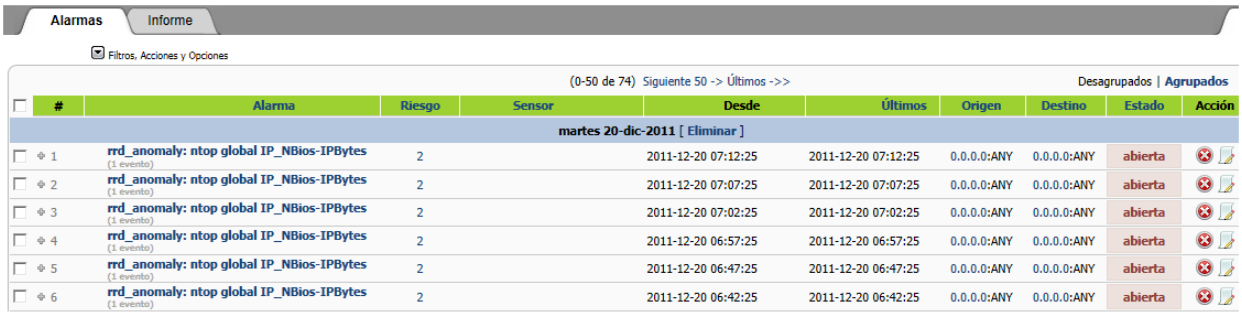

Figura 9: OSSIM - Alarmas

Cuando en el SIEM se detecte por ejemplo, un evento, con id de plugin X hará lo siguiente: buscará en las políticas en orden ascendente (con respecto al número) para ver si dicho plugin coincide con alguna de ellas y ejecutará la acción asociada.

Adicionalmente buscará en las Directivas de Correlación para ver el plugin X se corresponde con el/los plugin/s asociados a las mismas.

Conclusiones de la herramienta

Esta herramienta provee un análisis muy profundo de todos los eventos que ocurren en la red, gracias a la inmensa cantidad de plugins que contiene para poder realizar las detecciones.

Es muy importante destacar el soporte que la herramienta provee para manejar la norma y controlar el estado del SGSI. Con Ossim podremos marcar que puntos de la norma están cubiertos, la relación con la política y a lo sumo alguna justificación. Con las otras herramientas puramente de compliance (que veremos más adelante) podremos realizar un análisis más profundo con respecto a los requermientos de la norma, centrándonos en el riesgo, planes de acción, revisiones, etc.

A pesar de esto Ossim podría utilizarse sin el acompañamiento de ninguna otra herramienta y así poder mantener el SGSI cumpliendo con la ISO/IEC 27001:2005.

La única contra o desventaja puede ser que su uso es un poco más complicado que las demás herramientas, pero esto es debido a la gran cantidad de opciones que provee.

5.2. OpenNMS

OpenNMS es una herramienta de monitoreo totalmente gratuita y de código abierto.

OpenNMS es completamente libre. Ésta es una herramienta únicamente de descubrimiento y monitoreo de los hosts que se encuentran en la red. Es muy similar a Nagios ya que integra un dashboard web donde se puede acceder a todos los eventos que ocurrieron recientemente. A diferencia de otras herramientas de descubrimiento de hosts, en esta se pueden definir subrangos de la red permitiéndonos obtener información de todos los hosts sin importar en que segmento de la red o VLAN se encuentren.

Esta herramienta está más orientada a nivel de servicios que se encuentran en la red, tales como, páginas webs, accesos a bases de datos, DNS, DHCP, etc. Los servicios de un determinado hosts son agrupados en un conjunto denominado “Nodo” como puede

apreciarse en la siguiente imagen.

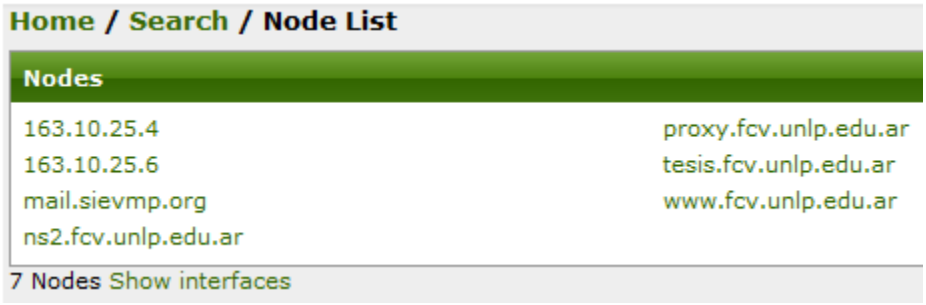

Figura 10: OpenNMS - Listado de activos

¿Cómo funciona OpenNMS?

OpenNMS es otra herramienta de monitoreo de activos tales como HypericHQ, que se verá más adelante; sin embargo ésta cuenta con algunas particularidades como por ejemplo la posibilidad de realizar una importación de los activos al inventario desde una fuente externa y la posibilidad de definir un mapa de la topología de la red.

Durante la instalación nos pide que definamos cual es el subrango de red que vamos a utilizar para descubrir los hosts, de esa manera, cuando ingresamos al dashboard web nos autenticamos y nos encontramos con todos los hosts encontrados dentro del rango definido. Como mencionamos anteriormente se pueden definir más de un subrango de red, URLs e IPs específicas dentro de la configuración (Admin >Configure Discovery).

El sistema tiene una barra superior la cual contiene los siguientes menues:

- Node List
- Search
- Outages
- Path Outages
- Dashboard
- Events
- Alarms
- Notifications
- Assets
- Reports
- Charts
- Surveliance
- Distributed Map (no implementado)
- Map
- Add Node

- Admin
- Support

En primer lugar tenemos a la lista de nodos (menú “Node List”) que descubrió en la LAN. Cada uno de ellos tiene un detalle en el que se visualizan la cantidad de servicios encontrados, la disponibilidad de los mismos, las notificaciones asociadas a dicho nodo, los eventos y cortes de servicios recientes.

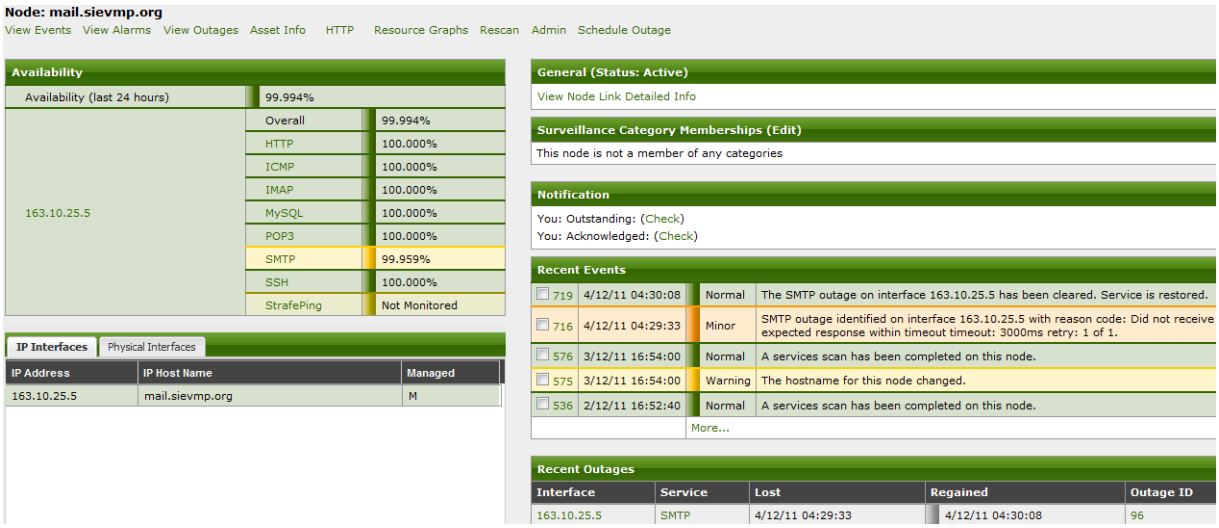

Figura 11: OpenNMS - Detalle del activo

A su vez dentro de este menú, podemos ver el histórico de los eventos, alarmas, cortes de servicios, información más detallada del activo, gráficos de recursos, administrar el activo y cortes de servicios programados.

Dentro de estos submenúes podemos elegir ver gráficos asociados al nodo. Podemos elegir diversos gráficos de tiempo de respuesta de protocolos ICMP, HTTP, POP3, SMTP y SSH y filtrarlo por tiempo como se ve en la imagen debajo.

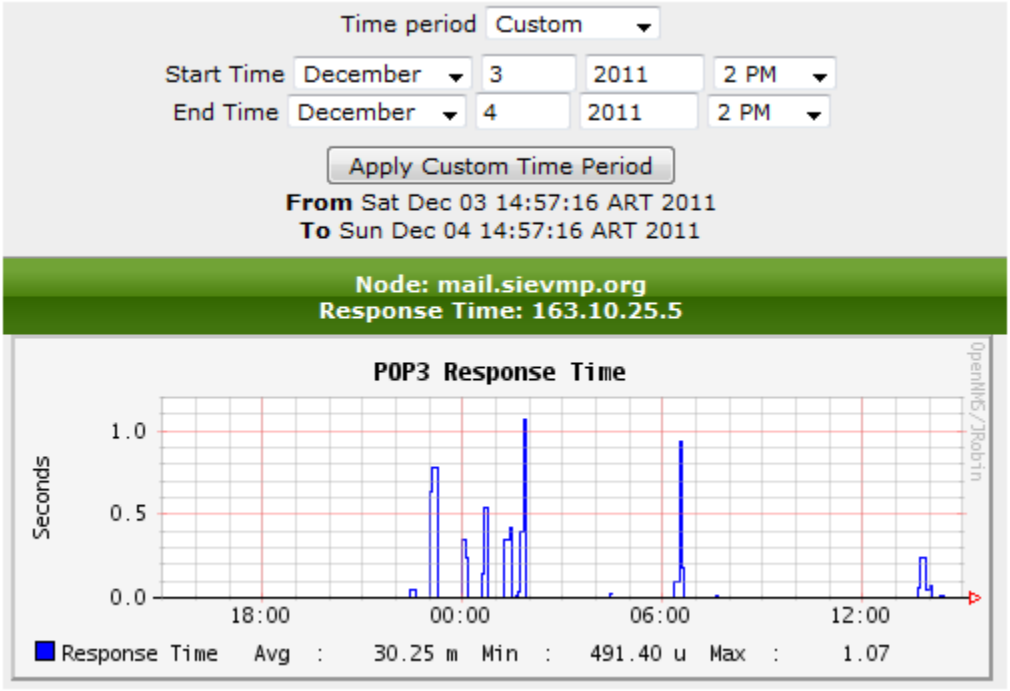

Figura 12: OpenNMS - Gráfico MRTG del tráfico POP3

Para que los servicios se mantengan operando apropiadamente, a menudo es necesario realizar cortes de servicios manuales para realizar mantenimiento. En vez de tener dichas bajas de servicio reflejadas como un corte de servicio real pueden ser incluidas en el Corte de Servicio Programado, para que sean referenciadas por el paquete de encuestas que se basa en el calendario de cortes. De esta manera, si usualmente realizamos mantenimiento a un servidor todos los miércoles de 8pm a 10pm, podemos incluirlo en el calendario de cortes para que no aparezca como un corte no intencional.

Una funcionalidad interesante desencadenada por los cortes de servicio y/o alarmas, es que cada vez se da una de estas situaciones se pueden crear notificaciones que informen a un responsable la ocurrencia de dicho evento.

Dichos eventos pueden ser tildados como conocidos por el usuario logueado de manera tal que los demás no verán a ese evento porque ya ha sido conocido por uno de ellos. Cuando hablamos de “conocer a un evento” nos referimos a que el usuario que lo tildó deberá hacerse cargo y tomar responsabilidad en el problema que lo originó. Esto mismo sucede con las Alarmas que son disparadas cada vez que un evento ocurre.

Se pueden configurar notificaciones que se activen cuando los eventos importantes son detectados por OpenNMS, los usuarios pueden recibir un aviso siendo un mensaje descriptivo que se envía automáticamente a un celular por SMS, a una dirección de correo electrónico, o ambas. Es importante mencionar que con el fin de recibir las notificaciones, el usuario debe tener la información de la notificación configurado en su

perfil de usuario, como por ejemplo, tipos de notificaciones y niveles de prioridad.

Una vez que se envía un aviso, se considera crítico hasta que alguien acuse de recibo de la notificación a través de la interfaz de notificación (menú "Notifications") de OpenNMS. Si el evento que ha activado el aviso estaba relacionado con los dispositivos de red o sistemas, éstos serán notificados, uno por uno, con una notificación enviada al siguiente miembro de la lista sólo después de que han transcurrido 15 minutos desde el último mensaje que fue enviado. Este escalado de notificaciones, se puede detener en cualquier momento mediante el reconocimiento de la notificación. Se debe tener en cuenta que esto no es lo mismo que reconocer el acontecimiento que provocó el aviso. Si todos los miembros del grupo han sido notificados y la notificación no se ha confirmado, el aviso será enviado a los usuarios del grupo de gestión, donde todos los miembros de ese grupo se le notificarán a la vez.

El menú "Path Outages" sirve para configurar la necesidad de ignorar notificaciones de nodos que parecen estar caídos frente a OpenNMS debido a una falla en un camino de la red entre los nodos y OpenNMS. Por ejemplo, si falla un enlace WAN, entonces todos los nodos en el sitio remoto detrás del dicho enlace parecerán estar caídos. Dado que recibiremos una notificación indicando que el router en la punta del enlace WAN no está respondiendo, no necesitamos notificaciones para todos los dispositivos que están detrás de dicho router.

En el "Dashboard" tenemos una visualización de los nodos discriminados por Routers, Switches y Servers y dentro de estos, Production, Test, y Development. Junto con esto vemos las alarmas, notificaciones, estados y un área donde podemos elegir diferentes gráficos asociados al nodo. Este menú es similar al menú de información del nodo.

En el menú de "Reports" podemos crear una gran variedad de reportes.

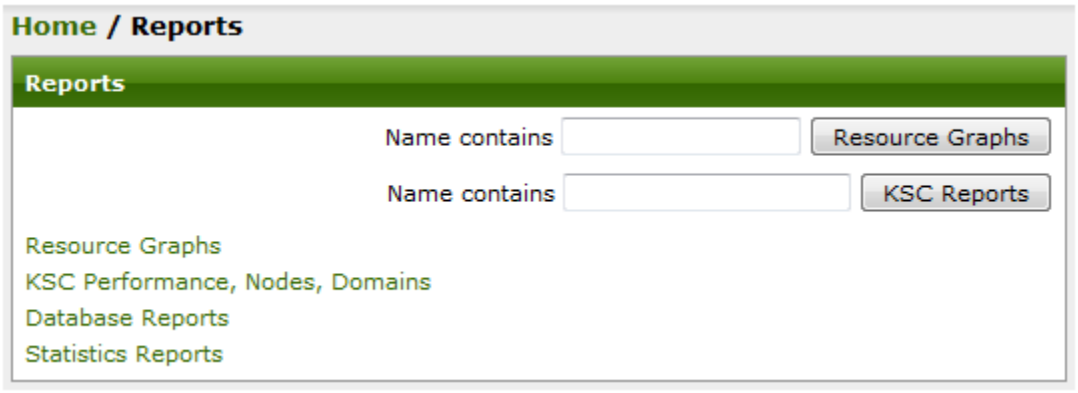

Figura 13: OpenNMS - Reportes

Gráficos de Recursos: Proveen una manera sencilla de visualizar SNMP, tiempo de

respuesta y otros datos recolectados de los nodos manejados a través de la red.

Reportes KSC (Key SNMP Customized), de Performance, de Nodos y de Dominio: Los KSC permiten al usuario crear y ver datos de performance SNMP utilizando tipos de gráficos prefabricados. Los reportes proveen una gran flexibilidad en cuanto a rangos de tiempo y tipos de gráficos. Las configuraciones de los reportes KSC puede ser guardada permitiendo al usuario definir reportes claves que puedan ser referenciados en el futuro. Los reportes de Nodos muestran datos SNMP para todas las interfaces SNMP de un nodo. Los reportes de Dominio muestran datos SNMP para todas las interfaces SNMP en un dominio. Estos dos últimos pueden ser cargados en el "personalizador" y guardados como un reporte KSC.

Reportes de Base de Datos: Proveen una vista gráfica o numérica de las métricas en cuanto al nivel del servicio para el mes en curso, mes anterior, y los últimos doce meses por categorías.

Reportes de Estadísticas: Proveen reportes estadísticos planificados regularmente en forma de datos numéricos (tiempo de respuesta, SNMP, performance, etc.).

En "Charts" podemos ver 3 gráficos. Uno de ellos representa los eventos y alarmas que se dispararon. Otro de los gráficos nos muestra los cortes de servicio que ocurrieron en los últimos 7 días discriminado por servicio. El tercer gráfico muestra el inventario de nodos, interfaces y servicios.

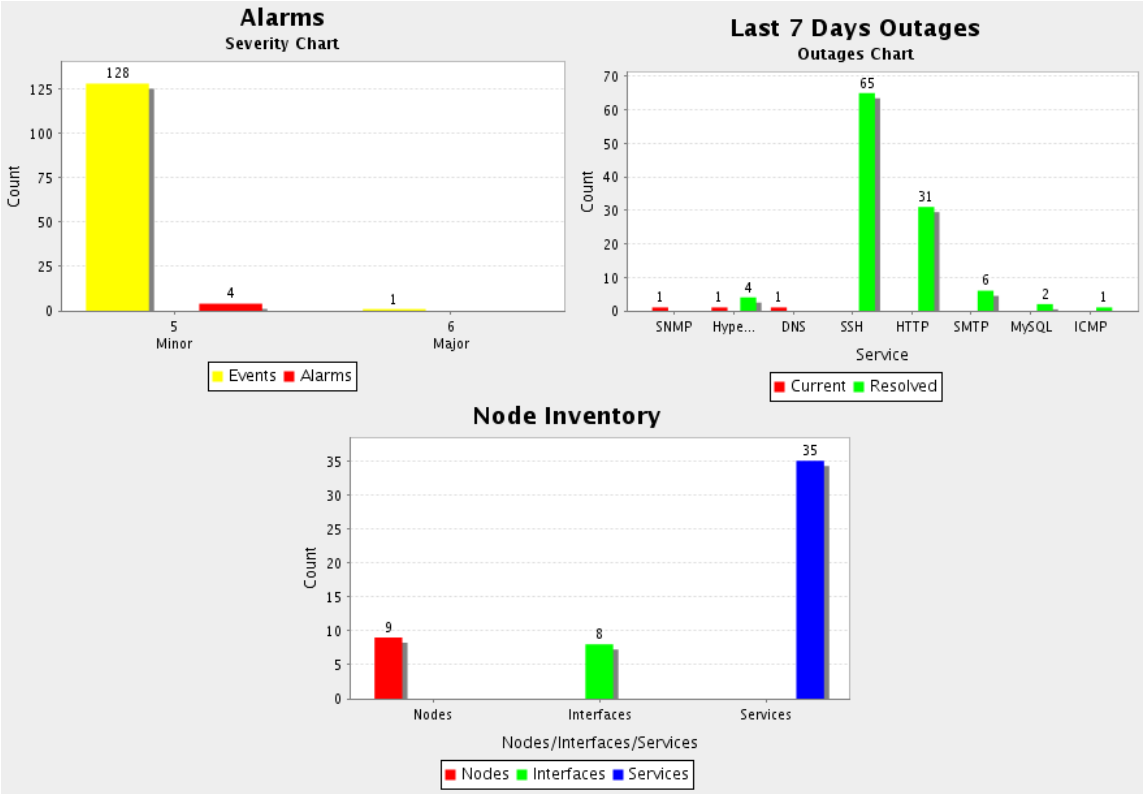

Figura 14: OpenNMS - Estadísticas

El menú “Survelliance” muestra un poco menos de información que el menú de “Dashboard”.

En “Map” podremos definir un mapa de la topología de la red agregando los nodos, uniéndolos, y administrándolos desde el mismo menú permitiéndonos realizar Ping, Traceroute, viendo alarmas y eventos y demás datos relacionados al nodo en cuestión.

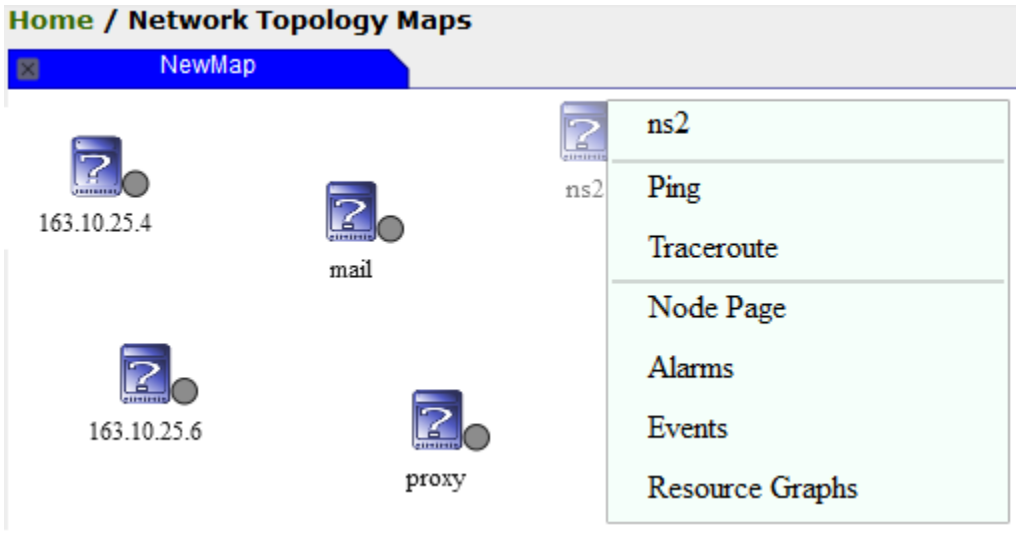

Figura 15: OpenNMS - Mapa de topología

En “Add Node” podemos agregar los activos de forma manual o bien seleccionandolos desde una fuente externa.

En el menú “Admin” podemos configurar Usuarios, Grupos, Roles, ver información detallada del sistema, logs, configurar el descubrimiento de los activos, notificaciones, cortes planificados, administrar nodos, etc.

En “Support” podemos ver información del sistema, licencia y derechos reservados del mismo.

Por último tenemos varios menues cuyos nombres son auto explicativos tales como “Search” y “Assets” quienes buscan activos, “Outages” que busca cortes de servicios, “Events” que busca eventos y “Alarms” que permite buscar alarmas.

Conclusiones de la herramienta

Lo que nos resultó muy interesante de esta herramienta fueron los gráficos y la posibilidad de cargar la información de los activos desde una fuente externa. Otra cosa muy interesante es el hecho de establecer un rango de direcciones IP para que OpenNMS realice el descubrimiento. Con esto la red podría trabajar con direcciones IP dinámicas.

Como desventaja notamos que la herramienta carece absolutamente de controles o medios para poder llevar a cabo un control de la norma. Por eso sería ideal utilizar OpenNMS junto con una herramienta puramente de compliance.

5.3. Hyperic HQ

HypericHQ es una herramienta de monitoreo. Esta herramienta es comercial, sin embargo se ofrece un Trial de 30 días.

Esta aplicación está compuesta por un servidor y un agente que se instala en cada activo a ser monitorizado con la característica particular que mediante dicho agente, el servidor, puede descubrir automáticamente los servicios y recursos con soporte para más de 75 tecnologías diferentes. Hyperic HQ es una herramienta bastante completa a la hora de elaborar Reportes y realizar estadísticas, producto del monitoreo y de análisis de los datos arrojados. Las métricas analizadas por el sistema basado en estadísticas de uso permiten evaluar el tráfico de salida, la utilización de los recursos y la disponibilidad de los mismos.

Un detalle no menos importante es el manejo de un esquema de alertas ante cualquier evento que ocurra sobre el activo. Posteriormente, de acuerdo a la configuración elegida, el sistema generará una notificación o tan solo escalará la misma a personal encargado de resolverla.

¿Cómo funciona HyperHQ?

Esta herramienta consta de cuatro pestañas fundamentales:

- Dashboard
- Resources
- Analyze
- Administration

La primer pestaña es “Dashboard”, la cual centraliza toda la información de los activos que monitoriza, como por ejemplo, el estado de los mismos, las ultimas alertas que se han disparado, los activos que fueron añadidos al inventario para ser monitorizados recientemente, un buscador de activos, etc. Otra característica que posee es la posibilidad de personalizarlo modificando la información de este menú de acuerdo a las necesidades de la organización.

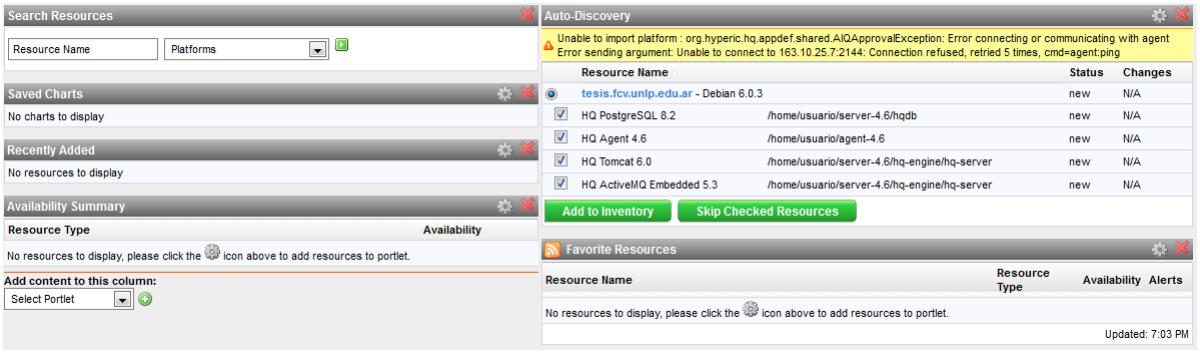

Figura 16: HypericHQ - Dashboard

La segunda pestaña, “Resources”, es un inventario de activos monitoreados que se encuentran diferenciados por: sus servicios, sistemas operativos instalados, tipo de procesador, cantidad de interfaces de red, etc. Dentro de esta misma pestaña está la posibilidad de listar todos los activos que están actualmente apagados. Este listado puede además, ser discriminado por servicios de los activos al igual que por activo.

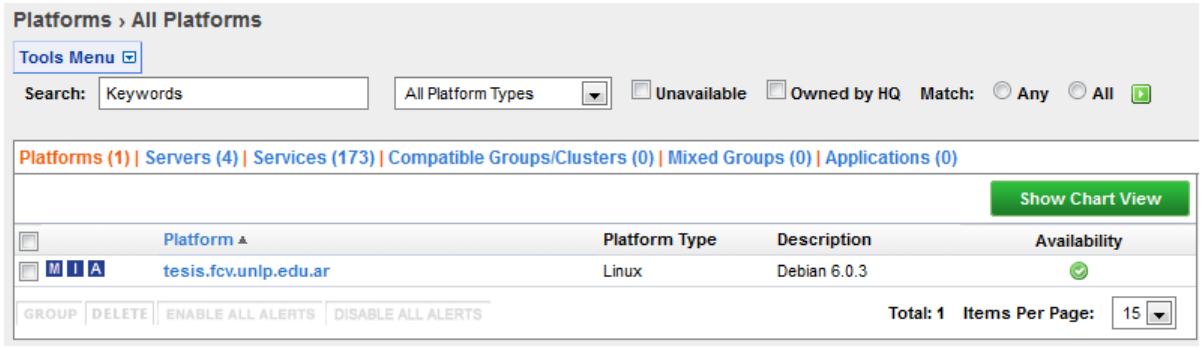

Figura 17: HypericHQ - Inventario de activos

Por cada activo listado se puede obtener el detalle de cada uno de sus componentes (cliqueando en el mismo) discriminado por tipo y marca del mismo y una serie de métricas que el sistema realiza al monitorizar. Una vez elegido el activo accederemos 4 submenues “Monitor”, “Inventory”, “Alert” y “Views”.

El primer menú al cual accederemos es “Monitor”, el cual nos muestra en la parte superior, los datos pertinentes al equipo físico.

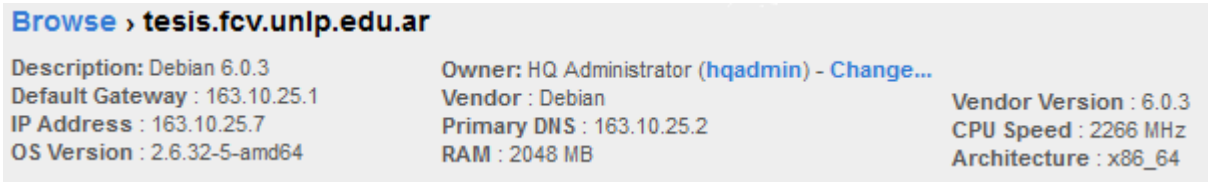

Figura 18: HypericHQ - Detales del activo

Luego en la parte inferior izquierda podemos ver los servicios que están ejecutándose en el activo y su disponibilidad.

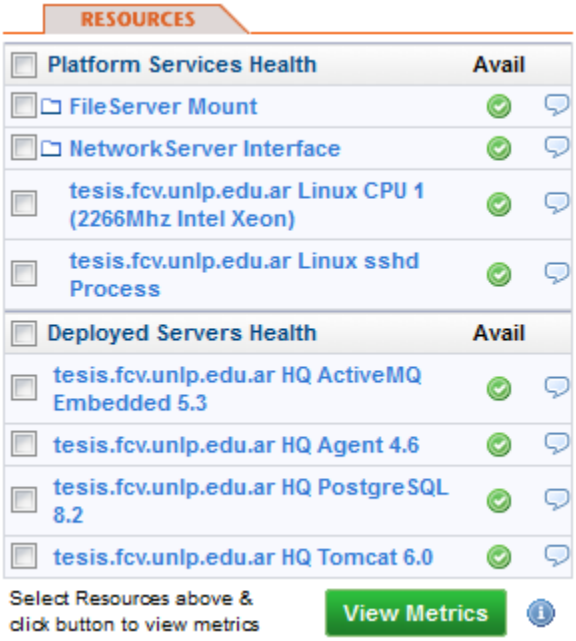

Figura 19: HypericHQ - Servicios del activo

En la imagen anterior vemos que todos los servicios están iniciados y funcionando, por ende todos se muestran en color verde con su ícono correspondiente. A continuación se muestran todos los indicadores que el sistema seleccionará de acuerdo a la disponibilidad del servicio:

	100 % disponibilidad
	Disponibilidad entre 0 % y 100 %
	0 % disponibilidad
	El recurso está pausado
	No se recolectaron datos de disponibilidad en el marco de tiempo especificado

Cuadro 2: HypericHQ - Indicadores de disponibilidad

En la parte inferior derecha podemos ver información detallada del activo tal como memoria libre, memoria de swap, carga del procesador, etc. Esto podemos verlo en forma numérica como se ve en la siguiente imagen o bien en forma de gráfica.

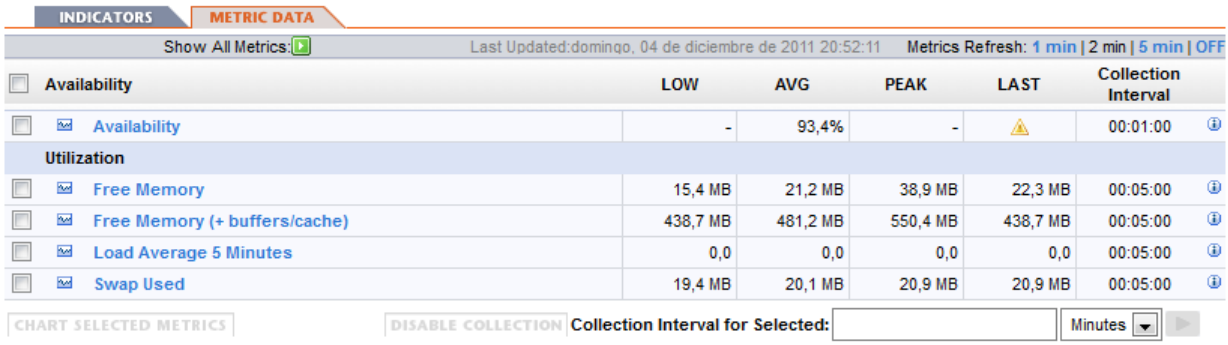

Figura 20: HypericHQ - Mediciones del activo

En el submenú “Inventory” vamos a ver la misma información (excepto la de monitoreo en tiempo real) del activo seleccionado. Aquí nos da la posibilidad de editar la información inherente al activo y/o a los servicios del mismo en caso de que no hayan sido cargados correctamente por el sistema.

En el submenú “Alert” podremos definir nombre-descripción de la alerta, las condiciones que harán que la alerta se haga presente y una acción a ejecutar. El sistema nos presenta diferentes opciones a la hora de establecer la condición para que se ejecute la alerta. Estas opciones están determinadas por métricas (disponibilidad, memoria libre, etc.), propiedades del activo (Version del SO, RAM, Velocidad de CPU, etc.), tipo de evento ocurrido (Error, Advertencia, etc.) o cambios en la configuración del activo.

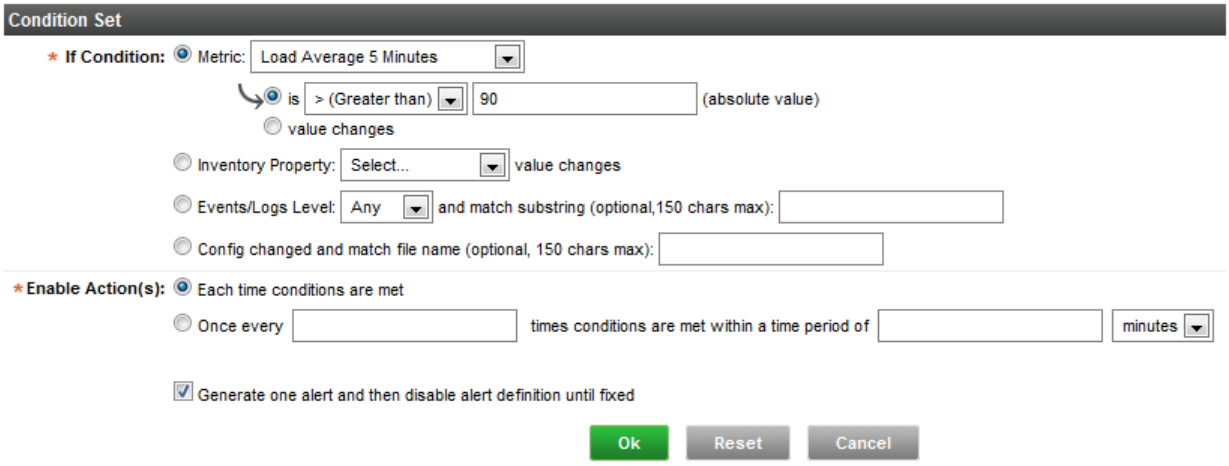

Figura 21: HypericHQ - Definición de reglas

Por último el submenú views nos presenta un listado de comandos de consola que pueden ser ejecutados en tiempo real, tales como netstat (listado de conexiones activas), cpuinfo, top (listado de procesos), entre otros.

El sistema se basa en la siguiente tabla para realizar estimaciones sobre la disponibilidad de los activos.

A su vez, las alertas proveen la opción de notificar a los usuarios del sistema mediante el Dashboard web, por mail o SMS a través de un escalamiento de la alerta. Para ello podemos definir un esquema tipo plantilla en el que se puede definir diferentes tipos de notificaciones que se pueden entregar al aparecer una alerta. Esta plantilla puede definirse desde el menú “Administration” como se puede ver en la imagen a continuación.

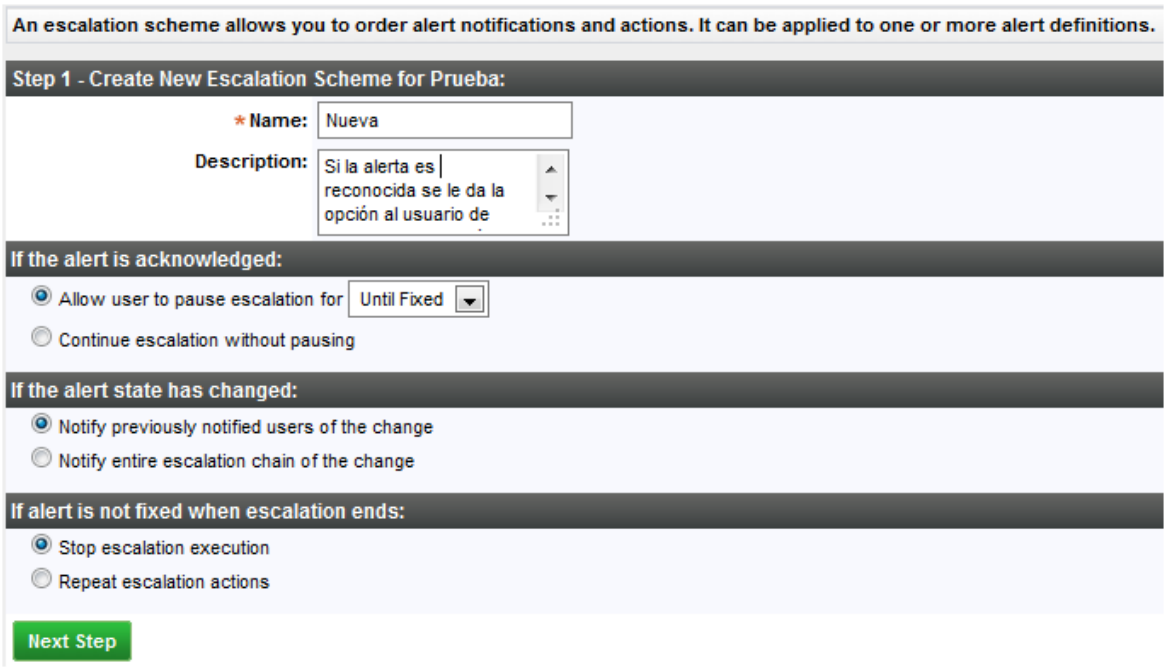

Figura 22: HypericHQ - Esquemas de notificación

En el siguiente paso definimos el método de notificación y los destinatarios.

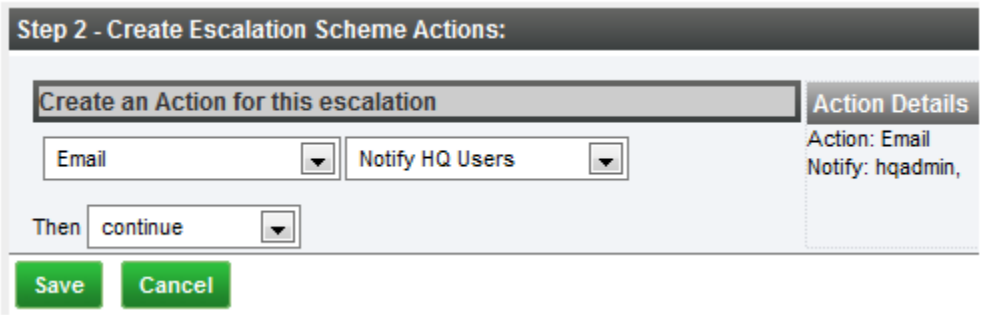

Figura 23: HypericHQ - Esquemas de escalado

Una vez definida la misma, podremos verla en el panel principal de alertas.

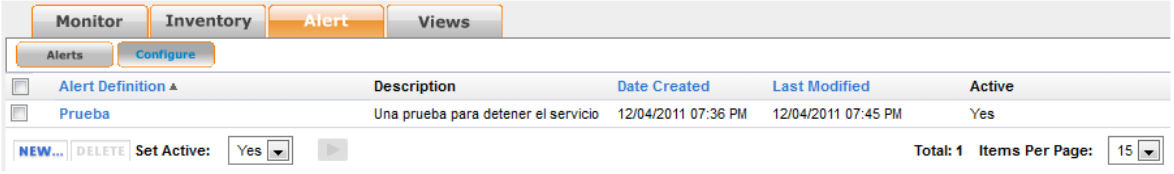

Figura 24: HypericHQ - Panel de alertas

La tercer pestaña llamada “Análisis” se puede decir que es la más importante a la hora de configurar una notificación por algún evento que ocurra sobre los activos monitorizados, esencialmente tiene dos submenús: el primero es “Alert Center” en donde se listan todas las alertas que han ocurrido sobre un determinado activo, ya sea por algún evento en su servicios o en su plataforma. El segundo, “Event Center”, es en donde se listan todos los eventos realizados por el sistema, por ejemplo, el lanzamiento de una alerta.

Como podemos apreciar en la siguiente imagen, en “Alert Center” podemos ver la manifestación de la alerta que configuramos previamente (la cual se generó a partir de la caída de uno de los servidores).

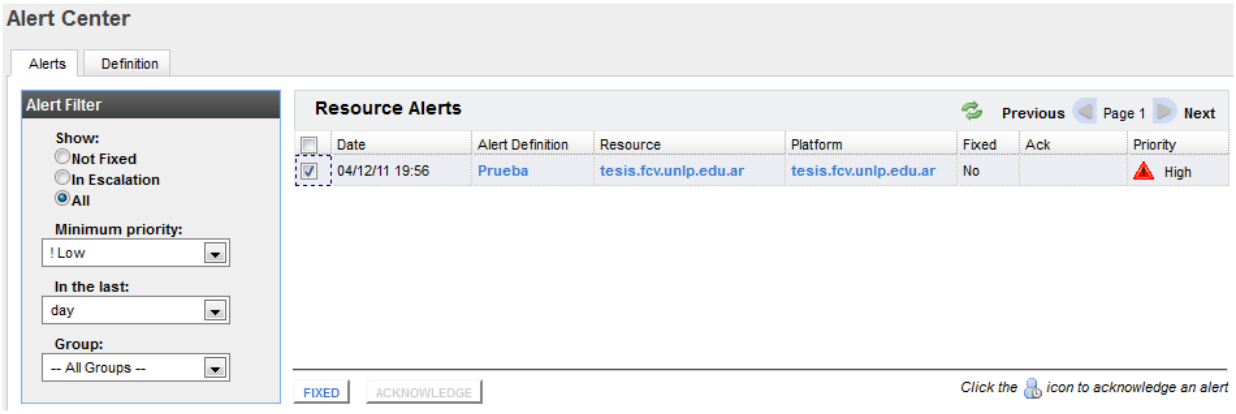

Figura 25: HypericHQ - Centrol de alertas

Cuando se dispara una alerta tenemos la opción de arreglar el problema que surgió e hizo dispararla, en ese momento podemos tildarla como “Fixed” para que el sistema deje de notificarte por la misma alerta.

Para tratar una alerta en la versión Trial sólo podemos resolverla con el botón Fixed, aclarando con comentarios cuál fue la acción tomada. Con la versión paga (Enterprise) podemos generar roles y escalar la alerta a otro tipo de usuario (elevar la alerta de acuerdo a una jerarquía organizacional que refleje a los perfiles en la organización).

Conclusiones de la herramienta

Una de las ventajas que vimos en HypericHQ es que al instalar el agente, en cada uno de los clientes podemos acceder a información mucho más completa de los activos en la red. De esa manera también es más fácil detectar intrusos ya que tenemos más datos del equipo que está en la red (a pesar que el software no está orientado a monitorear la misma).

Como desventaja notamos que al configurar el agente te requiere que se le indique la IP y el puerto al cual el servidor debe conectarse para obtener el estado y demás

datos del agente. Con este esquema, el agente se ve imposibilitado de utilizar una IP dinámica.

Sería interesante que el programa cliente (agente) pueda reportar al servidor ante un cambio de IP sin tener que ser configurado manualmente.

Con Hyperic HQ obtenemos más datos sobre los activos que con otros sistemas. El sistema está orientado al monitoreo de activos y no a la red. Debido a que una gran parte de las organizaciones son los activos eso sería de gran utilidad usarlo en conjunto con otros sistemas que tengan monitoreo de red o herramientas puramente de compliance.

5.4. Securia SGSI

Securia SGSI es una herramienta de compliance totalmente gratuita y de código cerrado.

Esta herramienta permite realizar un seguimiento de la implementación de la norma ISO/IEC 27001:2005, puesta en funcionamiento, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información.

Es un software completamente gratuito que se estructura en cuatro módulos:

- Módulo de Gestión Documental.
- Módulo de Análisis y Gestión de Riesgos.
- Módulo de Gestión de Incidencias y No Conformidades.
- Módulo de Mejora Continua.

El módulo de **Gestión Documental** se caracteriza por establecer una organización de los documentos exigidos por la norma para evitar cualquier daño físico de los mismos ya que deben estar protegidos y controlados.

El módulo de **Análisis y Gestión de Riesgos** es el que está en contacto con los activos que se monitorizan. Posee un inventario de procesos y activos, una valoración del impacto de cada uno de los mismos, identificación de amenazas y vulnerabilidades, cálculos de riesgo (cuál es el riesgo de que ocurra un evento sobre un determinado activo), decisión de criterios de aceptación (a qué nivel se considera un riesgo aceptable), toma de decisiones (ante un evento, que acción correctiva o preventiva se debe aplicar) y evaluación del nivel de seguridad.

El módulo de **Gestión de Incidencias y No conformidades** se destaca por brindar seguridad a la organización de que los eventos que ocurran sobre los activos o las

vulnerabilidades de los mismos estarán cubiertos con la posibilidad de elaborar acciones correctivas.

En el módulo de **Mejora Continua** se pueden elaborar acciones preventivas y de mejora que permitan al SGSI adaptarlo a nuevos cambios y mantener al mismo en constante evaluación de manera tal que la seguridad de los activos perdure a lo largo del tiempo.

¿Cómo funciona Securia SGSI?

Este sistema está formado por dos aplicaciones, una aplicación de **Administración** y otra **Cliente**. En la aplicación de administración se configuran todos los parámetros necesarios para implementar y mantener un SGSI. Se definen los usuarios que intervienen en el sistema y sus respectivos roles. Esta aplicación conecta contra una base de datos en la que se almacena toda la información relativa al sistema.

Como mencionamos anteriormente SecuriaSGSI incluye un cliente a través del cual permitirá a cada usuario acceder al sistema y poder realizar las funciones necesarias en función de su perfil de usuario en el sistema. Tiene como función principal conectar al usuario con el SGSI, validando previamente la identidad de éste, y otorgando los privilegios de acceso correspondientes previamente establecidos. Una vez conectado, el sistema proporciona toda la funcionalidad necesaria para interactuar con los módulos presentes en el SGSI antes mencionados.

El Programa de **Administración** es el encargado de configurar los módulos que componen el sistema, así como los usuarios con acceso al mismo, y sus privilegios de acceso. En primer lugar al iniciar por primera vez el programa de administración se debe crear un nuevo Sistema de Gestión de Seguridad de la Información, el cuál simulará al sistema que realmente se quiere incorporar a la entidad. En cuanto a la definición de usuarios, tenemos una interfaz que nos permite cargar los datos personales del usuario para que luego puedan ser asociados a diferentes perfiles. Al sistema de Administración se accede con un usuario administrador que es el usuario de la base de datos Postgres (de la cual depende SecuriaSGSI); cuando accedemos con este usuario se mostrarán los siguientes menues.

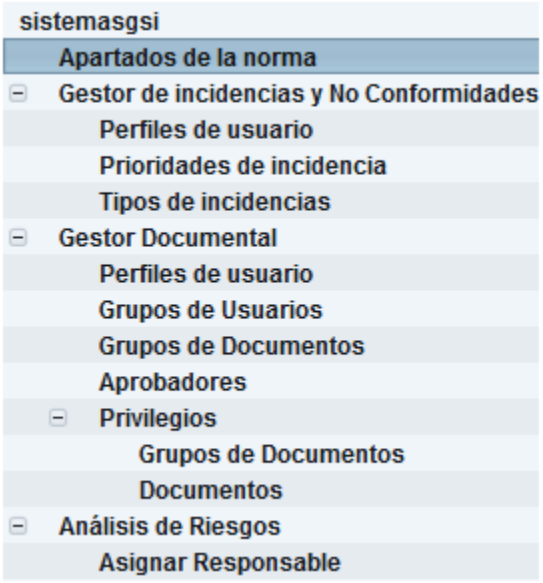

Figura 26: SecuriaSGSI - Panel de administracion

Dentro de la Gestión de Incidencias y No Conformidades tenemos la posibilidad de definir Perfiles de usuarios que pueden acceder a ciertas áreas del sistema, los cuales podrían mapearse con los cargos definidos en la organización. También se pueden definir Prioridades y tipos de incidencias, las prioridades indican el nivel de atención que se le debe aplicar, por ejemplo, existen incidentes cuya resolución no debe demorarse y otros que se atienden por orden de ocurrencia, mientras que el tipo indica la descripción de la incidencia, por ejemplo, Denegación de Servicio, Derechos de Acceso, etc.

En la gestión Documental tenemos la misma opción con respecto a los perfiles de usuarios, en este caso definimos si pertenece al grupo de usuarios lectores o escritores de documentos, con la posibilidad de ampliar los grupos definidos. En esta sección se pueden detallar nuevos grupos documentales a parte de los ya definidos por SecuriaSGSI, éstos servirán para reunir un conjunto de documentos que traten un mismo tema.

En el menú de Aprobadores, se deben definir responsables de aprobar estos documentos como también los privilegios que deben tener los diferentes perfiles usuarios sobre estos documentos. Es importante destacar que para ser un responsable para el análisis de riesgos, el usuario no debe pertenecer a ningún perfil de usuario de la sección Gestor Documental.

Para el análisis de riesgos el sistema sólo asigna responsables que son usuarios del sistema, dichos responsables serán los encargados de realizar una evaluación sobre el nivel de riesgos que puede sufrir la organización, ya sea por vulnerabilidades en los activos o por inseguridad física.

Con respecto a la aplicación **Cliente**, está conformada por una organización similar a la aplicación de Administración, sin embargo el objetivo es proveer al usuario las

características para manejar el sistema y gestionar el SGSI.

Para la operatoria del mismo se nos presentarán los cuatro módulos indicados anteriormente (de acuerdo al perfil del usuario logueado algunos pueden no estar disponibles), los cuales aparecen en la pantalla principal:

Figura 27: SecuriaSGSI - Menu principal de aplicación Cliente

El **Gestor Documental** es una base de documentos que está clasificada por grupo documental, un código, fecha de creación y de caducidad, si es un borrador o es el documento aprobado por la persona responsable, la versión y otros datos relevantes.

En primer lugar podemos crear una representación de un documento existente (siempre y cuando seamos usuarios pertenecientes al perfil "Escritor"). Para esto el sistema permite adjuntar dicho documento en cualquier formato y solicitar al menos una revisión del mismo para que pueda ser aprobado por el responsable, y desde ese momento se puede descargar el documento [1]. Cabe destacar que, en el caso de que haya más de una versión de un mismo documento, esta debe ser revisada.

Una vez creada la representación de dicho documento (actualmente en estado borrador) se debe pedir una revisión. La misma solo podrá ser llevada a cabo por un usuario con perfil de "Aprobador". Una vez elegido el usuario que realizará la aprobación el sistema nos abre una pantalla para enviar un mail.

Otra de las cosas que nos permite hacer es indicar a uno o más usuarios de la lectura obligada del documento en cuestión. Con lo cual, el sistema avisará a dichos usuarios que deben leer el documento y confirmar su lectura.

[1] Con respecto a esto, el sistema posee un manejo poco claro con el cual se debe tener cuidado. Al crear una representación de un documento, el usuario que lo creó puede "aprobarlo" y a su vez descargar el documento real para su uso.

En el sistema de Administración los Escritores no pueden ser los mismos que aprueban los documentos. En el menú de creación de documentos quien escribe puede "aprobarlo" y puede descargarlo. A pesar de esto, el documento aparecerá como "pendiente de aprobación" hasta que sea realmente aprobado por alguien con los permisos necesarios. Sin embargo el documento podrá ser descargado para su uso por cualquier usuario (incluso un Lector). El documento real asociado al sistema solo debería ser descargable una vez que el mismo haya sido aprobado por un "Aprobador" y figure en estado "Aprobado", con lo cual haciendo lo anteriormente indicado podemos evitar esta regla.

Adicionalmente podemos relacionar otros documentos al documento previamente creado. Todo esto se puede ver en la siguiente imagen.

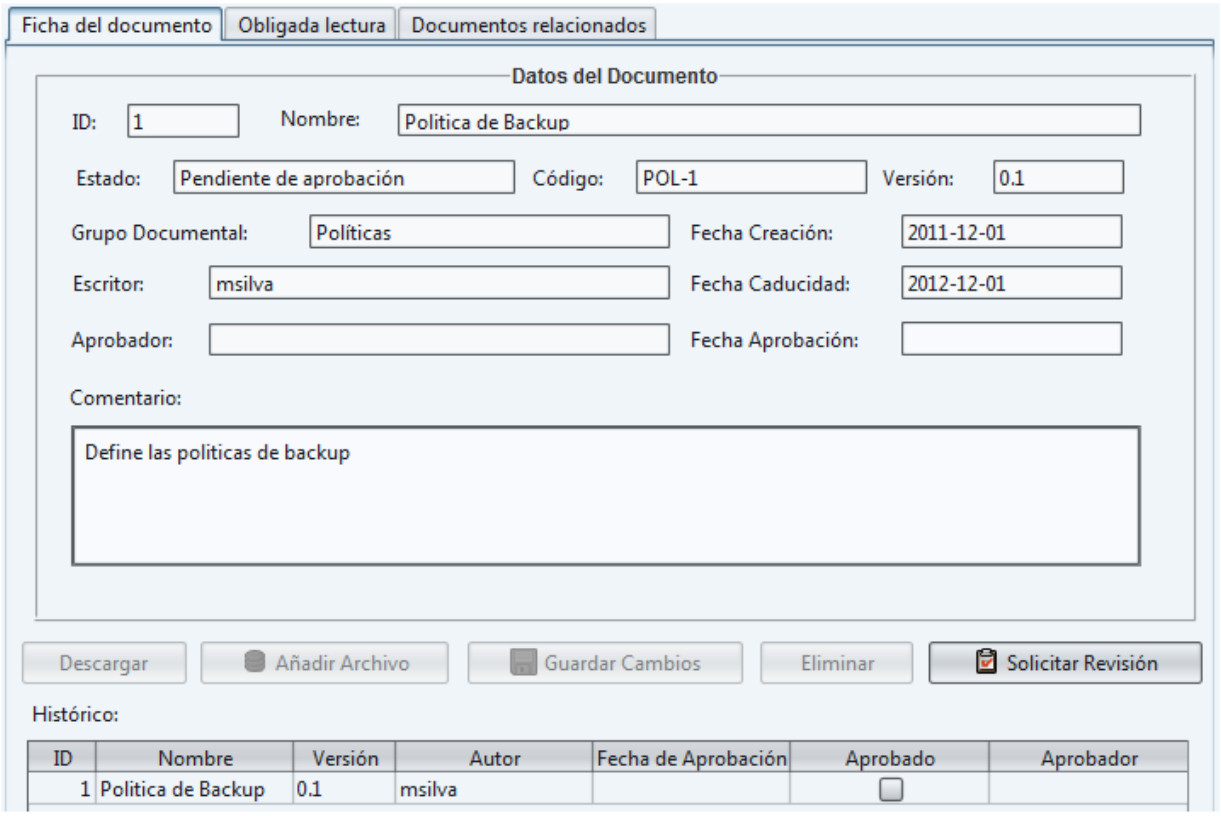

Figura 28: SecuriaSGSI - Datos del documento

La sección de **Análisis de Riesgos** se divide en dos partes, por una lado la configuración y por otro el análisis.

En la Configuración el sistema nos permite configurar todos los detalles previos que deben conocerse de la organización para poder analizarlos en función de obtener un nivel del riesgo, es decir, utilizaremos estos datos para realizar la gestión de los riesgos. Es importante recordar que el nivel de riesgo se calcula en base al valor del activo + el valor del impacto (cuán importante es la pérdida del activo) + el valor de la probabilidad de que la amenaza ocurra.

Entre los detalles de configuración se encuentran los siguientes:

Figura 29: SecuriaSGSI - Menu de análisis de riesgos

En el menú para Editar las Dimensiones, se pueden definir los criterios que se deben plantear en términos de integridad, disponibilidad y confidencialidad.

Con respecto a los Escenarios que pueden manifestarse en caso de la ocurrencia de alguna amenaza que impacte de manera notable a la organización.

En el menú de Controles definimos aquellos que aplican o aplicarían a la organización estableciendo a qué grupo y subgrupo de control pertenecen, el identificador asociado, el estado actual y el estado objetivo.

Se pueden definir las Vulnerabilidades que tienen los activos, asociándolas a sus respectivas. También se pueden configurar los Niveles de Riesgo, es decir a qué nivel el riesgo se considera aceptable o no.

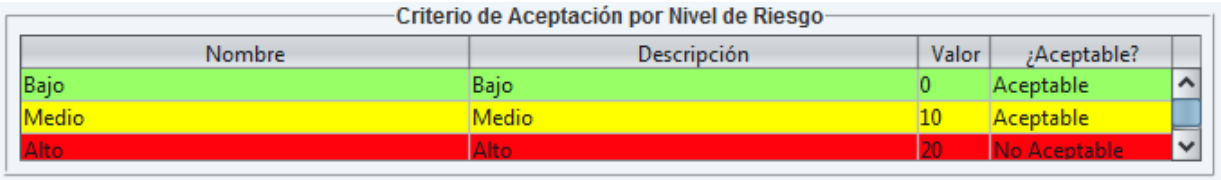

Figura 30: SecuriaSGSI - Niveles de aceptación del riesgo

Por último, en el menú de Probabilidad definimos la nomenclatura de la probabilidad de la ocurrencia de las amenazas.

Con respecto al Análisis de los riesgos tenemos el siguiente menú, que nos permitirá realizar las evaluaciones correspondientes para calcular el nivel de riesgo:

Figura 31: SecuriaSGSI - Menu de análisis

Existen una serie de pautas que debemos establecer, en el menú "Actividades/Procesos de Negocios". Para que el análisis de riesgos tenga un efecto positivo en la organización es necesario identificar las diferentes prioridades a lo largo de cada uno de sus procesos de negocio. De esta forma podremos realizar un plan estratégico basado en la importancia y el impacto de nuestras acciones que beneficien la seguridad de la información de nuestra compañía. En segundo lugar especificamos los Activos que tenemos y queremos proteger identificando la categoría a la que pertenecen (Organización, Hardware, Software, Servicios, Datos o información, etc.), el responsable de cada uno de ellos, el cargo del mismo dentro de la organización y la actividad o proceso en el que interviene.

Otro de los menues es el de "Amenazas". Aquí, el sistema permite definir nuevas amenazas entre las que ya se encuentran definidas, cada una de ellas tiene un nombre, descripción, a que naturaleza pertenece (desastres naturales, de origen industrial, errores o fallos no intencionales, o ataques intencionados), y a qué dimensión/es afecta/n.

En el menú de "Test Inicial" podremos asignar a los controles de la norma una serie de preguntas que vienen por defecto en el sistema. A pesar de esto se pueden agregar preguntas personalizadas. De esta manera podremos ir teniendo un registro con el detalle de los controles que están siendo implementados. En el caso de que los controles no apliquen tenemos la posibilidad de marcalos como no aplicables y describir por qué no aplican. Además se nos provee un reporte con el cual podemos ver todos los controles, sus preguntas y respuestas.

Luego tenemos el cálculo de riesgos divididos en dos menús: Cálculo Riesgo Intrínseco y Riesgo Efectivo.

La evaluación del riesgo intrínseco se lleva a cabo sin tener en consideración los mecanismos de salvaguarda que puedan actuar. Este tipo de riesgo intrínseco se toma como referencia para evaluar la efectividad de las salvaguardas a aplicar.

Cuando hablamos de salvaguarda nos referimos a las acciones a aplicar para redu-

cir el riesgo. Entonces, el riesgo efectivo es aquel en el que si se toma en cuenta la salvaguarda.

Al riesgo le asignaremos una categoría (Hardware, Sofware, Servicios, etc. predefinidos en el sistema), la probabilidad y la salvaguarda.

En el menú "Declaración de Aplicabilidad (SOA)" dispondremos de todos los controles que fueron definidos previamente en el menú "Controles" dentro de la parte de Configuración del Análisis de Riesgo, indicando su aplicabilidad o no y por qué. Lo que podremos hacer en este menu es simplemente agregar/cambiar la justificación y generar un reporte de aquellos controles que aplican y no aplican a la organización.

En el "Plan de Acción" deberíamos ver el listado de los controles y el plan de acción de cada uno de acuerdo a lo definido en el menú "Test Inicial". Debido a que el sistema tiene un bug, éste menú no muestra nada.

En el menú de "Cálculo Riesgo Residual" el sistema nos hace una cruza de los activos, las amenazas y las categorías de los mismos. Aquí podremos definir, a cada uno de estos ítems, la probabilidad de riesgo residual. Vale la pena aclarar que el riesgo residual es el riesgo resultante luego de aplicar un control o tomar una acción. También podremos realizar reportes de Riesgo residual por categorías y por activos.

En el menú de "Selección de Contoles" deberíamos ver un cruce de los controles asociados con sus amenazas y categorías. Este es otro de los menúes que no muestra información. Estamos casi seguros que se debe a un bug en el sistema.

En el **Gestor de Incidencias y No conformidades** tenemos las siguientes opciones:

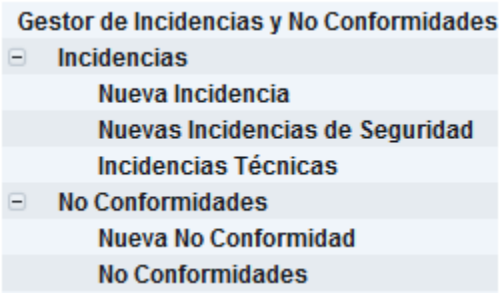

Figura 32: SecuriaSGSI - Menú de gestor de incidencias y no conformidades

En principio podemos definir una Nuevas Incidencia junto con sus datos respectivos. En este momento la misma aparecerá dentro del menú "Nuevas Incidencias de Seguridad". Al editarla tendremos la opción de clasificarla como incidencia técnica o no conformidad y asignar responsables (los cuales serán notificados a través e-mail). Por consiguiente, la misma se moverá de "Nuevas Incidencias de Seguridad" a "Incidencias Técnicas" (independientemente de su clasificación).

A esta incidencia le podemos asociar una acción correctiva, asignando un responsable para su implementación, un plazo de ejecución y el costo asociado.

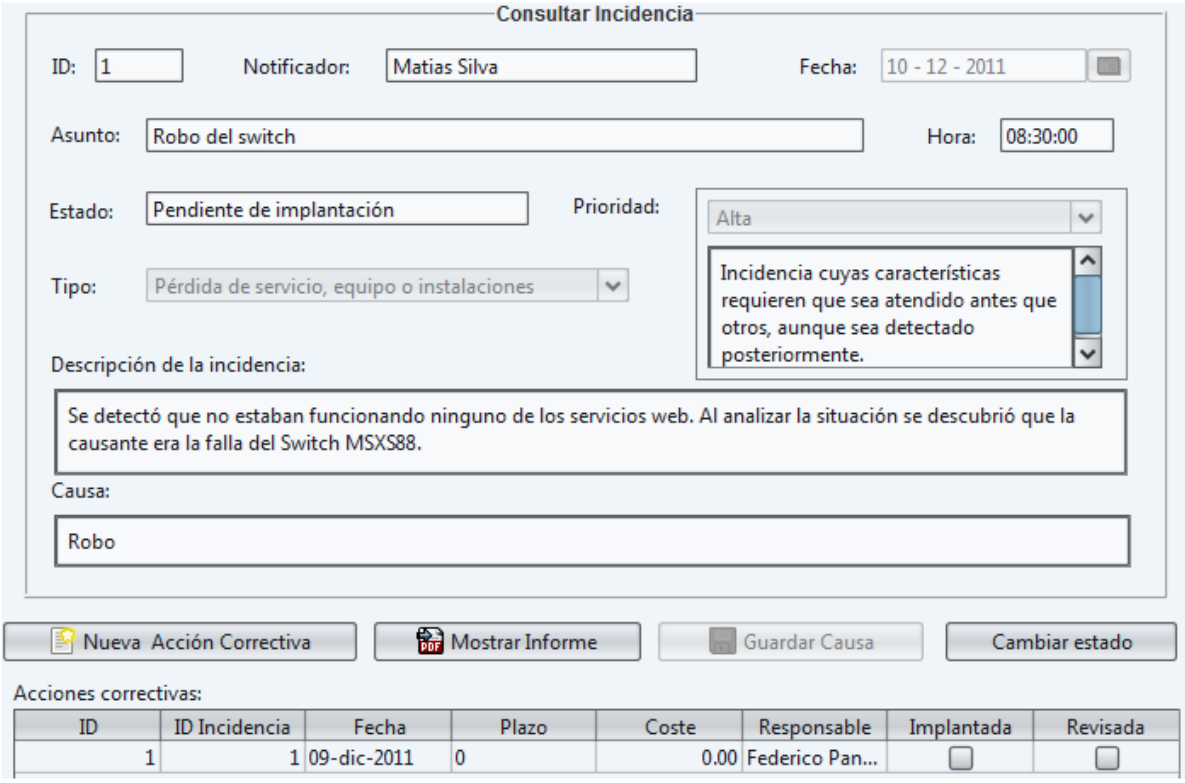

Figura 33: SecuriaSGSI - Detalles de una incidencia

A su vez podemos realizar un seguimiento de esta acción correctiva mediante la opción "Control de Eficacia y Cierre de la acción" que aparece en el detalle de la acción correctiva en cuestión. Aquí se pone la fecha, el responsable del control, si ha sido revisado (y si así lo fue si ha sido eficaz o no).

De la misma manera que con las incidencias podemos crear una Nueva No Conformidad en donde debemos indicar el apartado de la norma con el cual no se está cumpliendo, la fecha, y la explicación de la misma. Al crear la misma aparecerá en el menú de "No Conformidades". También podemos asociarle una acción correctiva junto con su seguimiento, como se explicó anteriormente.

La acción correctiva puede ser cerrada sin aplicar una acción correctiva (para los casos donde su resolución sea inmediata y no sea necesario). En este caso no tenemos ninguna forma de indicar una acción inmediata (que no es lo mismo que una acción correctiva).

SecuriaSGSI, a su vez, permite hacer búsquedas filtradas por algún criterio y además se pueden elaborar informes en PDF indicando las incidencias y no conformidades que

se han manifestado.

Por otro lado tenemos el módulo de **Mejora Continua**.

Lo primero que debemos hacer, es definir qué tipo de acción es (preventiva o de mejora).

Una vez definida la acción, la misma aparecerá listada "Acciones de Mejora" o "Acciones Preventivas" según sea su tipo. Durante el Control de la Eficacia de la misma, el responsable del control debe describir cuales fueron sus métodos de control y si ha cumplido o no con los plazos pautados, luego el responsable del sistema debe indicar si ha revisado dicha acción y si ha sido eficaz, de lo contrario, deberá señalar a su criterio que observaciones ha hecho.

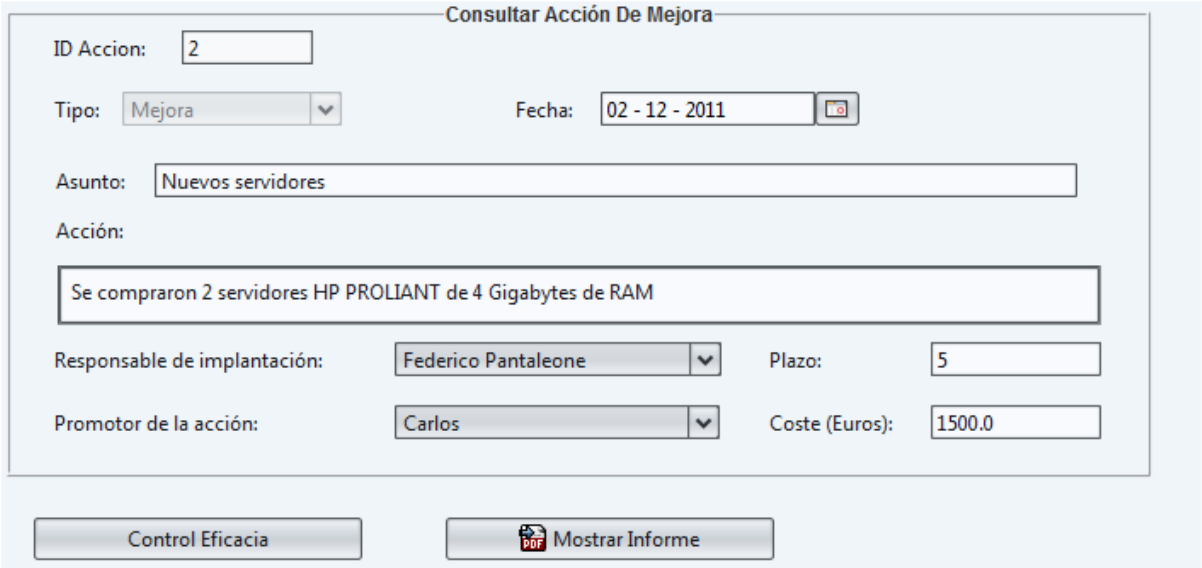

Figura 34: SecuriaSGSI - Acción de mejora

A nivel de sistema la pantalla de acciones correctivas, acciones preventivas y mejoras son iguales. La diferencia radica en el significado y el tipo de uso que se le dé a las mismas:

- Las *acciones correctivas* se dan después de un incidente.
- Las *acciones preventivas* se hacen para evitar el riesgo; antes de que ocurran incidentes.
- Las *acciones de mejora* se toman para mejorar el SGSI o a la organización, pero la falta de éstas no resulta directamente en un riesgo (a diferencia de las otras preventivas).

Conclusiones de la herramienta

Encontramos como desventaja el hecho que no está muy clara bien la diferencia entre Grupos y Perfiles. Si un usuario está en un grupo el mismo no puede realizar aprobaciones de documentos. Esto es un poco confuso.

Otra desventaja es que las notificaciones a través de e-mail no son automáticas, sino que SecuriaSGSI abre una ventana de correo electrónico para que el usuario envíe un mail, con lo cual queda a criterio del usuario el envío o no y en el primer caso, que información enviar.

Con respecto a la parte de análisis de riesgo encontramos como desventaja técnica el hecho de que el sistema posee bugs. Hay ciertos menús que no muestran datos, por ejemplo al hacer un reporte de activos, la valoración del impacto de activos, el plan de acción y la selección de controles. Debido a eso dichas características no pudieron ser analizadas correctamente.

Como ventaja podemos destacar que es muy completa en cuanto al manejo de la norma. A partir de una incidencia se puede generar una no conformidad y a partir de ella cerrarla o definir una acción correctiva. Para la misma existen opciones para verificar la implementación de dicha acción y luego verificar su eficacia.

5.5. Easy2Comply

Ésta es una herramienta de compliance comercial y de código cerrado.

Easy2Comply está compuesta por 5 familias de productos.

1. El Software de Manejo de Control Interno
2. Software de Manejo de Riesgo
3. Software de Manejo de IT-GRC (Governance Risk Controls)
4. Software de Manejo de Auditorías
5. Framework de Open-Compliance

Todo esto se encuentra en un solo sistema accedido a través de usuario y contraseña. El mismo es altamente configurable y se ajusta a cualquier tipo de organización asimismo como a cualquier norma, entre ellas, ISO/IEC 27001:2005.

Al loguearnos al sistema tenemos acceso a los siguientes ítems:

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

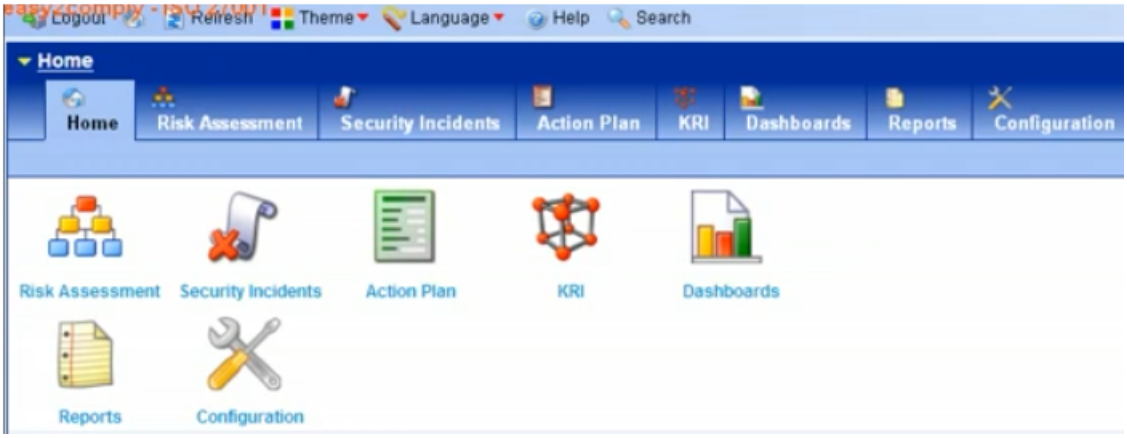

Figura 35: Eas2Comply - Panel principal

Éstos pueden variar dependiendo del nivel de acceso del usuario, excepto la configuración que está disponible para todos los usuarios. Los menues mencionados anteriormente pueden ser configurados y cambiados de nombre. Por ejemplo al primer menú de la lista lo puedo llamar "Documentación y Prueba" o "Asesoramiento del Riesgo" o como me resulte más útil.

Dentro del menú de **Documentación y Prueba / Asesoramiento del Riesgo**, tenemos una pantalla dividida en dos. A la izquierda se encuentra una especia de árbol de directorios al estilo del Explorador de Windows, donde la raíz es el nombre del ítem que estamos administrando. A la derecha tendremos la información relativa al ítem seleccionado.

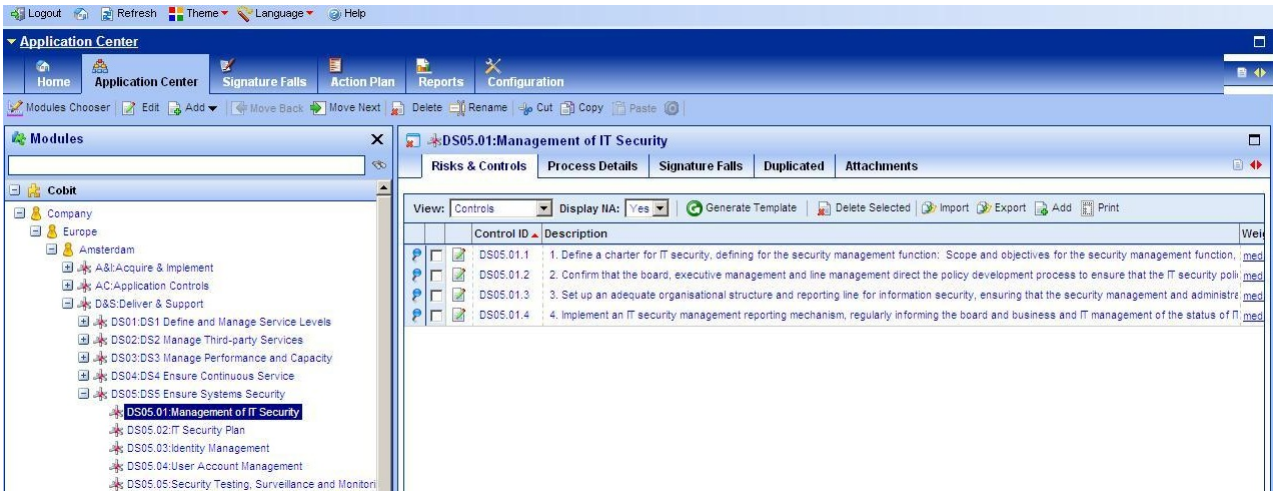

Figura 36: Eas2Comply - Centro de aplicación

Puede haber más de un árbol. Por ejemplo uno para manejar los controles de la ISO/IEC 27001:2005 (puntos de la norma asociados a las características de la organización) y otra para manejar ítems específicos de la organización (activos, empleados, etc.). Estos árboles pueden ser armados totalmente de acuerdo a las necesidades del usuario, lo presentado aquí es solo a modo de ejemplo.

Los sub-ítems son los que definimos como unidades de negocio y procesos. Cuando creamos o elegimos uno, se abre a la derecha una pantalla para registrar información relevante a dichas unidades de negocio y/o procesos. Dentro de éstos podemos agregar a su vez sub-ítems, en los cuales podemos agregar más detalle sobre el proceso.

Cada uno de estos ítems tienen las siguientes solapas (que se ve en la parte derecha de la pantalla) “Riesgo y Control”, “Gráfico de Flujo”, “Narrativo”, “Detalles Generales”, “Perfil del Riesgo”, “Firma” y “Adjuntos”.

- Dentro de ”Riesgo y Control” tenemos una lista de riesgos para el ítem y dentro de cada riesgo podemos especificar diversos controles.

Figura 37: Eas2Comply - Riesgos y controles

Con respecto a los riesgos, podemos categorizarlos y clasificarlos (abriendo una ventana para tal fin) y agregar información de acuerdo a nuestras necesidades. En la pestaña "Asistencia Cualitativa" dentro de dicha ventana, podemos analizar el riesgo en cuestión indicando el impacto vs probabilidad lo cual nos mostrará un puntaje asociado al riesgo y una tabla con colores para hacer más visual y ágil la tarea de análisis del mismo.

Figura 38: Eas2Comply - Probabilidad/Impacto del riesgo

En la pestaña "Asistencia Cuantitativa" donde podremos asociar el riesgo con lo material (en términos monetarios) y la pérdida que supondría la efectivización de tal riesgo.

Para un control, podemos especificar el "Peso" (prioridad), si debe llevarse a cabo o no (puede ser sólo una recomendación), su efectividad, la prueba de la efectividad, si es o no ejecutable y quien fue el responsable de la prueba del control.

Aquí podemos seguir agregando complejidad al proceso agregando el Control de la Documentación. Podemos categorizar el control, definir el propietario, indicar cuáles son los controles claves y la frecuencia de control (indicando al sistema para que genere recordatorios vía email cada cierto tiempo). El siguiente paso es la Prueba del Control, donde podemos crear el Plan de Pruebas, junto con la frecuencia, la metodología y el procedimiento asociado. Una vez que el Plan de Pruebas es creado, Easy2Comply notificará al Tester vía email sobre la creación de dicho Plan de Pruebas. Luego, dentro

de la solapa “Estado del Control” tenemos una pestaña de ”Hallazgos” donde podemos volcar los resultados de las pruebas y luego en la pestaña ”History” podemos ver los escenarios de prueba y mails intercambiados en el transcurso del tiempo.

Además, a los controles dentro de esta pestaña podemos agregar tareas (que luego podremos ver desde el menú principal Plan de Acción) asociadas (abriendo una ventana para tal fin), a las cuales les podemos indicar el tipo, costos, sub-tareas, estados, fecha de creación, mensajes, adjuntos, etc. Cuando la tarea sea completada, el responsable será notificado automáticamente por Easy2Comply.

- Dentro de “Detalles Generales” podemos asignarle tags para su futura búsqueda, un nombre, descripción, fecha, relevancia, propietario del proceso y demás al ítem en cuestión. A su vez, dentro de esta solapa tenemos otras dos relacionadas con Cuentas Financieras y Sistemas de Computación que estén relacionados con el proceso.

- En la solapa “Gráfico de Flujo” podemos definir la representación del proceso y asociarlo con los controles y riesgos. Esta información será completada automáticamente en la solapa “Narrativo”.

- En “Adjuntos” podemos asociar uno o más documentos .doc, .xls, .pdf, etc. para asociarlo al proceso.

- La solapa Perfil de Riesgo se basa en una serie de preguntas predefinidas por el sistema (aunque también podemos crear nuestras propias preguntas y asociarlas a un template) las cuales definen el tipo de pregunta, el peso o importancia, y la respuesta (completada por nosotros). Luego, en la misma pantalla se nos presenta un Nivel de Riesgo y ciertas métricas para manejar el mismo.

Con respecto a los **Eventos de Pérdida / Incidentes de Seguridad** veremos una pantalla con diversa información que nos indicará los detalles, la descripción, el estado, los riesgos que causaron la pérdida, quien lo registró, junto con el costo material asociado en dos pestañas “Pérdida Directa” y “Pérdida Indirecta”. También podemos documentar lo sucedido y hacer un seguimiento del mismo.

En el menú de **Indicadores claves de Riesgo / Métricas de Riesgo** podemos medir cualquier evento relacionado con la organización. Este menú no es muy complejo y nos da la posibilidad de personalizar la métrica asignando un valor en un formato predefinido por el sistema (por ejemplo, numérico), agregar una descripción y rangos (mayor o igual, menor, etc.,) para que el sistema analice y luego el responsable analice generando pruebas del mismo.

El menú de **Firma** nos permite poder trabajar con Firmas digitales para dar veracidad de que la información que describe a los procesos es precisa y confiable.

La funcionalidad **Reportes** nos presenta tres tipos de reportes “Reportes Embebidos”, “Reportes en Excel” y “Templates de Reportes”. Los “Reportes Embebidos” van a mostrarse dentro de la interfaz del sistema. Se pueden generar reportes de varios tipos como procesos de firma, matriz de documentación, fechas de controles, etc.

Los “Reportes en Excel” y “Templates de Reportes” son reportes específicos donde podemos definir la información específica que queremos ver.

En el **Dashboard** vamos a ver gráficos de los procesos, riesgos, controles, eventos de pérdida, entre otros, que seleccionemos. La mayoría de los gráficos son interactivos y pueden explotarse para sacarle el máximo provecho y tener una visualización más rápida de lo que deseamos saber. Hay una larga variedad de gráficos disponibles como ser gráficos de tortas, barras, etc.

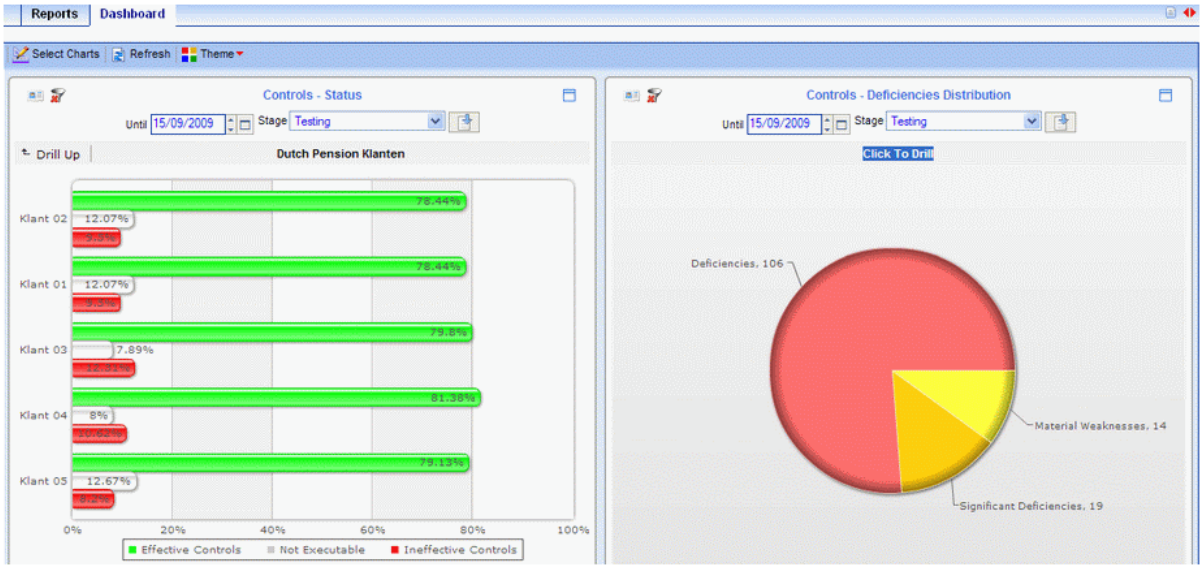

Figura 39: Eas2Comply - Reportes gráficos

Conclusiones de la herramienta

Esta herramienta no posee monitoreo de ningún tipo. Es por ello que sería interesante utilizarla junto con una herramienta que provea esto, como por ejemplo, las ya vistas OpenNMS o HypecicHQ.

Como ventaja encontramos la posibilidad de configurar prácticamente toda la herramienta para que se ajuste a la organización en cuestión. También podemos adaptarla para que controle cualquier norma (incluso interna a la organización).

Easy2Comply provee muchas opciones para realizar la gestión de la documentación, activos, riesgos y demás, permitiendo realizar varias revisiones dentro de un calendario dado y mantener el seguimiento de todas las revisiones.

Capitulo 6

6 Conclusiones

La idea de este capítulo es plasmar las conclusiones obtenidas en base al análisis de la norma ISO/IEC 27001:2005, IRAM-ISO/IEC 27004:2011 y de las herramientas de monitoreo y compliance, que herramientas podemos aplicar para los distintos requerimientos de la norma, cuales son las características claves de las mismas y en consecuenca, cuales deberían ser las características deseables en un sistema para implementar un SGSI.

6.1. Cuadro Comparativo y Checklist

A continuación presentaremos un cuadro que permitirá un rápido análisis de las características de las herramientas. A partir de él podremos realizar una comparación visual entre las mismas y transformar los resultados en un checklist que podría utilizarse para seguir como guía en la implementación de un sistema de gestión de un SGSI.

Estos criterios fueron tomados en base a los requerimientos de la norma ISO/IEC 27001:2005 para la implementación de un SGSI. Al analizar las herramientas se observaron las características presentes en ellas, de mayor importancia que sirvieron de guía para conformar el siguiente cuadro comparativo.

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 %**

Cuadro 3: Funcionalidades de las herramientas

6.2. Herramientas e ISO27001

En esta sección iremos recorriendo cada uno de los requerimientos generales de la norma ISO/IEC 27001:2005 y analizaremos con cuales de las herramientas analizadas

podremos implementar dichos requerimientos.

Los requerimientos de la norma ISO/IEC 27001:2005 han sido previamente detallados en la seccion 3.3. En esta sección sólo se hará referencia a los requerimientos de manera global (sin entrar en detalle en cada uno de los requerimientos específicos de cada sección).

La **Sección 4.2** de la norma ISO/IEC 27001:2005 habla del SGSI, como establecerlo, implementarlo, monitorearlo, revisarlo, mantenerlo y mejorarlo. Debido a que las herramientas que nosotros analizamos son todas capaces de gestionar un SGSI podremos decir que todas en menor o mayor grado pueden cumplir con todos los requerimientos de un SGSI.

La **Sección 4.3** habla de los requerimientos de documentación.

Dentro de la **Sección 4.3.1** y **4.3.2** habla de los documentos generales y su control.

Easy2Comply nos provee de una característica para controlar la documentación (cualquiera sea ella), asociando todos los detalles pertinentes al documento, cargando el documento en el sistema, generando recordatorios para su revisión, dando la posibilidad de generar un plan de pruebas en el cual podemos realizar hallazgos y mejorar el documento.
SecuriaSGSI nos provee un módulo completo dedicado a la gestión documental, el cual nos permite asociar todos los datos pertinentes del documento, cargarlo en el sistema, relacionarlo con otros documentos, asignale un aprobador, de manera tal que el documento no pueda ser leído hasta que el mismo no haya sido aprobado. También provee una opción de lectura obligada del documento, con lo cual el sistema notifica a la/s personas/s que debe/n leer el documento. Los documentos deberán tener una fecha de caducidad con lo cual el sistema automáticamente avisará a las personas responsables de su aprobación para realizar una revisión.

Dentro de la **Sección 4.3.3** se especifican los requerimientos de los registros.

Con respecto a los registros, todos los sistemas analizados en esta tesis funcionan como registros, ya que toda la información monitorizada y cargada por usuarios queda registrada y disponible para su futura referencia. Ahora, Easy2Comply y Securia, al proveer manejo de la documentación tienen a su vez un mejor manejo de lo que podria ser un registro. Sin embargo, ninguna de las herramientas provee una característica para definir plantillas personalizadas de registros, ej.: registro de visitas, auditorías, etc.

La **Sección 5** especifica requerimientos sobre la Alta Dirección. Este tipo de requerimientos no pueden ser solventados por ningun sistema. Lo que la norma pide es que la Alta Dirección tenga el compromiso de realizar determinadas tareas para la gestión

de un SGSI, con lo cual para esta sección no aplica ninguna herramienta, depende del factor humano.

La **Sección 6** habla de las auditorías internas. Para esta sección podemos aplicar diferentes herramientas de diferentes maneras.

Una de las herramientas mas completas para mantener información sobre auditorías es SecuriaSGSI, debido a que la misma tiene un módulo completo dedicado a Incidencias y No conformidades, las cuales son sumamente útiles a la hora de realizar auditorias y gestionar los hallazgos encontrados en estas. También posee manejo de acciones preventivas y de mejora. Otra de las cosas que pueden llegar a ser importantes en una auditoria interna es el estado de los controles requeridos por la norma, el estado de las amenazas, vulnerabilidades y riesgos.

Otra de las herramientas que nos podría ser de gran utilidad para esta sección es Easy2Comply quien posee manejo del riesgo y los controles requeridos por la norma que están siendo aplicados. También tenemos un manejador de Incidentes de Seguridad con el cual podremos revisar el histórico de las mismas y aplicar un plan de acción.

Luego OSSIM también puede sernos de utilidad en una auditoría interna para revisar el estado de la red, las amenazas, vulnerabilidades e incidentes ocurridos. En base a los resultados obtenidos podemos generar un plan de acción. Sin embargo éste plan no podremos generarlo con esta herramienta. Otra de las cosas que podemos realizar en la auditoria seria revisar el estado de los controles requeridos por la norma gracias al Compliance Mapping.

La **Sección 7** especifica requerimientos sobre la revision gerencial del SGSI. Para asistir tales requerimientos podriamos utilizar todas las herramientas analizadas de alguna u otra manera.

Dentro de la sección **Sección 7.2** hay requerimientos sobre los insumos para poder realizar la revisión.

Con Easy2Comply podriamos revisar el estado de la documentación, controles aplicados y mediciones de riesgo.

Con SecuriaSGSI podríamos revisar el estado de los controles aplicados, documentación, estado de acciones preventivas y correctivas y las recomendaciones de mejora.

Con las herramientas de monitoreo (OSSIM, OpenNMS y HypericHQ) podríamos identificar todos aquellos cambios que puedieran afectar el SGSI tales como, amenazas, vulnerabilidades, eventos de la red, ataques, etc. Adicionalmente con OSSIM podremos ver el el estado de los controles aplicados y el nivel de riesgo actual.

Dentro de la **Sección 7.3** se detallan los requerimientos del resultado de la revisión.

Con Easy2Comply y SecuriaSGSI podremos revisar los niveles de riesgo y/o criterios

de aceptación del mismo y plan de tratamiento del riesgo.

Con OSSIM podremos revisar el nivel de riesgo actual.

El resto de las herramientas no pueden asistir practicamente en nada en el resultado de la revisión.

La **Sección 8** habla del mejoramiento continuo.

Dentro de la **Sección 8.2** se detallan los requerimientos para una Acción Correctiva.

SecuriaSGSI provee de una funcionalidad específica para tratar las acciones correctivas, con lo cual lo hace la herramienta ideal para esta sección. Ésta es la única herramienta que puede ser utilizada en esta sección.

Dentro de la **Sección 8.3** habla sobre los requerimientos de una Acción Preventiva.

Nuevamente SecuriaSGSI, por proveer una funcionalidad dedicada a las acciones preventivas la hace la herramienta ideal para esta sección.

Sin embargo las herramientas de monitoreo como OSSIM, OpenNMS e HypericHQ pueden servir como la base necesaria para prevenir incidentes de seguridad, ya que estas pueden detectalos y alertarnos sobre los mismos. Lo que no podremos hacer con estas herramientas sera registrar la información pertinente y requerida para registrar una acción preventiva.

Como conclusión quisieramos explicar que a pesar de que Easy2Comply, SecuriaSGSI y en algunos casos OSSIM son las que más toman relevancia en las diferentes secciones de la norma, es muy importante contar con herramientas de monitoreo para relevar ciertos datos que de otra manera no podríamos hacelo.

Por último se muestra a modo de resumen del análisis previamente realizado un cuadro con las distintas secciónes de la norma y las herramientas que pueden/podrian asistir en su implmementación.

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	✔	✔	✔	✘	✔

Cuadro 4: Herramientas e ISO 27001

6.3. Requerimientos para una herramienta de Gestión un SGSI

Para la elaboración de una herramienta de gestión de un SGSI debemos tener en cuenta diversos aspectos. En este punto se presentarán funcionalidades que fueron reunidas en base a criterios obtenidos del análisis de la norma ISO/IEC 27001:2005 y a las mejores características observadas en las herramientas previamente investigadas.

A continuación se listan cada una de las funcionalidades y se detalla que es lo que se pretende de cada una de ellas:

Manejo de Activos En primer lugar, una herramienta de gestión de un SGSI debería poseer la funcionalidad para controlar los activos. Esto es muy importante ya que en este tipo de sistemas los activos son la base del SGSI. Las características deseables con las que la misma debería contar son:

- Identificación por IP
- Nombre de usuario (si aplica)
- Servicios que está ejecutando
- Información del hardware / SO
- Estado de recursos del hardware
- Log de sucesos relevantes del activo
- Disponibilidad del activo y sus servicios

Tratamiento de Riesgos El objetivo de dicha funcionalidad es proveer de cierta manera un nivel de riesgo, que puede representado de manera gráfica o numérica y que esté asociado al SGSI y/o a las diferentes partes del mismo. Las características deseables con las que la misma debería contar son:

- Vista rápida del nivel de riesgo (gráfico/numérico)
- Cálculo del riesgo (valoración de activos y probabilidad de impacto)
- Manejo de vulnerabilidades
- Escala de riesgo (Ej.: 1,. . . , 5 o Bajo,. . . , Alto)
- Valoración del riesgo (Impacto / Probabilidad)
- Manejo de amenazas
- Manejo de planes de acción
- Correlación de controles con amenazas
- Correlación de riesgos y controles

Gestión de Documentación La herramienta debería poseer la habilidad de manejar documentos ya que los mismos son vitales en cualquier organización. Las características deseables con las que la misma debería contar son:

- Manejo de documentos (Identificación, nombre, revisión, vigencia, etc.)
- Revisión y aprobación de documentos
- Perfiles de usuarios y niveles de acceso a los documentos
- Manejo de registros no-tecnicos (auditorías, visitas, capacitación del personal, etc.)

Compliance Checklist La Herramienta debe poseer como mínimo una lista donde se presenten los controles requeridos por la norma ISO/IEC 27001:2005. Las características deseables con las que la misma debería contar son:

- Listado de controles requeridos
- Manejo de aplicabilidad de los controles
- Correlación de controles y documentación/planes/monitoreo

Monitoreo Una característica extremadamente útil para una herramienta de un SGSI es sin duda la habilidad de monitorear sucesos en la red. Las características deseables con las que la misma debería contar son:

- Monitoreo de conexiones entrantes/salientes de hosts
- Análisis de tráfico de la red
- Análisis de puertos
- Log de sucesos relevantes
- Filtros de búsqueda por IP, puertos, servicios, etc.
- Configuración de alarmas
- Gestión de vulnerabilidades
- Mapa de topología de la red
- Notificaciones de eventos (SMS, mail, etc.)

Plan de Pruebas Por último sería muy interesante el hecho de que la herramienta cuente con un plan de pruebas. Esto sería muy útil para gestionar las actividades administrativas de un SGSI, tales como Revisión por la dirección, vigencia de la documentación, actualización de procedimientos, auditorías internas, pruebas del SGSI previa a la auditoría, etc. Las características deseables con las que la misma debería contar son:

- Planificación de la prueba (PLAN)
- Documentación de la prueba (DO)
- Revisión y hallazgos de la prueba (CHECK)
- Plan de acción resultante de la prueba (ACT)

6.4. Aportes de la Tesis

En este trabajo se analizó la norma ISO/IEC 27001:2005 la cual habla de un SGSI y los requerimientos adicionales para certificar la norma.

Por un lado estudiamos las herramientas que podrian dar soporte a la implementación de un SGSI en lo que respecta al sistema informático. En base al estudio realizado hemos visto que ninguna de ellas cubren en forma completa los aspectos necesarios para gestionar un SGSI. Dichos aspectos, que nosotros consideramos de suma importancia han sido presentados en la sección 6.1.

Por otro lado se analizaron los requirimientos para certificar la norma ISO/IEC 27001:2005 analizando que herramienta podria dar soporte a la implementación de cada uno de dichos requerimientos en cada una de las secciones de la norma. Esto fue presentado en la seccion 6.2.

En base mencionado anteriormente y debido a la importancia de contar con un SGSI realizamos un checklist (sección 6.3) de lo que serian las caracteristicas con las que deberia contar una herramienta pada poder dar soporte completo a un SGSI. Esto sirve de base a un trabajo futuro de implmementación de una herramienta de ese tipo o para

la evaluación de otras herramientas para gestionar un SGSI.

Adicionalmente se estudiaron los aportes que realiza la IRAM-ISO/IEC 27004:2011 (Capítulo 4) y concluímos en que no hay ninguna herramienta (de las analizadas) que puedan asistir en la generación/implementación de un programa de medición de manera directa, es decir ninguna provee una caracteristica para armar un programa de medición.

Sin embargo para realizar las mediciones necesitaremos datos que pueden ser recabados de las herramientas. En el caso de las herramientas de monitoreo podría recolectar datos técnicos de incidentes de la red, con los cuales generaríamos nuestras propias mediciones. Con respecto a las herramientas de compliance podriamos generar métricas en base a la cantidad de controles que actualmente estamso aplicando y medir su eficacia o su eficiencia.

Otra de las conclusiones que obtuvimos es, que, de acuerdo a nuestra experiencia en Sistemas, nunca existirá un sistema ideal que que se encargue de controlar todos los aspectos en un SGSI (o de otro tipo de sistema). De hecho gran parte de los requerimientos y controles a realizar requieren la intervención humana.

Nos parece importante mencionar un ejemplo con respecto a lo anterior. Ninguna de las herramientas analizadas provee el manejo que la norma requiere en cuanto a los registros. Si bien seria una caracteristica útil, en general, en cualquier organización, para mantener registros se utilizan planillas de cálculos tales como Microsoft Excel o Open Office u alguna otra herramienta especializada para el manejo de registros.

Hay que tener en cuenta que, a pesar de que herramientas de compliance parecen entrar en juego con más frecuencia en cuanto a dar soporte a la norma (por o a lo analizado en la sección 6.2) debemos entender que muchos de los ítems que require la norma están relacionados con la documentación y la evidencia, con lo cual éste tipo de herramientas parecen (a simple vista) ser mas adecuadas.

No obstante, las herramientas de monitoreo poseen una característica muy importante: la habilidad de detectar eventos de diferentes tipos, clasificaros y alertar sobre la ocurrencia de los mismos. Dicha característica es la base de todas las mediciones y análisis, que luego serán reflejados en informes o documentos propios herramientas de compliance. Es por ello que siempre hemos remarcado, a lo largo del trabajo, la importancia que tiene una herramienta de monitoreo como una de compliance.

6.5. Trabajo a futuro

Por último se listan los ìtems que por motivo de alcance no fueron incluídos en esta tesis pero que son de gran importancia para que sean tomados como referencia para trabajos a futuro.

- Implementación de una aplicación o modificación de herramientas existentes para cumplir con los criterios previamente establecidos para un software de gestion de un SGSI.

- Análisis en profundidad de las necesidades de una herramienta que dé soporte a la norma IRAM-ISO/IEC 27004:2011.
- Análisis de la ISO/IEC 27006:2007, que establece los requerimientos para los auditores y SGSI, y su relación con las herramientas existentes. Posibilidad de desarrollo de una herramienta para dar soporte a una auditoría de un SGSI.

Referencias

[1] ISO/IEC 27001:2005 - *Sistemas de gestión de seguridad de la información – Requerimientos*

[2] IRAM-ISO/IEC 27004:2011 - *Gestión de seguridad de la información - Medición*

[3] iSetec - Seguridad de la información
http://www.isetec.com.ar

[4] El portal de ISO 27001 en español
http://www.iso27000.es

[5] Instituto Nacional de Tecnologías de la Comunicación
http://www.inteco.es

[6] AlienVault
http://www.alienvault.com

[7] The OpenNMS Project
http://www.opennms.org

[8] Securia SGSI
http://www.securia.es/forja

[9] Hyperic
http://www.hyperic.com

[10] Easy2Comply - Governance, Risk and Compliance Software
http://www.easy2comply.com

[11] Denial of Dervidce (DoS)
http://en.wikipedia.org/wiki/Denial-of-service_attack

[12] CISSP Certification (2003) - Shon Harris