UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL, SISTEMAS Y ARQUITECTURA

"GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA TOMA DE DECISIONES EN LA INFRAESTRUCTURA DE LA RED TELEMÁTICA DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO UTILIZANDO COBIT 5 Y SOFTWARE OPEN SOURCE"

Tesis para optar el título de **Ingeniero de Sistemas** que presentan los autores:

César Augusto Junior Arenas Villanueva

Diana De Los Santos Mendoza

ASESOR:

M. Sc. Ing. Ernesto Karlo Celi Arévalo

LAMBAYEQUE – PERÚ

DICIEMBRE 2017

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL, SISTEMAS Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA TOMA DE DECISIONES EN LA INFRAESTRUCTURA DE LA RED TELEMÁTICA DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO UTILIZANDO COBIT 5 Y SOFTWARE OPEN SOURCE"

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PRESENTADO POR:

Bach. César Augusto J. Arenas Villanueva
RESPONSABLE

Bach. Diana De Los Santos Mendoza
RESPONSABLE

M. Sc. Ing. Ernesto Karlo Celi Arévalo
ASESOR

APROBADO POR:

M. Sc. Ing. Bernardo Núñez Montenegro
PRESIDENTE DEL JURADO

M. A. Ing. Robert Edgar Puican Gutiérrez
MIEMBRO DEL JURADO

Mg. Ing. Juan Elías Villegas Cubas
MIEMBRO DEL JURADO

ASPECTO INFORMATIVO

TÍTULO DEL PROYECTO DE INVESTIGACIÓN:

Gestión de la seguridad de la información para la toma de decisiones en la infraestructura de la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo utilizando COBIT 5 y software Open Source.

PERSONAL INVESTIGADOR:

Autores:

Arenas Villanueva César Augusto Junior

De Los Santos Mendoza Diana

Asesor:

M. Sc. Ing. Celi Arévalo Ernesto Karlo

DECRETO DECANAL DE APROBACION:

110 – 2016 – UNPRG - FICSA

ESCUELA PROFESIONAL:

Ingeniería de Sistemas

TIPO DE INVESTIGACIÓN:

La presente investigación es del tipo:

- **Tecnológica**, porque se encamina a descubrir nuevos conocimientos, a la que posteriormente se le buscan aplicaciones prácticas dentro de un entorno. En este caso, a la mejora de la gestión de la seguridad de la información.
- **No experimental**, porque se realizará sin manipular deliberadamente las variables en juego y se basará fundamentalmente en la observación del fenómenos tal y como se da en el contexto natural para analizarlo con posterioridad.
- **Descriptiva**, debido a que los datos se utilizarán directamente de la realidad sin manipulación alguna que pueda alterar los resultados. Por otro lado, se definirán las características, procedimientos, fuentes, técnicas, categorías, observaciones, etc. que influyan directamente con el objeto de estudio, es decir con la gestión de la seguridad de la información en la UNPRG.

ÁREA DE INVESTIGACIÓN:

a) Según la UNESCO, la presente investigación pertenece al área 33: Ciencias Tecnológicas.
b) Según el Plan Estratégico de la UNPRG 2013 – 2021, la presente investigación pertenece al área: Desarrollo de tecnologías e innovación.

LÍNEA DE INVESTIGACIÓN:

a) Según la UNESCO, la presente investigación pertenece a la línea 3304: Tecnología de los ordenadores.
b) Según el Plan Estratégico de la UNPRG 2013 – 2021, la presente investigación pertenece a la línea: Tecnologías de la Información y Comunicación (TIC).

PROGRAMA DE INVESTIGACIÓN:

a) Según la UNESCO, la presente investigación pertenece al programa 3325: Tecnología de las comunicaciones.
b) Según el Plan Estratégico de la UNPRG 2013 – 2021, la presente investigación pertenece al modelo: Modelos de madurez de tecnologías de la información.

LOCALIDAD E INSTITUCIÓN DONDE SE REALIZARÁ EL PROYECTO

Red Telemática de la Universidad Nacional Pedro Ruiz Gallo de Lambayeque.

AGRADECIMIENTOS

En primer lugar quiero agradecer a nuestro Creador por iluminarnos y permitirnos terminar nuestro proyecto de tesis con éxito.

En segundo lugar agradezco a mis padres que a lo largo de toda mi vida siempre me han apoyado para alcanzar mis metas.

En tercer lugar un agradecimiento muy especial a nuestro asesor el M. Sc. Ing. Ernesto Karlo Celi Arévalo por sus conocimientos brindados así como su apoyo en todo momento para el desarrollo de la presente investigación y al Ing. Vladimir Gonzales Mechán por su guía durante la implementación de la prueba piloto en la Red Telemática de nuestra casa de estudios.

Finalmente agradezco a Michael y mis amigos cercanos que de alguna manera han aportado para la culminación de este proyecto.

Diana De Los Santos Mendoza

Un agradecimiento especial a Jehová mi Dios, quien gracias a su ayuda y bendición he logrado cumplir uno de mis más grandes logros: ser un profesional.

A mi familia, quienes de alguna u otra forma, me apoyaron siempre en el cumplimiento de mis metas.

Y finalmente, un agradecimiento a nuestro asesor el Ing. M. Sc. Ernesto Karlo Celi Arévalo por todo el apoyo brindado y al Ing. Vladimir Gonzales Mechán por las facilidades en la aplicación de las pruebas piloto concernientes a la presente investigación.

César Arenas Villanueva

DEDICATORIAS

A Dios

Por haberme dado la vida, guiarme en el camino correcto y por regalarme cada día para alcanzar mis metas y sueños.

A mis padres, Sonia y Eduardo

Que en todo momento me brindan su amor, comprensión y apoyo incondicional.

A mi hermano, Miguel Ángel

Por estar pendiente del desarrollo de la tesis y por motivarme a seguir adelante.

A mi hermanita, Stephanie Luana

Por su amor, inocencia y dulzura que llenan de alegría mi vida.

Diana De Los Santos Mendoza

A **César y Eloiza**, mis queridos padres, quienes con su esfuerzo, dedicación, consejos, ánimo y sobre todo por su gran amor han hecho de mí una buena persona, reflejo de su maravilloso ejemplo.

Y a mi gran amiga, confidente, amor de mi vida y esposita **Reinery**, quien estuvo y está siempre a mi lado apoyando cada decisión importante que tomo en la vida. Gracias por el "empujoncito" y el ánimo.

César Arenas Villanueva

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

La presente investigación aborda la gestión de la seguridad de la información desde una óptica tecnológica-moderna en relación al tratamiento de información para la toma de decisiones. Se analiza la relación entre la plataforma de gestión de la seguridad de la información desarrollada en código abierto OSSIM 5.3 de AlienVault- que es un SIEM que opera en tiempo real y recopila información sensible dentro de un entorno de red- junto con una guía de mejores prácticas reconocida y aplicada mundialmente, COBIT®, que está dirigida al control y supervisión de tecnologías de la información. El análisis e implementación de un nuevo modelo de gestión de la seguridad para la toma de decisiones en base a dicha relación, se desarrolla en el Área Telemática de la Universidad Nacional Pedro Ruiz Gallo en Lambayeque – Perú. Se describen las fases del desarrollo del modelo en base a los procesos habilitadores para cada objetivo de TI de acuerdo al caso de estudio. Los resultados obtenidos de la aplicación de este modelo, se miden y evalúan descriptivamente usando la norma ISO/IEC 15504, que permite la evaluación fiable, consistente y repetible de un proceso en el ámbito de la gestión de la empresa de TI basada en la evidencia.

PALABRAS CLAVES: activo, amenaza, confidencialidad, correlación, disponibilidad, integridad, política de seguridad, riesgo, SEM, SIEM.

ABSTRACT

This research addresses the management of information security from a technological-modern perspective in relation to the treatment of information for decision-making. The relationship between the information security management platform developed in open source OSSIM 5.3 of AlienVault - which is a SIEM that operates in real time and collects sensitive information within a network environment - together with a guide of better recognized and applied practices worldwide, COBIT®, which is directed to the control and supervision of information technologies. The analysis and implementation of a new security management model for decision making based on this relationship is developed in the Telematics Area of the Pedro Ruiz Gallo National University in Lambayeque, Peru. It describes the phases of the development of the model based on the enabling processes for each IT objective according to the case study. The results obtained from the application of this model are measured and evaluated descriptively using ISO/IEC 15504, which allows the reliable, consistent and repeatable evaluation of a process in the field of evidence-based IT management.

KEY WORDS: active, threat, confidentiality, correlation, availability, integrity, security policy, risk, SEM, SIEM.

INTRODUCCION

La presente investigación, comienza a desarrollarse a partir de la descripción de la realidad problemática donde se analiza la criticidad de la gestión de la seguridad de la información en toda organización la cual debería ser administrada de forma eficiente a través de alguna herramienta de software y soportada por un marco de referencia aceptado internacionalmente; esto finalmente deberá garantizar la toma acertada de decisiones reduciendo considerablemente los riesgos y amenazas presentes en la gestión de la información. Además, se describen los objetivos de esta tesis, que van desde la evaluación del impacto en la seguridad de la información hasta la implementación en tiempo real del modelo propuesto. Por otro lado, se justifica la importancia y las limitaciones presentadas en el desarrollo de esta propuesta.

En el segundo capítulo, se define el estado del arte, es decir todas las investigaciones relacionadas directamente con esta tesis y que sirvan como modelos de referencia para el desarrollo de la propuesta. Esta sección concluye con el glosario de términos relacionados y el marco legal que da soporte a la misma.

En el tercer capítulo, se detalla el desarrollo del modelo propuesto en 6 etapas, donde se incluyen: el análisis del caso de estudio, la identificación de los objetivos e indicadores según COBIT, el análisis de los procesos aplicables, el análisis de la herramienta Open Source como plataforma de la seguridad de la información, la integración OSSIM-COBIT y el diseño de fases de implementación en tiempo real.

En el cuarto capítulo, se expondrán los resultados obtenidos a partir de la implementación de la prueba piloto del modelo propuesto sobre el entorno de prueba seleccionado para el caso de estudio. Dichos resultados, se basan en la definición de los indicadores que miden el impacto del modelo sobre la toma de decisiones de acuerdo a lo establecido en el capítulo anterior. Y como parte final, se identifica el nivel actual de madurez para cada uno de los procesos habilitadores, determinando si el modelo de gestión cumple con la hipótesis propuesta en esta investigación. Para esto, se emplea el modelo de evaluación de procesos COBIT PAM, basada en la ISO/IEC 15504.

Y finalmente, el quinto capítulo recopila las conclusiones y recomendaciones a la que los investigadores llegaron después de la implementación de la prueba piloto, analizando el impacto del modelo sobre la toma de decisiones.

CAPÍTULO 1. EL PROBLEMA DE LA INVESTIGACION

1.1 Descripción de la realidad problemática

No hay duda de que la gestión de la seguridad de la información en las organizaciones de hoy tiene una relevancia que se acrecienta con el paso del tiempo.

Los Sistemas de Gestión de Seguridad de la Información, así como las redes de trabajo de dichas organizaciones, se están viendo afectadas por amenazas de seguridad, ataques y fraudes informáticos, problemas de sabotajes, virus informáticos y otro tipo de contingencias, que no hacen más que poner en riesgo los activos más importantes en una organización.

Según Herrera (2006), las empresas públicas y privadas están valorando cada día más la creciente importancia que representa mantener sistemas informáticos seguros, confiables y confidenciales, que eviten o prevengan la ocurrencia de errores u operaciones ilegales a partir de debilidades en los sistemas de control.

Por otro lado, existen muchas diferentes razones para violaciones de seguridad que se producen en las redes de computadoras como: errores en las políticas de seguridad, vulnerabilidades, configuraciones incorrectas, etc. Los ciberdelincuentes pueden utilizar las diferentes vulnerabilidades, los cuellos de botella de la configuración de la red y la política de seguridad para llevar a cabo diferentes estrategias de penetración. Estas estrategias están dirigidas a diferentes recursos de red e incluyen diversas cadenas de acciones de asalto. Estos mismos, pueden comprometer gradualmente los hosts de la red y realizar diferentes amenazas de seguridad (Kotenko & Chechulin, 2012).

Es por ello, que la relación entre las tecnologías de la información, la seguridad de las instalaciones, el personal y su "know how"[1], la protección de la información y los procesos de negocio es cada vez más estrecha. (Robles & Rodríguez de Roa, 2006).

De lo anterior se desprende que el aseguramiento de la información es la base sobre la que se construye la toma de decisiones de una organización. De no existir esta base, habría incertidumbre de que la información sobre la que se tome una decisión sea confiable, segura y

[1] El ***know-how*** tiene una directa relación con la experiencia, es decir la práctica prolongada que proporciona conocimiento o habilidad para hacer algo.

esté disponible cuando se necesite. Por otro lado, el administrador debe conocer el estado real de la red para poder identificar los puntos vulnerables tomando medidas, aplicando controles y herramientas que permitan implementar salvaguardas en los activos críticos de la organización.

Un aporte fundamental es el que proporciona Montesino Perurena, Baluja García & Porvén Rubier (2013) quienes informan que las pérdidas promedio de las instituciones, debido a incidentes de seguridad informática, fueron de 234 mil dólares en el año 2009. Teniendo en cuenta además el crecimiento exponencial de los programas malignos, los cuales aumentan por decenas de miles diariamente, las más de 8 mil nuevas vulnerabilidades de sistemas operativos y aplicaciones descubiertas anualmente y la organización cada vez más estructurada de los atacantes informáticos; es evidente la necesidad de garantizar la seguridad informática de las instituciones.

Por lo tanto, la seguridad de la información debe considerarse como un factor estratégico, crítico y necesario para procurar la continuidad del negocio (Nazareno Torrecillas, 2013).

Con el fin de detectar intrusiones y ataques, los administradores de sistemas y analistas de seguridad de la información hacen uso de herramientas, tales como IDS/IPS (Sistema de Detección de Intrusión/Prevención) y el análisis de logs (registros de eventos) de los servidores y dispositivos de red, en busca de cualquier evento significativo desde un punto de vista de seguridad (Shivhare & Savaridassan, 2015).

Sin embargo el hecho de que deban emplearse varias de ellas en conjunto para monitorear los diferentes frentes del sistema informático trae consigo varios problemas graves:

- Falta de uniformidad en el formato de los registros de actividad.
- Exceso de alertas. En sistemas grandes, o con actividad alta, el número de alertas que se genera en un determinado período de tiempo puede exceder la capacidad de trabajo del administrador.
- Manejo de falsos positivos. Dependiendo de la configuración de las herramientas, pueden reportarse como alertas de seguridad eventos que son, en realidad, parte del funcionamiento habitual del sistema

(Madrid Molina, y otros, 2008).

Ante este panorama, resulta necesario contar con una herramienta que permita unificar y centralizar la gestión de las alertas de seguridad. Para ello, una buena alternativa son los sistemas SIEM[2].

Las herramientas SIEM combinan eficazmente elementos de Gestión de la Seguridad de la Información (SIM) con Gestión de Eventos de Seguridad (SEM). Una de las principales características de estas soluciones es sus capacidades avanzadas de gestión de registros. La gestión de registros es el proceso de hacer frente a grandes volúmenes de datos que generan los mensajes de registro. Las cuestiones clave con la administración de registros tienden a ser el gran volumen de los datos de registro y la diversidad de los registros. Un producto SIEM normalmente se correlaciona, analiza y reporta información de una variedad de fuentes de datos, tales como los dispositivos de red, dispositivos de gestión de identidad, dispositivos de gestión de acceso y sistemas operativos. El resultado final es una visión integral de la seguridad de TI (Cerullo, Formicola, Iamiglio, & Sgaglione, 2014).

Puede entenderse, por tanto, que las herramientas de tipo SIEM favorecen en gran manera al administrador, pues le brinda información centralizada y con una visión integral de una gran variedad de fuentes de datos mediante la gestión y correlación de registros evitando por tanto la generación de falsos eventos, ayudando al administrador a tomar decisiones favorables respecto a la seguridad de la información.
Hay una serie de proveedores líderes en esta área, sobre todo HP-ArcSight, EMC RSA, e IBM (Q_1 Labs). HP-ArcSight es visto por la mayoría como el líder del mercado en este ámbito con su Enterprise Security Manager (ESM), que funciona como una suite integrada de productos para la recolección, análisis y evaluación de la información de seguridad y riesgo (Cerullo, Formicola, Iamiglio, & Sgaglione, 2014).

Sin embargo, los sistemas SIEM existentes tienen múltiples limitaciones en el uso de redes e infraestructuras heterogéneas. Dentro de las limitaciones más importantes se mencionan: baja escalabilidad, restricciones sobre las funciones reales de la infraestructura, incapacidad de una adecuada interpretación de incidentes y eventos en los distintos niveles y la imposibilidad de proporcionar una alta fiabilidad y tolerancia a fallos en entornos distribuidos para capturar datos de eventos. (Kotenko, Polubelova, Chechulin, & Saenko, 2013).

[2] SIEM por sus siglas en inglés: **Security Information and Event Management** (Seguridad de la información y Gestión de eventos).

A pesar de ello, hay una creciente necesidad de utilizar la tecnología SIEM para proteger a gran escala la infraestructura de las Tecnologías de la Información (TI), tomando en cuenta aún los más estrictos requisitos de seguridad. (Vianello, y otros, 2013).

Se traduce, por tanto, que en la actualidad el mercado de herramientas SIEM presenta una creciente tendencia debido a la gran cantidad de proveedores que desarrollan este tipo de soluciones y a pesar de contar con algunas limitaciones, son las únicas herramientas que brindan al administrador información en tiempo real de la red con el objetivo de tomar decisiones acertadas y asegurar en gran escala la infraestructura de las tecnologías de la información.

De acuerdo al último reporte de ESET, con respecto a la seguridad, tras el análisis de opiniones de más de 3900 ejecutivos que trabajan en seguridad en diversas organizaciones de Latinoamérica se demostró que a un ciberdelincuente no le interesa el tamaño de la organización siempre y cuando pueda obtener algún tipo de ganancia económica. Por otro lado, cada organización se enfrenta a los retos de mantener costos bajos y a la vez conseguir el control de la seguridad y disponibilidad de los sistemas que necesita para mantenerse a la vanguardia (Eset Latinoamérica, 2015).

Se concluye entonces, que no importa el tamaño de la organización para implementar soluciones confiables que gestionen la seguridad y garanticen la continuidad de la organización. Una alternativa tentativa, para este caso, serían los Sistemas Open Source.

Un análisis desde la perspectiva de Open Source

Las soluciones SIEM prometen brindar integraciones entre lo complejo, pero a menudo introducen demasiados costos por muy poco valor para las organizaciones. Por lo que estas organizaciones pueden decidir por SIEM de código abierto (Shivhare & Savaridassan, 2015).

Una de las herramientas de gestión de código abierto más populares en la actualidad es OSSIM[3] (Asociacion Colombiana de Facultades de ingeniería, 2008).

OSSIM por su parte, tiene ciertas ventajas sobre muchos otros SIEM propietarios como:

- Es gratuito.
- Es compatible con la mayoría de los dispositivos actuales.
- Mantiene actualizado al sistema sin costo alguno.
- Es adaptable al entorno donde opere

(Baluja García, Caro Reina, & Cancio Bello, 2012).

[3] Por sus siglas en inglés: **Open Source Security Information Management** (Gestión de la seguridad de la información de código abierto) cuyo proveedor es AlienVault Inc.

Además, cuenta con algunas características sobresalientes como:
Tiene la capacidad de consolidar alertas de una gran cantidad de sistemas de seguridad basados en código abierto, y es altamente configurable, de tal manera que permite procesar información de todo tipo de programas y dispositivos de seguridad (Asociacion Colombiana de Facultades de ingeniería, 2008).

Recolecta y uniformiza los eventos de los diferentes sistemas, correlaciona aquellos que ocurren en el sistema bajo análisis, con el fin de minimizar el número de alarmas que el administrador recibe y eliminar falsos positivos (Madrid Molina, y otros, 2008).

Permite obtener una visión general del estado, a nivel de seguridad, en el que se encuentra un sistema. Además, en base a la correlación de la información almacenada, hace de ella una potente herramienta de prevención de intrusiones en los sistemas (Parra Truyol, 2013).

Se deja claro, entonces, que la consola OSSIM presta un invaluable servicio al administrador de un sistema informático, brindándole información útil para la toma de decisiones en el campo de la seguridad informática (Madrid Molina, y otros, 2008).

Finalmente, OSSIM posibilita aumentar la efectividad de los controles implementados y disminuir la complejidad de la gestión de la seguridad de la información (Montesino Perurena, Baluja García, & Porvén Rubier, 2013).

Sobre la última referencia, se destaca la necesidad de implementar controles, indicadores y procesos que puedan ser soportados eficazmente por OSSIM con el fin de gestionar la información que finalmente llevará al administrador a tomar decisiones acertadas, a nivel gerencial, en cuando a la seguridad de la infraestructura de red.

Pensando en lo anterior se propone COBIT 5.0 como marco referencial.

Influencia de COBIT 5.0 en la seguridad de la Información

De acuerdo a lo mencionado por Sánchez Peña, Fernández Vicente, & Moratilla Ocaña (2013) COBIT es un conjunto de mejores prácticas (framework) para la gestión de tecnología de la información creada por Information Systems Audit and Control Association (ISACA) y el ITGI. En 1992 COBIT fue lanzado…. Más tarde se añadieron Directrices para su Gestión y COBIT se convirtió en un marco internacionalmente aceptado para la gobernanza y el control de TI. COBIT proporciona a los administradores, auditores y usuarios de TI con un conjunto de

medidas generalmente aceptadas, indicadores, procesos y mejores prácticas para ayudarles a maximizar los beneficios que se derivan del uso de tecnologías de la información y el desarrollo apropiado del gobierno y control de TI para una empresa.

El marco de referencia COBIT 5, representa un marco completo para la definición, implementación y supervisión de procedimientos de mejora continua y buenas prácticas relacionadas con la gestión de la información para cualquier tipo de empresa y su tecnología de la información relacionada (Gualsaqui, 2013).

Con la cascada de objetivos de COBIT 5, cada proceso habilitador tiene un componente que se adapta a la necesidad y los procesos seleccionados de la empresa, los cuales se reducen al realizar el análisis de acuerdo al enfoque seleccionado, que puede variar de acuerdo a la realidad de la organización, sus procesos y prioridades (Lepage Hoces, 2014).

Por otro lado, un modelo basado en COBIT 5 brindará a la institución un valor agregado por el lado de la gestión tecnológica, pues se garantiza el alineamiento estratégico y la entrega de beneficios a los stakeholders siguiendo actividades y estableciendo roles y responsabilidades de acuerdo a un enfoque identificado y que se adapte a lo que la empresa pueda alcanzar en un determinado espacio de tiempo (Lepage Hoces, 2014).

Sin embargo, para gobernar una empresa totalmente es indispensable la integración de COBIT e ISO 27001. Implementar sólo COBIT serviría para identificar y dirigir las funciones de seguridad de la información. Sin embargo, estándares como ISO 27001, describen de manera más completa una manera de implementar lo que se establece en COBIT. Por lo tanto, con el fin de poner en práctica la gobernanza de TI en las empresas, es necesario que se considere normas como la ISO 27001 (Mataracioglu & Ozkan, 2011).

Esto no es un inconveniente para la herramienta SIEM seleccionada, pues OSSIM de AlienVault proporciona un módulo de cumplimiento de normativas dentro de las cuales tiene implementados algunos controles esenciales de la ISO 27001, por lo que integrar el marco de referencia COBIT 5 con OSSIM proporcionaría un sistema de gestión de seguridad de la información más completo y alineado con los objetivos de seguridad deseados por la organización.

Con respecto a COBIT 5, como marco de referencia a aplicar, una entidad bancaria de Medio Oriente obtuvo los siguientes beneficios como consecuencia de una iniciativa por mejorar la seguridad de la información (COBIT FOCUS: Volumen 1, enero de 2014):

- Mejorar la integración de la seguridad de la información dentro de la organización.
- Comunicar decisiones vinculadas al riesgo y crear conciencia sobre los riesgos.
- Mejorar la prevención, detección y recuperación.
- Reducir (el impacto de) los incidentes vinculados a la seguridad de la información.
- Aumentar el soporte relacionado con la innovación y la competitividad.
- Mejorar la gestión de costos relacionados con la función de seguridad de la información.
- Adquirir un entendimiento más profundo sobre la seguridad de la información.

Como conclusión del contexto descrito podemos señalar que la gestión de la seguridad de la información es un factor crítico en toda organización, independientemente de su tamaño, y que a su vez debería ser administrada de forma eficiente a través de la integración de algunas herramientas de seguridad como lo son los sistemas SIEM y sobre todo soportadas por marcos de referencia aceptados y aplicados internacionalmente, como COBIT, que garanticen a la organización la seguridad de tomar decisiones acertadas y de cumplir con los objetivos propuestos.

Situación problemática en el campo de estudio

La Universidad Nacional Pedro Ruiz Gallo cuenta con un órgano de apoyo, encargado de gestionar los sistemas informáticos académicos, investigativos y de administración. Esta es la OGSI (Oficina General de Sistemas Informáticos), que dentro de su jefatura tiene a cargo al **Área de Administración de Red**, la cual se divide en:

- Área de Conectividad, Redes y Soporte
- Área de Seguridad, Servidores y Base de Datos

Las principales funciones de la OGSI son las siguientes:

- Diseñar, planificar, ejecutar, actualizar y supervisar los procesos informáticos académicos, administrativos y de investigación de la Universidad.
- Desarrollar, actualizar y mantener el software y el hardware institucional.
- Asesorar a las diferentes dependencias en asuntos de sistemas informáticos y de comunicación.
- Apoyar las actividades de actualización institucional en el avance de las tecnologías de información y la comunicación (TICs).
- Prestar servicios a terceros, funcionando en este caso como un órgano generador de ingresos propios.

Por otro lado, dentro sus principales servicios figuran:

- Servidor Web
- Servidor de Correo
- Servidor FTP
- Servidor de archivos
- SIAF
- GESTAC
- SIGA
- Telefonía IP
- Acceso a Internet, etc.

Como se puede notar, la diversidad de servicios brindados sumado con el crecimiento continuo de la infraestructura tecnológica en la universidad hace que la gestión de la seguridad de la información sea compleja y muchas veces difícil de monitorear en su totalidad, trayendo como consecuencia que las decisiones que se tomen a nivel gerencial, no se realicen de forma acertada y eficiente teniendo en cuenta los objetivos propuestos a largo plazo.

Aunque existen infinidad de herramientas de seguridad que se pueden implementar, actualmente la red Telemática de la Universidad Nacional Pedro Ruiz Gallo cuenta con algunas de ellas, pero estas muestran formatos de reportería y archivos completamente descentralizados y la toma de decisiones con respecto a la seguridad de la información afecta considerablemente a los principales procesos que brinda como: matrícula, registro de notas, admisión, etc.

Por ello, proponemos un modelo procedimental de implementación e integración de la herramienta OSSIM (de AlienVault) y el marco de referencia COBIT 5 (de ISACA) alineando los objetivos de control con los objetivos de seguridad perseguidos por la universidad.

Actualmente no existe ninguna investigación sobre dicha solución y los beneficios para las organizaciones que la implementen, en nuestro caso ayudarán a los encargados de la gestión de la red a la correcta toma de decisiones de TI garantizando así la continuidad y el buen desempeño de los procesos principales de la universidad; y a su vez servirá de base para futuras investigaciones.

1.2 Descripción del proyecto

El presente proyecto de tesis se inscribe en la línea de investigación de Tecnologías de la Información y Comunicación perteneciente al área Desarrollo de Tecnologías e Innovación, implementándose el Sistema de Gestión de Seguridad Open Source (OSSIM de AlienVault) y

utilizando como marco referencial de buenas prácticas COBIT 5 con la finalidad de gestionar la información crítica de los principales procesos, de tal manera que la información proporcionada por esta integración (OSSIM - COBIT) ayude a los encargados de la gestión, mediante cuadros de mando, a la correcta toma de decisiones de TI de acuerdo a las políticas y objetivos establecidos.

1.3 Objetivo general

Evaluar el impacto que produce en la toma de decisiones de TI en la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo el uso de una plataforma de Gestión de Seguridad Open Source bajo un entorno de objetivos de control según el enfoque de COBIT 5.

1.4 Objetivos específicos

- Definir el diseño, arquitectura y dimensionamiento adecuado para la plataforma de gestión de Seguridad que integre módulos de recolección de la información para la toma de decisiones en la Gestión de TI.
- Implementar la plataforma OSSIM para identificar, clasificar y evaluar los eventos de seguridad de la red provenientes de herramientas integradas en un sistema con una única consola de administración.
- Definir políticas de valoración de riesgos para la generación de alertas, dada una contextualización de la arquitectura de red informática que requiera gestionarse tomando decisiones.
- Implementar módulos de reportería como informes de eventos de seguridad en la red monitorizada.
- Identificar los procesos de COBIT que serán evaluados a partir de la descripción de proceso de TI que actualmente la Red Telemática brinda y desarrolla.
- Determinar los niveles de capacidad específicos y genéricos de cada proceso de TI evaluado con la finalidad de determinar su nivel de madurez mediante la ISO/IEC 15504.
- Evaluar los niveles de efectividad del diseño del modelo de gestión de la seguridad propuesta mediante la ISO/IEC 15504.

1.5 Formulación de la pregunta de investigación

¿Cuál será el impacto del uso de una plataforma de Gestión de Seguridad Open Source bajo un entorno de objetivos de control según el enfoque de COBIT 5, en la toma de decisiones de TI de la red Telemática de la Universidad Nacional Pedro Ruiz Gallo?

1.6 Justificación e importancia

Existen 4 perspectivas que definen la justificación e importancia de este proyecto de tesis:

En lo tecnológico, la integración de la plataforma OSSIM y el marco de referencia COBIT lograrán construir una potente herramienta de análisis y gestión de la información, a partir de toda la infraestructura de red de la universidad, logrando centralizarla y convertirla en un conjunto de acciones que se tomarán de acuerdo a las políticas y objetivos perseguidos.

En lo Social, la propuesta de integración proporcionará al administrador de red (como responsable de la seguridad de la información) contar con una valiosa herramienta que mejorará considerablemente tanto su rendimiento como sus procedimientos. Sin embargo, los más beneficiados serían los usuarios finales, pues tendrían la satisfacción de contar con una herramienta útil y eficaz en la reducción de tiempos de espera ante incidentes mayores, disminución de caídas de servicios, protección y seguridad de su información, etc.

Con respecto a lo económico, esta propuesta de integración se implementa sobre una plataforma de software libre que reduce de forma aceptable, los costos de instalación, capacitación y sobre todo de recuperación ante posibles caídas.

Y finalmente este proyecto se justicia científicamente ya que aporta a la ciencia una innovadora propuesta para la gestión de la seguridad de la información mediante la integración de OSSIM y COBIT, así como, también ayudará y orientará investigaciones posteriores sobre consideraciones que se deben tener presente para conseguir resultados similares en contextos diferentes.

1.7 Alcances y limitaciones

Como parte de la investigación, se tomarán en cuenta los siguientes puntos:

- Debido a la complejidad de la infraestructura de la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo, se procederá a seleccionar un tramo de red oportuno que cumpla con los requisitos básicos de la propuesta definida y que a través de una prueba piloto se generalicen los resultados obtenidos al final del experimento.
- La información vital para la aplicación de la presente investigación, en cuanto a la implementación de la plataforma OSSIM bajo los objetivos de control de COBIT 5, es muy escasa o nula en el ámbito aplicado de la universidad, razón por la cual nos basaremos en la información proporcionada por el administrador de la red.
- Inicialmente, se propuso un modelo cuasi-experimental para la evaluación de los resultados, teniendo en cuenta un antes y un después de la aplicación del experimento; sin embargo, después de un análisis minucioso del problema, vimos la necesidad de

evaluar nuestro modelo a través de un análisis descriptivo no experimental que nos permitirá determinar el grado de aceptación a través de los resultados y beneficios obtenidos de implementar la propuesta a nivel global dentro del campo de estudio y validándola mediante el uso de una norma ISO/IEC.

CAPÍTULO 2. MARCO TEÓRICO Y REVISIÓN DEL ESTADO DEL ARTE

2.1 Estado del arte

Actualmente, no existen propuestas o diseños similares en otras investigaciones referentes a la relación de la herramienta OSSIM bajo el marco de referencia COBIT 5.0 para la gestión de la seguridad de la información, razón por la que se considera a este modelo propuesto como un *nuevo modelo*. Sin embargo, existen investigaciones que abordan el tema desde una perspectiva diferente con resultados similares a los que se pretende llegar mediante la implementación del modelo relacional. A continuación, algunas investigaciones desarrolladas durante los últimos años y el respectivo aporte al presente proyecto.

TITULO	**INTEGRACIÓN DE OSSIM Y UNTANGLE**
UNIVERSIDAD	UNIVERSIDAD ICESI (SANTIAGO DE CALI)
FECHA	2010
AUTOR(ES)	Marcofi Andretti Torres Manrique, Diego Alejandro Villegas Oliveros
RESUMEN	El presente proyecto consiste en integrar eventos de monitorización generados por aplicaciones de UNTANGLE a la arquitectura tipo SIEM provista por la consola de seguridad de OSSIM, para lograr de esta manera la consecución de un sistema de gestión y control centralizado y eficiente.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	Esta investigación permite visualizar la capacidad de integración que posee la plataforma OSSIM con otras herramientas del tipo Open Source como UTANGLE así como los resultados obtenidos. También, muestra la necesidad de complementar esta integración con algún marco de referencia para garantizar aún más su porcentaje de fiabilidad.

TITULO	**CENTRO DE GESTIÓN DE RIESGOS PARA MONITOREO DE REDES, EN LA FACULTAD DE INGENIERÍA CIENCIAS FÍSICAS Y MATEMÁTICA**
UNIVERSIDAD	UNIVERSIDAD CENTRAL DEL ECUADOR
FECHA	2012
AUTOR(ES)	Alexandra Mireya Espinosa Criollo, Freddy Marcelino Roldán González y Dennis Ricardo Collaguazo Lapo.
RESUMEN	En esta tesis se desarrollaron plugins de monitoreo de red acoplados al framework de Open Source SIEM (OSSIM), que permita detectar problemas ofreciendo información confiable y oportuna para reaccionar ante eventos que se generan en la red, a través de herramientas de Software libre GPL bajo una plataforma Linux, con la aplicación de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Magerit v2.0) en la Facultad de Ingeniería, Ciencias Físicas y Matemática.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	Esta investigación, muestra la posibilidad de integrar el framework OSSIM con una metodología de análisis y gestión de riesgos reconocida como es MAGERIT v2.0 ofreciendo finalmente un sistema de monitoreo que centralice la información filtrada y permita tomar decisiones oportunas en casos concretos. Por otro lado, detalla la configuración y operatividad de algunas aplicaciones dedicadas de OSSIM.

TITULO	**IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN Y ADMINISTRACIÓN DE SEGURIDAD PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA UNIVERSIDAD CENTRAL DEL ECUADOR (DTIC)**
UNIVERSIDAD	UNIVERSIDAD CENTRAL DEL ECUADOR
FECHA	2012

AUTOR(ES)	Darwin Alfredo Chanaluisa Viera, Andrés Leonardo Meza Castillo y Jessica Valeria Tasipanta Chicaiza
RESUMEN	Este proyecto está enfocado como una herramienta de apoyo para la Universidad Central del Ecuador, cuya expectativa a cumplirse es la de proporcionar un sistema que permita obtener una visibilidad de todos los eventos que ocurran en tiempo real, de tal forma que se garantice una red constantemente supervisada, una correlación de eventos y el procesamiento de la información permitiendo aumentar la capacidad de detección, priorizar los eventos según el contexto en que se producen, y monitorizar el estado de seguridad de la red
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	Se detallan las configuraciones necesarias para implementar una plataforma OSSIM que gestione la seguridad de la información en una Universidad Pública. Además, se muestran los beneficios obtenidos en su implementación así como la configuración y seguimiento de las políticas de seguridad a alcanzar

TITULO	**LABORATORIO DE MALWARE: AUTOMATIZACIÓN DE LA GESTIÓN DE RECURSOS VIRTUALES PARA EL ESTUDIO DE MALWARE**
UNIVERSIDAD	UNIVERSIDAD CARLOS III DE MADRID
FECHA	MAYO 2013
AUTOR(ES)	Antonio Parra Truyol
RESUMEN	En este proyecto se han diseñado unos laboratorios donde poder realizar un estudio del malware. En los mismos se podrán ejecutar experimentos en entornos aislados que servirán para poder analizar dicho comportamiento. Se proporciona también la habilidad de crear una infinidad de entornos de red con diferentes sistemas operativos y

	aplicaciones que facilitarán el estudio del mismo.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	La citada tesis, proporciona el análisis e implementación de algunas herramientas de monitorización y detección de software malintencionado instalado sobre plataforma Open Source con resultados efectivos. Además, muestra configuraciones de herramientas de seguridad en plataformas SIEM (OSSIM).

TITULO	**DESARROLLO DEL MARCO DE REFERENCIA COBIT 5.0 PARA LA GESTIÓN DEL ÁREA DE TI DE LA EMPRESA BLUE CARD**
UNIVERSIDAD	PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
FECHA	2013
AUTOR(ES)	Juan Carlos Gualsaquí Vivar
RESUMEN	COBIT 5.0 brinda un marco de trabajo integro que ayuda a las organizaciones a lograr sus objetivos basados en la gestión de Gobierno y de las TI corporativas, creando valores óptimos desde TI generando beneficios y optimizando el riesgo y uso de recursos. Adicionalmente, COBIT 5.0 permite una gestión completa de las TI involucrando a la organización por completo, es decir permitiendo la interacción de todas las unidades funcionales y considerando sus intereses relacionados con TI.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	La relación existente, se sitúa en la manera sobre como adecuar o relacionar los objetivos de control proporcionados por COBIT y los objetivos de seguridad que se pretenden alcanzar en la organización. El éxito obtenido en la implementación de este marco referencial proporciona una visión general de lo que es posible lograr durante el desarrollo de nuestro proyecto.

TITULO	**DISEÑO DE UN MODELO DE GOBIERNO DE TI CON ENFOQUE DE SEGURIDAD DE INFORMACIÓN PARA EMPRESAS PRESTADOREAS DE SERVICIOS DE SALUD BAJO LA ÓPTICA DE COBIT 5.0**
UNIVERSIDAD	PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU
FECHA	ABRIL 2014
AUTOR(ES)	Diana Estefanía Legape Hoces
RESUMEN	Se plantea una solución integrada que brinde un enfoque estratégico y comprometa a la Alta Dirección para que participe del cambio que conlleve a que las empresas logren sus objetivos de la mano de la tecnología correctamente gestionada. Para el proyecto se empleará un marco de negocio mundialmente reconocido, COBIT 5.0 que brinda buenas prácticas para implementar esta solución dentro de cualquier organización según sea el contexto
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	Esta investigación, proporciona el desarrollo de un modelo de gestión de seguridad de la información basado en el marco referencial COBIT 5.0 garantizando el alineamiento estratégico y la correspondencia con los objetivos de negocio. Por otro lado, se analiza la importancia del empleo de cuadros de mando como herramientas de medición de los objetivos.

TITULO	**ANÁLISIS PARA LA INTEGRACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN (SGSI) ISO-27001 UTILIZANDO OSSIM PARA EMPRESA INDUSTRIAL**
UNIVERSIDAD	UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL
FECHA	2014

AUTOR(ES)	Claudia Yagual Del Valle, Leslie Chilán Rodríguez
RESUMEN	El presente trabajo se basa en la identificación de amenazas y vulnerabilidades hacia los activos más críticos de una empresa industrial para los cuales, ya sabiendo que tan vulnerables pueden materializarse, se recomendarán los controles adecuados basándose en la norma ISO 27001, de tal manera que la empresa pueda minimizar sus riesgos. Además, se deja un plan de contingencias sobre los riesgos a las que se encuentra expuesto el centro de cómputo y servicios informáticos de la empresa. También se usó el método de investigación de riesgos llamado "Magerit", la cual nos guio con la realización de una matriz de evaluación y riesgos para cada proceso de la empresa, determinando que tan expuesto se encontraba un activo hacia alguna vulnerabilidad
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	El uso de OSSIM, como herramienta libre y centralizada para obtener información completa y selecta de los diferentes eventos reportados, es la principal relación con la presente investigación. Por otro lado, proporciona un análisis de resultados óptimos al utilizar uno de sus componentes (OpenVas) como detector de vulnerabilidades.

TITULO	**PROPUESTA DE MEJORAMIENTO DE LA HERRAMIENTA OSSIM SIEM (OPEN SOURCE), PARA OBTENER LOS NIVELES ÓPTIMOS DE GESTIÓN EN LA ADMINISTRACIÓN DE LA SEGURIDAD, EN UNA RED IMPLEMENTADA EN CLOUD COMPUTING**
UNIVERSIDAD	UNIVERSIDAD POLITÉCNICA SALESIANA
FECHA	ABRIL 2015
AUTOR(ES)	Alexis Fernando Balarezo Chávez, Diego Xavier Poveda Pilatasig

RESUMEN	Trata sobre la optimización de un sistema OSSIM, el cual se implementó en la Cloud Computing, tecnología en crecimiento a nivel empresarial, motivo por el cual se busca integrar un sistema de monitoreo que preste confiabilidad a la red y a sus activos. Entre las herramientas tratadas se encuentran el detector OSSEC, teniendo un funcionamiento basado en logs generados por los equipos que forman parte de la red, los monitores NMAP y NAGIOS los cuales funcionan basados en respuestas a solicitudes realizadas y herramientas.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	Este proyecto está enfocado al mejoramiento de la herramienta OSSIM, que al poseer las funcionalidades de un SIEM, permite integrar la información en tiempo real detectando anomalías en una red de servicios. Analiza las funciones de dos módulos integrados de OSSIM: NAGIOS Y NMAP mostrando los beneficios en el logro de las políticas de seguridad perseguidas.

2.2 Fundamento Teórico

2.2.1 Conceptos directamente relacionados

2.2.1.1 La seguridad de la Información y su importancia actual

El cambio social producido por Internet y la rapidez en el intercambio de información, ha producido que las empresas empiecen a tomar conciencia del valor que tiene la información para sus organizaciones y se preocupen por proteger sus datos. Con la creciente dependencia que la sociedad de la información tiene de las TIC, la necesidad de proteger la información está creciendo enormemente (Sanchez, Luis & Piattini, Mario, 2015).

Hoy en día son múltiples los riesgos asociados a que los equipos y sistemas de información y comunicaciones no cuenten con controles de seguridad. Las amenazas en las TIC son globales, y están repartidas en distintos niveles de criticidad según sea la orientación y el ámbito de su utilización. Preocupante es para grandes, medianas y pequeñas organizaciones el espionaje industrial, los ladrones de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información.

Cada día, se desarrollan nuevos métodos que afectan a la seguridad de la información de las organizaciones, es por ello la necesidad de una estrategia completa de seguridad, de manera de prevenir fugas y fallas en los sistemas. A lo antes expuesto se suman vulnerabilidades internas que son un factor de riesgo no menor, y por lo tanto, existe alta probabilidad de pérdida de dinero y repercusiones en la confiabilidad por parte de los usuarios, clientes y socios de negocios (Burgos, Jose & Campos, Pedro, 2013).
La seguridad de TI o Seguridad Informática se ocupa de la salvaguarda de la tecnología y de la información contenida en ella, mientras que la seguridad de información se ocupa de los riesgos, beneficios y procesos involucrados en la manipulación de la información dentro de la organización, independientemente de cómo sea creada, manejada, transportada, o almacenada (Espinoza, 2013).

Además, se encarga de minimizar los riesgos asociados con el acceso y utilización de los sistemas de forma malintencionada, esto implica, que se debe tener una visión general de los bienes a los cuales se necesita proteger, los cuales deben ser analizados para poder reducir al mínimo los riegos, con esto se logra tener un control en la utilización de medidas preventivas y correctivas en la seguridad (Balarezo & Poveda, 2015).

Por otro lado, se encarga de la preservación de la confidencialidad, integridad y disponibilidad de la información. Esto se logra mediante la implantación de un grupo de controles que incluyen políticas, procedimientos, estructuras organizativas y sistemas de hardware y software. La seguridad de la información no es un estado que se alcanza en determinado instante de tiempo y permanece invariable, sino que es un proceso continuo que necesita ser gestionado (Montesino, Baluja, & Porvén, 2013).

La seguridad no es un producto, sino un proceso continuo que debe ser controlado, gestionado y monitorizado. Como tal la seguridad tiene un objetivo que es garantizar el buen funcionamiento de los procesos de negocio (Sanchez, Luis & Piattini, Mario, 2015).

Asegurar que las reglas de uso de los sistemas de información cumplan con las políticas de seguridad de información, garantiza una buena gestión de seguridad en una organización.

Los aspectos a tomar en cuenta incluyen la identificación de la importancia de los activos de información, la necesidad de seguridad, definición de la sensibilidad y criticidad de los mismos, su confidencialidad, integridad y disponibilidad (Villena, 2006).

Los controles deben estar construidos en base a áreas (procesos) y objetivos de control de los cuales se deben desprender las actividades y finalmente los controles en sí (Burgos, Jose & Campos, Pedro, 2013).

2.2.1.2 Incidentes, amenazas y evaluación de vulnerabilidades

La identificación de un incidente no es una ciencia exacta: existen metodologías que pueden usarse para identificar los incidentes, pero cuando algo ocurre sólo una vez es a menudo complicado identificar el evento como una deficiencia de seguridad o problema de sistema.

Se define un incidente como un evento que causa algún nivel de interrupción a los procesos normales de negocio, y que es precipitado generalmente por un individuo, de manera maliciosa o accidental.
Dada esta definición, algunos incidentes que pueden categorizarse como de seguridad son:

- Intrusiones en las computadoras o intentos de intrusión.
- Ataques de denegación de servicio.
- Acceso a información de manera no autorizada.

Algunos incidentes son muy obvios. Pero desafortunadamente no todos los incidentes son fácilmente identificables. Por ello usualmente existen indicios característicos cuando un verdadero incidente de seguridad ha ocurrido. Estos indicios pueden encontrarse en:

- Archivos de Log (de firewalls, ruteadores, sistemas, IDS 17, etc.).
- Tráfico de red.
- Configuraciones del sistema.

Los sistemas en sí son a menudo la mejor fuente para obtener información acerca de un potencial incidente de seguridad. Es complicado poder ocultar por completo la evidencia de una intrusión de un sistema comprometido. El atacante usualmente hará cambios al sistema que de alguna manera puede ser detectado (Villena, 2006).

La información es vulnerable a una serie de amenazas, las cuales pueden producir una gran cantidad de pérdidas que de una u otra manera afecta significativamente a una entidad.

En muchos casos las amenazas pueden producir simples errores en las aplicaciones de gestión que generan un fallo en la integridad de los datos y por medio de estos errores menos significativos se puede llegar a tener un fallo principal en el sistema afectando la disponibilidad.

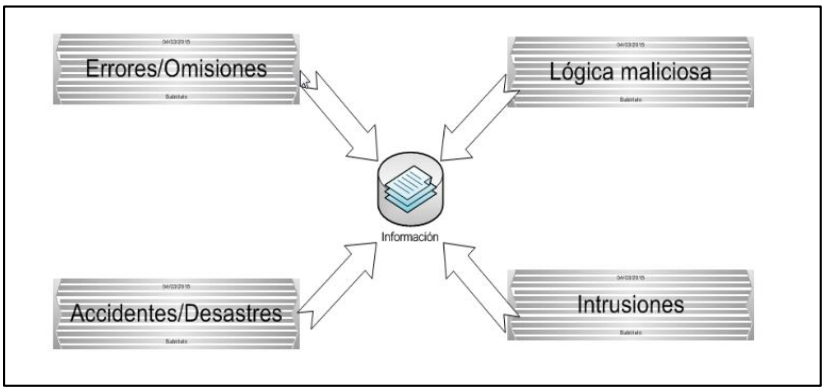


Figura N° 1. Tipos de amenazas
Fuente: (Balarezo & Poveda, 2015).

Las amenazas se clasifican en cuatro grandes grupos dependiendo del nivel y propósito de afectación: interrupción, intercepción, modificación y fabricación.

Tabla N° 1: Clasificación de las amenazas

PROPÓSITO	DESCRIPCIÓN
Interrupción	Produce que un objeto se pierda y que sea inutilizable.
Intercepción	Interceptar información la cual está siendo transmitida.
Modificación	Acceso no autorizado el cual permite modificar un objeto del sistema.
Fabricación	Objeto que sea difícil de distinguir entre el original.

Fuente: Amenazas según el propósito de afectación (Balarezo & Poveda, 2015).

2.2.1.3 Elementos considerados amenazas

En la actualidad, existe una gran cantidad de elementos que son considerados un peligro y amenazan a la seguridad de la información a continuación se detallan los principales:

Personas: La mayoría de ataques son producidos por personas que intencionalmente o involuntariamente causan grandes pérdidas y producen fallos en el sistema. Se pueden dividir en dos grupos a esta clase de amenazas como atacantes activos y pasivos. Los pasivos son aquellos que por curiosidad o investigación, ingresan a los sistemas pero no los modifican, al contrario de los activos, que son atacantes que buscan dañar el objeto alcanzado.

Amenazas: Lógicas: Se considera a todo software que pueda dañar lógicamente al sistema y se lo conoce como malware.

Software incorrecto: Las amenazas más frecuentes y conocidas son las generadas por fallas involuntarias de los programadores al desarrollar el sistema, se produce por alguna línea de código que se encuentre incompleta que al realizar alguna determinada tarea produzca algún tipo de bucle.
(Balarezo & Poveda, 2015)

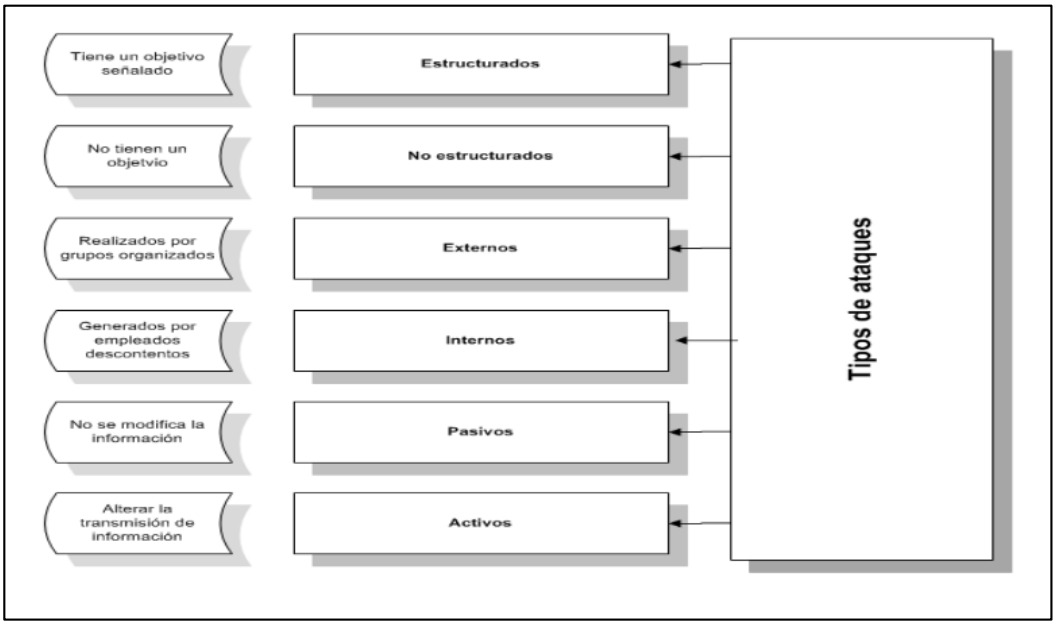


Figura N° 2. Tipos de ataques a la seguridad de la información
Fuente: (Balarezo & Poveda, 2015).

Según Villena (2006), con respecto a la evaluación de vulnerabilidades, son útiles para determinar las debilidades en un sistema, pero es importante tener en mente que la mayoría de veces existirá una amenaza que explote una vulnerabilidad y causará un impacto.

La evaluación de vulnerabilidades típicamente incluye:

- Revisión de controles de seguridad para determinar si existen vulnerabilidades.
- Prueba de controles en curso para determinar su efectividad.
- Pruebas de penetración para localizar vulnerabilidades.
- Desarrollo de recomendaciones para reducir las vulnerabilidades y mejorar la seguridad.
- Seguimiento de los progresos.
- Debilidades en los sistemas operativos.
- Deficiencias en las redes.
- Aplicaciones (incluyendo bases de datos, aplicaciones web, correo, etc.).

2.2.1.4 Principios Clave y mecanismos de protección

Para la correcta administración de la seguridad de la información se debe establecer y mantener acciones que busquen cumplir con los tres requerimientos de mayor importancia para la información, estos son:

Confidencialidad: busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización.

Integridad: busca asegurar que no se realicen modificación por personas no autorizadas a los datos o procesos, que no se realicen modificaciones no autorizadas por parte del personal autorizado a los datos y procesos y que los datos sean consistentes tanto interna como externamente.

Disponibilidad: busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado (Burgos, Jose & Campos, Pedro, 2013)**.**

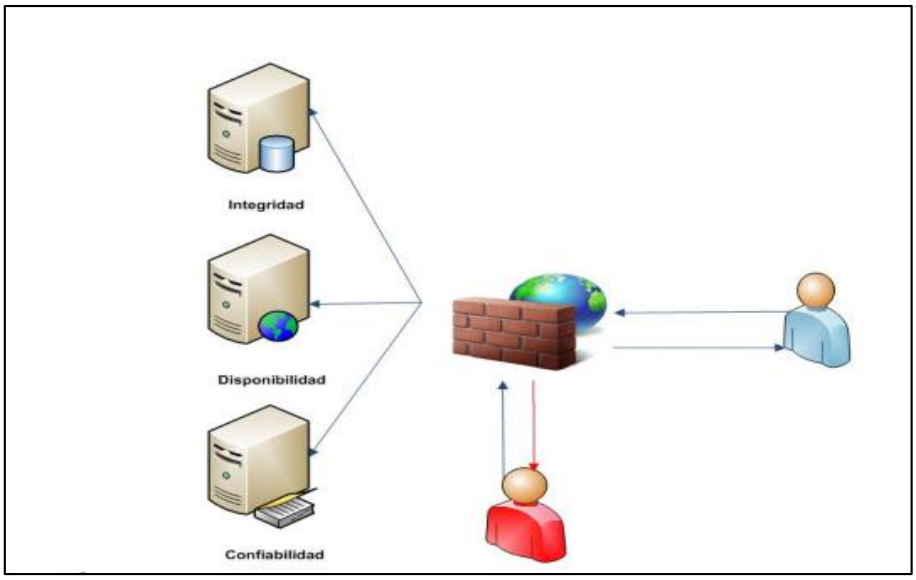


Figura N° 3. Principios clave de la seguridad de la información
Fuente: (Chanaluisa Viera, Meza Castillo, & Tasipanta Chicaiza, 2012)

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático.

Existen muchos y variados mecanismos de seguridad informática. Su selección depende del tipo de sistema, de su función y de los factores de riesgo que lo amenazan. Entre ellos tenemos:

- **Preventivos**: Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.
- **Detectores**: Actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.
- **Correctivos**: Actúan luego de ocurrido el hecho y su función es corregir las consecuencias.

(Chanaluisa, Darwin & Meza, Andres & Tasipanta, Jessica, 2012).

En definitiva, un buen sistema de seguridad debe proteger los sistemas vulnerables ante el posible acceso físico o remoto de intrusos no autorizados. Evidentemente, el nivel de seguridad establecido tendrá que ser consecuente con un análisis previo de los riesgos, considerando el impacto de dicho acceso no deseado contra las posibilidades de que este se produzca (Ferrer & Fernández, 2012).

2.2.1.5 Prácticas de seguridad de la Información

Se demandan muchos productos, sistemas y servicios para gestionar y mantener esa información, y no es suficiente con realizar unos controles de seguridad superficiales. Además, es necesario aplicar un enfoque riguroso para evaluar y mejorar la seguridad de los productos y también de los procesos que se llevan a cabo en el contexto de las Tecnologías de la Información y las Comunicaciones (Sanchez, Luis & Piattini, Mario, 2015).

Se considera que en la informática el análisis de los riesgos es complejo por la cantidad de información y el alto número de eventos potenciales, esto conlleva a que se tenga una gran cantidad de medidas de seguridad, las cuales al momento de utilizarlas dificulta su elección, sin embargo estas medidas servirán para proteger un bien de un conjunto de riesgos.

Al momento del diseño de un sistema informático se debe considerar que la seguridad es una parte fundamental, es la única medida que garantiza que la información utilizada en el sistema no sufra algún tipo de acceso inadecuado e indebido por terceras personas (Balarezo & Poveda, 2015).

El SGSI es una forma sistemática de administrar la información sensible de una institución, para que permanezca segura. Abarca a las personas, los procesos y las tecnologías de información. La forma total de la seguridad de la información, y la integración de diferentes iniciativas de seguridad necesitan ser administrados para que cada elemento sea completamente efectivo. Aquí es donde entra el Sistema de Gestión de Seguridad de la Información que permite coordinar esfuerzos de seguridad con mayor efectividad (Espinoza, 2013).

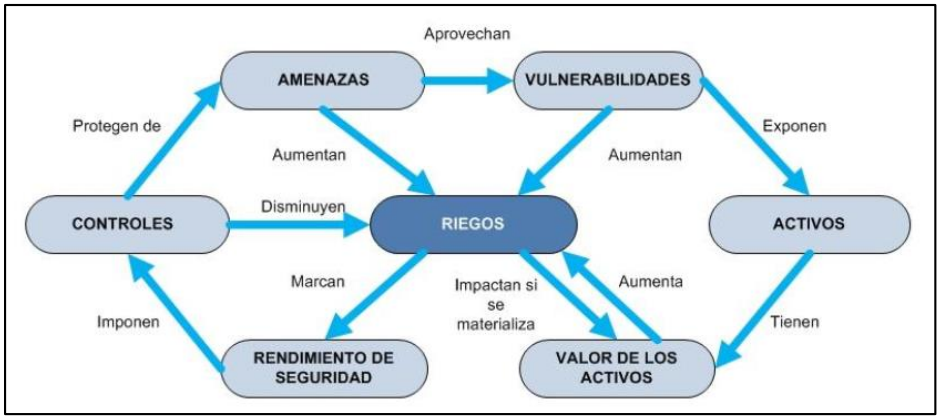


Figura N° 4. Sistema de gestión de seguridad de la información
Fuente: (Chanaluisa Viera, Meza Castillo, & Tasipanta Chicaiza, 2012).

El SGSI ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un bajo nivel de exposición de riesgo que la organización ha decidido asumir (Chanaluisa, Darwin & Meza, Andres & Tasipanta, Jessica, 2012).

2.2.1.6 Seguridad de la Información y gestión de eventos

El panorama de la tecnología ha cambiado drásticamente en los últimos 10 años y muchos de los enfoques de seguridad en las organizaciones que eran usados con anterioridad ya no son rival para las amenazas avanzadas de hoy en día. Herramientas como las de Seguridad de la Información y Gestión de Eventos (SIEM) se han convertido en elementos críticos para asegurar una infraestructura de red cada vez más compleja (Klaessig, 2014).

Estas herramientas, permiten centralizar el almacenamiento y la interpretación de registros o eventos generados por otras herramientas. Si bien existen casos de software comercial con funciones de SIEM (ArcSight, por ejemplo), hay una motivación especial para este tipo de arquitecturas en el mundo del Software Libre. La versatilidad y extensibilidad de las arquitecturas abiertas ha permitido que numerosos desarrolladores puedan escribir piezas de código con el objetivo de integrar sus sistemas específicos a una plataforma de monitorización estándar.
Dichas piezas de código se conocen como plugins, y son los encargados de normalizar los protocolos de contenido y transmisión de información concerniente a seguridad desde cualquier dispositivo que se desee integrar (Torres & Villegas, 2010).

2.2.2 Conceptos relacionados con la propuesta de solución

2.2.2.1 Definición SIEM

El acrónimo SIEM se atribuye a los analistas de Gartner: Amrit Williams y Mark Nicolett y se deriva a partir de dos tecnologías distintas, pero complementarias: Gestión de Eventos de Seguridad (SEM) y Gestión de la Información de Seguridad (SIM). Durante la última década, estas dos tecnologías han convergido en un único conjunto de soluciones que hoy conocemos como SIEM.

SEM fue una solución tecnológica que se centró en el seguimiento de eventos de seguridad en tiempo real, así como la correlación y el procesamiento. Estos eventos de seguridad eran típicamente alertas generadas por un dispositivo de seguridad de red, tales como un firewall o un Sistema de Detección de Intrusos (IDS por sus siglas en

inglés). SIM, por otra parte, se centró en el análisis histórico de la información del archivo de registro para apoyar las investigaciones forenses y los informes. SIM a menudo analiza los mismos eventos que SEM, pero no lo hace en tiempo real. SIM centraliza el almacenamiento de registros y archivos, búsqueda y análisis de funciones y, sólidas capacidades de presentación de informes. Los sistemas SIEMs combinan las capacidades de cada una de estas tecnologías en una única solución, de hecho, las soluciones SIEM actuales con frecuencia incorporan una función de gestión de registros mucho más amplia (ISACA, 2010).

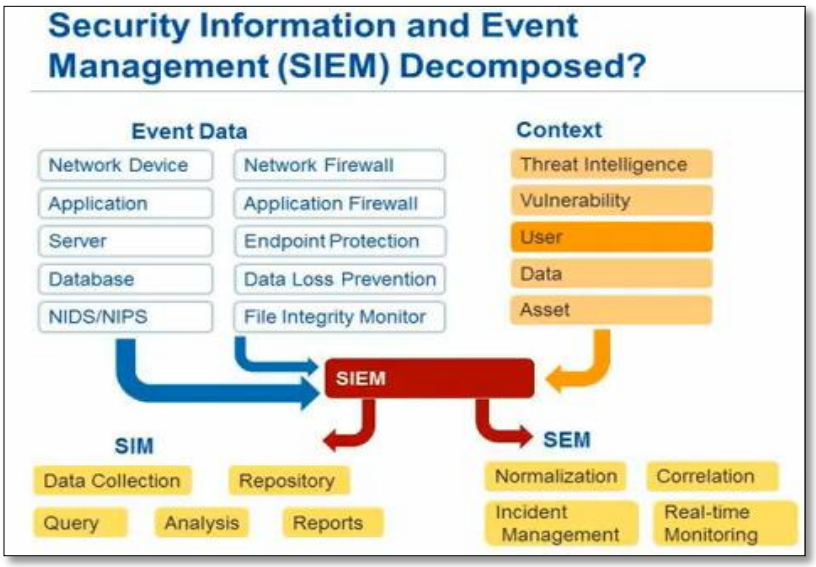


Figura N° 5. Fusión de SIM y SEM
Fuente: (Chikonga, 2014).

La figura N° 5 ilustra las capacidades individuales de SIM y SEM, demostrando cómo la fusión de estas tecnologías dio lugar a la tecnología SIEM.

2.2.2.2 Arquitectura básica de los sistemas SIEM

Los sistemas SIEM pueden ser comparados con una máquina compleja que posee un gran número de partes donde cada una realiza un trabajo específico e independiente. Todas estas partes deben colocarse a trabajar juntas adecuadamente o de lo contrario el sistema caerá en caos.

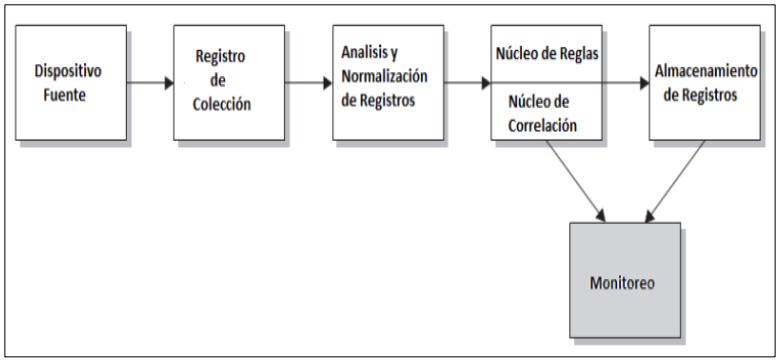


Figura N° 6. Arquitectura básica de un sistema SIEM
Fuente: (Baluja García, Caro Reina, & Cancio Bello, 2012).

Baluja García, Caro Reina, & Cancio Bello (2012) describen las partes o módulos que aparecen en la figura N° 6 de la siguiente manera:

Dispositivo Fuente: La primera parte de un sistema SIEM es el dispositivo que captura la información. Un Dispositivo Fuente es el dispositivo, aplicación que recupera los registros que se almacenan y procesan en el SIEM. El dispositivo de origen puede ser un dispositivo físico en la red (como un router, un switch, o algún tipo de servidor), aunque también pueden ser los registros de una aplicación o cualquier otra información que puede adquirir como por ejemplo firewalls, servidores proxy, IDS, Sistemas de Prevención de Intrusiones (IPS por sus siglas en inglés), bases de datos, entre otros. Su comunicación con el resto del sistema puede ser mediante protocolos estándares o protocolos privativos, dependiendo del fabricante de sistema.

Registro de Colección: La siguiente parte del sistema es el dispositivo o la aplicación de flujo de registro, el cual obtiene de alguna manera todos los registros de los dispositivos fuentes para luego transportarlos al SIEM. Actualmente, la recolección de datos ocurre de diferentes maneras y a menudo depende del método implementado dentro del sistema final, pero en su forma más básica, los procesos de recopilación de registros se pueden dividir en dos métodos fundamentales de colección: o el Dispositivo Fuente envía sus registros al SIEM, lo que se llama el método de empuje, o el SIEM se extiende y recupera los registros del dispositivo de origen, lo cual se llama el método de extracción. Cada uno de estos métodos tiene sus aspectos positivos y negativos cuando se utilizan en un determinado entorno, pero ambos logran obtener los datos desde el dispositivo de origen en el SIEM.

Análisis/Normalización de Registros: En este punto, los registros están todavía en su formato original en el repositorio centralizado y por tanto no resultan muy útiles para el

sistema. Para que estos registros resulten útiles para el SIEM se les debe dar un formato estándar, lo cual se conoce como normalización.

La normalización de los eventos no sólo hace que sean fácil de leer estos registros, sino que también facilita y permite un formato estándar para la generación de reglas del sistema, lo que significa que cada SIEM se encarga de las reglas de normalización de diferentes maneras. El resultado final es que todos los registros poseen el mismo aspecto dentro del sistema. Con frecuencia, antes de la normalización de los datos, se realizan copias de los registros, las cuales se almacenan en su formato original dentro del Log Storage.

Núcleo de Reglas/Núcleo de Correlación: Este componente se encuentra dividido en 2 segmentos, el Núcleo de Reglas y el Núcleo de Correlación de Reglas. El Núcleo de Reglas amplía la normalización de los eventos con el fin de activar alertas en el SIEM debido a las condiciones específicas en estos registros. Estas reglas generalmente vienen predefinidas en el sistema, pero también se pueden definir reglas personalizadas. Por lo general, se pueden escribir estas reglas usando una forma de lógica booleana para determinar si se cumplen condiciones específicas y analizar patrones en los campos de datos, pero se debe tener precaución para evitar el establecimiento de reglas de correlación demasiado complejas o demasiadas reglas, ya que cada nueva norma aumentará exponencialmente los requisitos computacionales y, eventualmente, pueden hacer que el proceso de correlación resulte ineficaz. La función del Núcleo de Correlación es comparar todos los eventos normalizados de diferentes fuentes con las reglas anteriormente creadas.

Almacenamiento de Registros: Este es usado para facilitar el trabajo en un único almacén de datos, facilitando la relación entre las diferentes funciones del SEM y las funciones forenses e informes del SIM. Su acoplamiento puede parecer sencillo, pero puede presentar una serie de retos y consideraciones. Este puede ser una base de datos, un archivo de texto plano o un archivo binario, ubicado de forma central o distribuida en dependencia al tamaño de la empresa, la cantidad de datos que son recogidos, y la infraestructura de TIC (Tecnologías de Información de Comunicación).

Monitoreo: Una vez que el SIEM tenga todos los registros y los acontecimientos que se han procesado, se necesita hacer algo útil con la información. Un SIEM tendrá una interfaz de consola y una interfaz que bien puede ser o basarse en una aplicación web. Ambas interfaces le permiten visualizar y analizar todos los datos almacenados en el

SIEM, facilitando de esta manera la gestión del sistema, pues brinda a los administradores una única visión de todo el entorno. También aquí se puede desarrollar el contenido y las reglas que se utilizan para extraer la información de los eventos que se están procesando.

Como menciona Sanchez, Luis & Piattini, Mario (2015), el cuadro de mando integral será la herramienta que nos permita evaluar de una forma rápida el estado de la seguridad y nos permitirá gestionar la seguridad en base a información cuantitativa y objetiva, lo que facilita la toma de decisiones alineadas con los requisitos del negocio.

2.2.2.3 SIEM y su posicionamiento en el mercado

El análisis realizado por Kavanagh & Rochford (2015) muestra que durante 2014, el mercado SIEM creció de $ 1.5 mil millones para aproximadamente $ 1690 millones, alcanzando una tasa de crecimiento de alrededor del 14%. En América del Norte sigue habiendo muchas nuevas implementaciones por parte de las empresas pequeñas que necesitan mejorar el control y detección de incumplimiento. Siguen habiendo nuevas implementaciones en empresas grandes que son conservadoras y que están adoptando esta nueva tecnología.

La demanda de tecnología SIEM en Europa y la región de Asia y el Pacífico sigue estable, impulsada por una combinación de requisitos de gestión de amenazas y los requisitos de cumplimiento. Las tasas de crecimiento en Asia y América Latina son muy superiores a las de EE.UU y Europa.

Clasificación en el cuadrante mágico de Gartner:

Los vendedores SIEM siguen mejorando gradualmente las capacidades del producto en áreas relacionadas con la detección de incumplimiento, la detección de anomalías y monitoreo de la actividad de la red , así como la investigación de flujo de trabajo y gestión de casos.

Los siguientes criterios tenían que cumplir para los vendedores que se incluirán en el Cuadrante Mágico SIEM 2015:

- El producto debe proporcionar capacidades SIM y SEM.
- El producto debe ser compatible con la captura de datos de fuentes de datos heterogéneas, incluyendo los dispositivos de red, dispositivos de seguridad, los programas de seguridad y servidores.

- El vendedor debe aparecer en las listas de evaluación de productos SIEM de organizaciones de usuarios finales.
- La solución debe ser entregado al entorno del cliente como un producto en software o basada en dispositivos (no es un servicio).

Los vendedores fueron excluidos si:

- Proporcionan funciones SIEM que están orientados principalmente a los datos de sus propios productos.
- Ellos posicionar sus productos como una ofrenda SIEM, pero los productos no aparecen en las listas de candidatos competitivas de las organizaciones de usuarios finales.
- Tenían menos de $ 13,5 millones en ingresos por productos SIEM durante 2014.
- La solución se entrega exclusivamente como un servicio gestionado.

Figura N° 7. Cuadrante mágico de Gartner para la Seguridad de la Información y la Gestión de Eventos
Fuente: (Kavanagh & Rochford, 2015).

Líderes

El Cuadrante de Líderes SIEM está compuesto por los vendedores que ofrecen productos que son un buen partido funcional a las necesidades del mercado en general, han sido los más exitosos en la construcción de una base instalada y la fuente de ingresos en el mercado SIEM. Además de proporcionar tecnología que es un buen partido a las necesidades actuales de los clientes, líderes también muestran evidencia de una visión superior y ejecución para los requisitos previstos. Por lo general tienen cuota de mercado relativamente alta y / o fuerte crecimiento de los ingresos, y han demostrado la retroalimentación positiva de los clientes para las capacidades de SIEM eficaces y servicios relacionados y de apoyo.

Como apreciamos en la figura N° 7 aquí se encuentran: IBM Security, HP, Splunk, Intel Security y LogRhythm.

Challengers

El cuadrante Challengers se compone de los vendedores que tienen un flujo de ingresos de gran tamaño (por lo general debido a que el vendedor tiene múltiples productos y / o líneas de servicio. Los vendedores en este cuadrante suelen tener fuertes capacidades de ejecución, como lo demuestran los recursos financieros, las ventas y la marca significativa presencia cosechado de la empresa en su conjunto o de otros factores. Sin embargo, Challengers no han demostrado una capacidad o trayectoria por sus tecnologías SIEM como proveedores en el cuadrante de líderes. Aquí encontramos a: EMC (RSA).

Visionarios

El cuadrante de Visionarios se compone de los vendedores que ofrecen productos que son un buen partido funcional a las necesidades generales del mercado SIEM, pero que tienen una menor capacidad para ejecutar calificación de los líderes. Esta calificación más baja se debe normalmente a una menor presencia en el mercado SIEM que los líderes, según lo medido por base instalada o el tamaño de los ingresos o el crecimiento, o por más pequeño tamaño de la empresa en general o la viabilidad general.

Aquí encontramos a AlienVault que ofrece productos comerciales como es USM y su versión open Source que es OSSIM.

Niche Players

El cuadrante Niche Players está compuesto principalmente de proveedores más pequeños que proporcionan la tecnología SIEM que es un buen partido para un caso específico uso SIEM, un subconjunto de las exigencias del mercado SIEM. Niche Players centran en un segmento particular de la base de clientes o de un conjunto de productos más limitada. Su capacidad para superar o innovar puede verse afectada por este enfoque estrecho. Los vendedores en este cuadrante pueden tener una pequeña base instalada o estar limitados, de acuerdo con criterios de Gartner, por una serie de factores. Estos factores pueden incluir inversiones limitadas o capacidades, una huella geográficamente limitada, u otros inhibidores de proporcionar un conjunto más amplio de capacidades para las empresas ahora y durante el horizonte de planificación de 12 meses. La inclusión en este cuadrante no refleja negativamente en el valor del proveedor en el espectro de un servicio más enfocado estrecho. Aquí se encuentran vendedores como: SolarWinds, Micro Focus (NetIQ), Trustwave, EventTracker, AcceIOps y BlackStratus.

2.2.2.4 Uso de Herramientas SIEM en Pymes

La creciente complejidad de los sistemas de información en combinación con sus problemas de cumplimiento normativo, las conexiones de red pública y necesidad competitiva representa incluso para las grandes empresas importantes desafíos de gestión de seguridad de la información. Para la pequeña y mediana empresa que puede parecer imposible conseguir realmente el control de la seguridad y disponibilidad de los sistemas que necesita para mantenerse a la vanguardia en los negocios (Shivhare & Savaridassan, 2015).

Como todos sabemos la seguridad es un tema que preocupa a todas las compañías, sin importar su tamaño ni tipo de negocio, tanto a nivel nacional como internacional (Izquierdo & Almazán, 2006).

Los sistemas SIEM demuestran ser una buena alternativa de gestionar la seguridad de red, una interfaz común (Baluja García, Caro Reina, & Cancio Bello, 2012).

Sin embargo implementar una solución SIEM tiene un costo elevado que incluye: costos iniciales de licenciamiento, costos de implementación/optimización, costos constantes de gestión, costos de Integración de fuentes de datos de diferentes tecnologías y formación de personal / personal nuevo (AlienVault).

Por lo que estas organizaciones pueden optar por SIEM Open Source**,** un ejemplo de las consolas de gestión de código abierto más populares en la actualidad es OSSIM (Madrid Molina, y otros, 2008).

A continuación mostramos una comparativa de la herramienta de código abierto OSSIM de AlienVault y algunas de las herramientas SIEM comerciales:

Tabla N° 2: Comparación de OSSIM con herramientas SIEM comerciales

	OSSIM	ARCSIGHT	RSA	Net IQ	IBM -ISS	Symantec	LogLogic	Cisco Security Mars
GENERAL								
Costo licencia	Sin costo	Muy alto	Alto	Alto	Muy alto	Alto	Normal	Normal
FUNCIONALIDAD								
SIM/SIEM	Si	Si	Si			Si	No	Si
Interfaz web	Si			No (Win 32)		Si	Si	Si
Log almacenamiento	Si	Si	Si	Si		Si	Si	Si
Log correlación	Si	Si	Si	Si		Si	Si	Si
Gestión de incidentes	Si	Si	Si	Si		Si	No	
Reportes DataMart	Si	Solo reportes	Solo reportes	Si		Si	Si	Solo reportes
HERRAMIENTAS								
Network IDS	Snort	No	No	No	Si	Symantec IDS	No	Si
Vulnerabilidades	Nessus	No	No	No	Si	Symantec Vulnerability Assessment	No	
Monitor de red	Ntop	No	No	No	No		No	No
Detección de anomalías	Spade	No	No	No	Si		No	Si
Host IDS	Snare & Osiris	No	No	No	Si	Symantec IDS	No	No
Inventario	OCS	No	No	No	No		No	No
Antivirus	ClamAV	No		No	No	Norton	No	
HARDWARE								
Appliances	Si	No	No		Si	Si	No	

Fuente: Comparación de Sistemas de Seguridad de Información y Gestión de Eventos (Chanaluisa Viera, Meza Castillo, & Tasipanta Chicaiza, 2012).

Como apreciamos en la tabla N° 2 existen varias herramientas que realizan las mismas funciones que OSSIM, pero como ya hemos visto implementarlas implican costos muy

elevados. Por lo que concluimos que OSSIM es la mejor herramienta que puede implementarse y generar ventaja competitiva.

Recalcando también que es la única herramienta open Source que se encuentra en el cuadro mágico de Gartner.

2.2.2.5 OSSIM

OSSIM AlienVault (Open Source Security Information Manager) es un SIEM desarrollado por Dominique Karg y Julio Casal en el año 2000, que implementa la detección y prevención de intrusiones, y la seguridad de redes en general (Baluja García, Caro Reina, & Cancio Bello, 2012).

Esta herramienta trae incorporada cerca de 22 Funciones, todas estas son Open Source capaces de correlacionarse y así poder tener el control centralizado, básicamente se lo puede representar en el siguiente diagrama (Bravo Bravo & Villafuerte Quiroz, 2015).

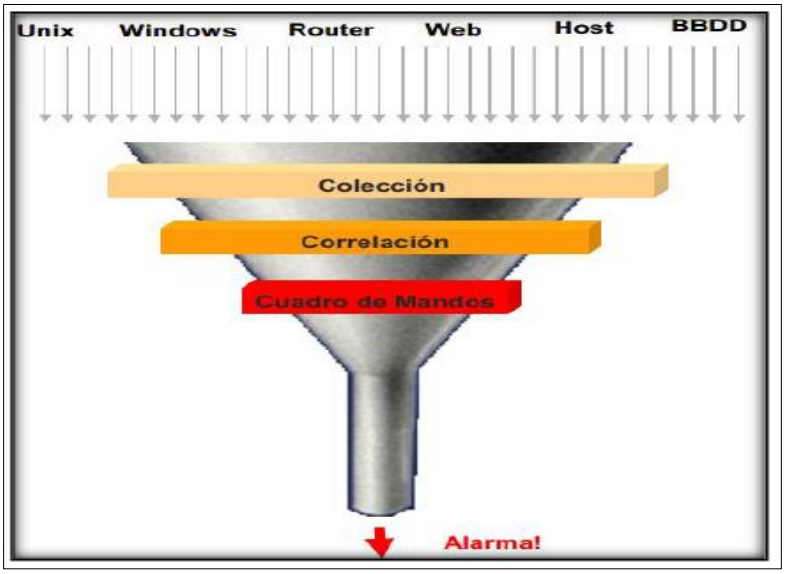


Figura N° 8. Modelo de OSSIM
Fuente: (Bravo Bravo & Villafuerte Quiroz, 2015).

El objetivo de OSSIM ha sido crear un framework capaz de recolectar toda la información de los diferentes plugins, para integrar e interrelacionar entre si y obtener una visualización única del estado de la red y con el mismo formato, con el objetivo de aumentar la capacidad de detección de anomalías, priorizar los eventos según el contexto en el que se producen y mejorar la visibilidad de la monitorización del estado de la red actual (Puchades Olmos, 2008).

A diferencia de muchas otras suites de seguridad, tanto libres como propietarias, OSSIM supera el clásico problema del exceso de alertas y de información ya que opera a diferentes niveles, de modo que evita recibir demasiadas alertas poco fiables (falsos positivos), al mismo tiempo que es altamente efectiva para identificar ataques con comportamientos más complejos (falsos negativos).

Una vez en funcionamiento, el software permite detectar ataques con comportamientos específicos de código malicioso, como por ejemplo un «Caballo de Troya», o bien ataques de comportamiento desconocido. En este último caso, la capacidad del sistema es mucho más relevante, ya que puede localizar ataques no conocidos o no detectables pues no se dispone de los patrones que caracterizan este ataque.

La forma de detección más compleja y de mayor valor de OSSIM es la que combina diferentes ataques específicos, de modo que descubre ataques distribuidos al encontrar la relación entre varios atacantes o ataques recibidos y el acceso a la red desde Internet (Izquierdo & Almazán, 2006) **.**

2.2.2.5.1 Componentes

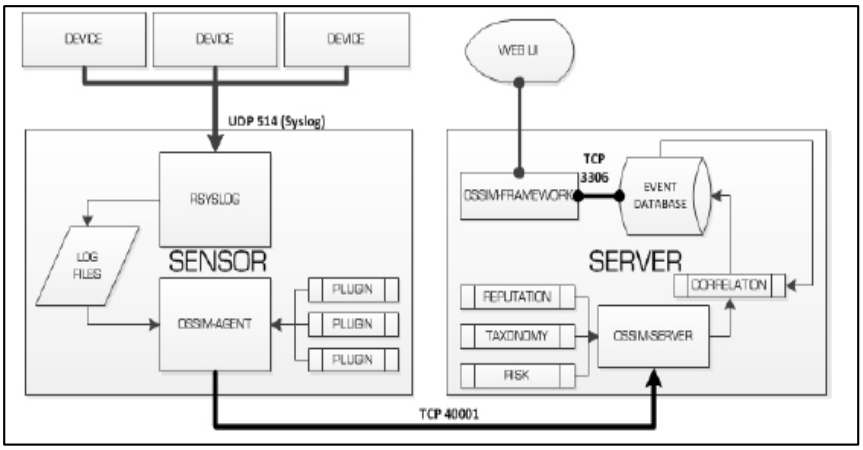


Figura N° 9. OSSIM Architecture
Fuente: (Alamanni, 2014).

OSSIM tiene 4 componentes principales:

Server

Es el componente principal de OSSIM. Recibe los eventos enviados por los distintos agentes y realiza además las funciones de priorización y correlación (Nuñez Martínez, 2008)**.**

El servidor OSSIM proporciona las funciones SIEM principales de agregación de log, la normalización, el establecimiento de prioridades, reputación y la correlación.

El proceso de servidor acepta la comunicación de los agentes (sensores) y el framework OSSIM, través del puerto TCP 40001 entrante.

Los agentes se comunican con AlienVault IDM (Gestión de Identificación) en el servidor mediante el puerto TCP 40002 entrante.

OSSIM Server se comunica con la base de datos en puerto TCP 3306 saliente.

El servidor OSSIM se gestiona mediante la línea de comandos sobre el puerto TCP 22 entrante (Secure Shell) (AlienVault, 2013).

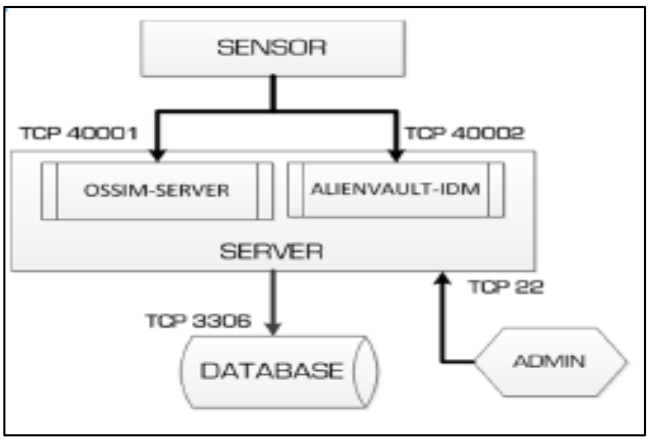


Figura N° 10. AlienVault Server
Fuente: (AlienVault, 2013).

Framework

Es el intermediario entre el servidor central y el usuario. La herramienta de administración utilizada para configurar y organizar los diferentes módulos tanto externos como propios que integra OSSIM. Contribuye a definir una topología, inventariar activos, definir políticas de seguridad, reglas de correlación y unir las diferentes herramientas integradas (Nuñez Martínez, 2008).

Framework proporciona conectividad y gestión entre los componentes OSSIM y la interfaz de usuario principal

La interfaz de usuario Web funciona a través de HTTPS, el puerto TCP 443 entrante. Puerto 80 entrantes también se activa por defecto, pero sólo sirve para redireccionar a los clientes del puerto HTTPS.

El framework OSSIM se comunica con la base de datos en el puerto TCP 3306 saliente.

El framework OSSIM se gestiona mediante la línea de comandos sobre el puerto TCP 22 entrante (Secure Shell) (AlienVault, 2013).

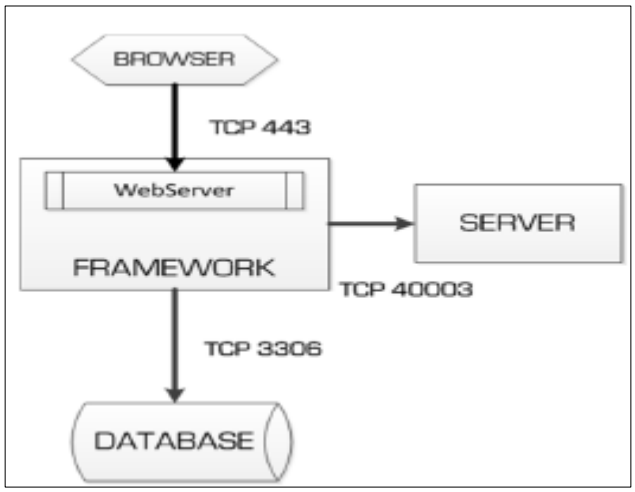


Figura N° 11. AlienVault Framework
Fuente: (AlienVault, 2013).

Sensor

Son host distribuidos en diferentes segmentos de la red, para monitorizar los distintos eventos. Estos se distribuyen sobre la base de los servicios que se van a monitorear. Cada agente o sensor tendrá configurado un conjunto de detectores o monitores, que generan eventos para que el agente los recolecte y reporte al servidor central (Nuñez Martínez, 2008).

Interfaces de red

Los sensores OSSIM están configurados con dos interfaces: una interfaz de administración y una interfaz de control. La interfaz de administración está configurada con una IP y se utiliza para la comunicación con otros OSSIM componentes, la interfaz de control requiere visibilidad en el tráfico de red (normalmente a través de un puerto SPAN de un conmutador de red) (AlienVault, 2013).

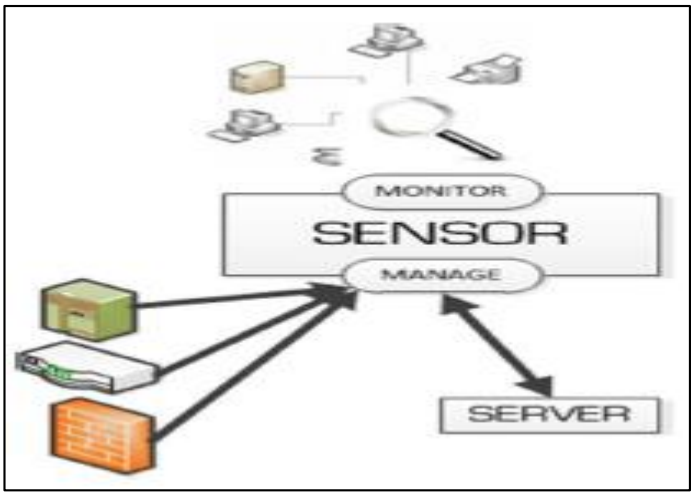


Figura N° 12. AlienVault Sensor (Interfaces de red)
Fuente: (AlienVault, 2013).

Conexiones

Los dispositivos transmiten los datos de registro a los sensores a través del protocolo syslog de UDP (y opcionalmente TCP cuando sea compatible) puerto 514.

Otros tipos de registro pueden requerir conexiones salientes desde el sensor hasta el dispositivo, consultan la documentación de un determinado tipo de dispositivo para obtener información acerca de qué puertos se utilizan.

Los sensores se comunican al servidor OSSIM a través de los puertos TCP 40001 y 40002 salientes.

El servidor obtiene las actualizaciones de inventario y monitoreo de la red mediante puertos TCP 3000 y 4949 y el puerto UDP 555.

El sistema de escaneo de vulnerabilidades funciona desde el sensor y es controlado mediante los puertos TCP 9390 y 9391 (AlienVault, 2013).

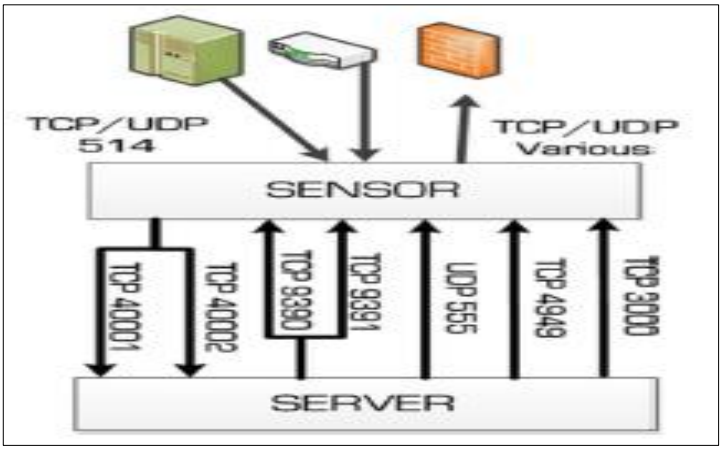


Figura N° 13. Conexiones del sensor
Fuente: (AlienVault, 2013).

Sensores remotos a través de VPN

Los Sensores de AlienVault también pueden ser configurado para establecer un túnel VPN al Servidor de AlienVault.

En esta configuración toda la conectividad entre el sensor y el servidor se produce a lo largo de puerto UDP 1194 (AlienVault, 2013).

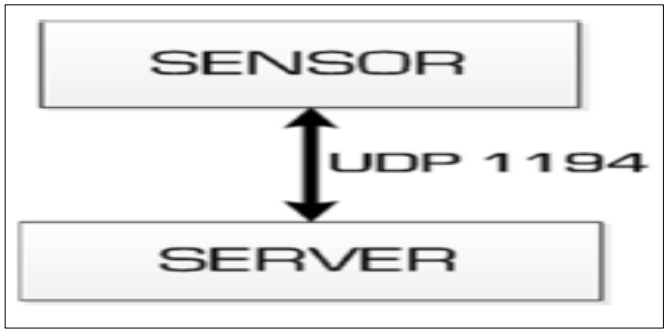


Figura N° 14. Sensor remoto a través de VPN
Fuente: (AlienVault, 2013)

Data Base

Aquí se almacenan los diferentes eventos recolectados por los agentes, y las configuraciones de las distintas herramientas y OSSIM.

Los componentes Servidor, Framework y la Base de Datos se encuentran ubicados en un equipo que se desempeña como servidor central de OSSIM y los agentes pueden estar distribuidos en los distintos equipos (Nuñez Martínez, 2008).

La base de datos del sistema almacena datos de evento y configuraciones en tiempo de ejecución los componentes OSSIM.

Tanto el servidor OSSIM Servidor y el framework OSSIM se conectan a la base de datos en puerto TCP 3306 (AlienVault, 2013).

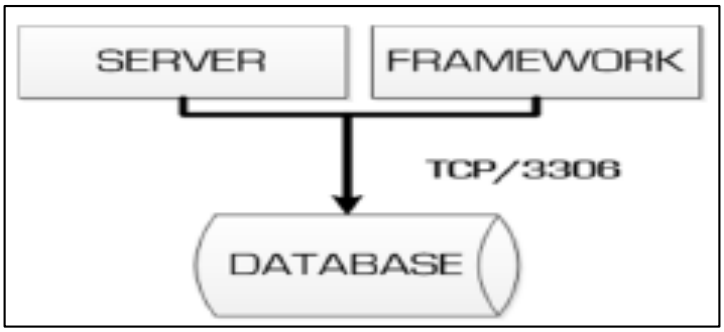


Figura N° 15. Base de Datos AlienVault
Fuente: (AlienVault, 2013).

Yagual Del Valle & Chilán Rodríguez (2014) describen que OSSIM utiliza tres bases de datos heterogéneas para los distintos tipos de datos almacenados las cuales son:

EDB Base de datos de eventos, la más voluminosa pues almacena todos los eventos recibidos desde los detectores y monitores.

KDB Base de datos del framework, en la cual se almacena toda la información referente a la red y la definición de la política de seguridad.

UDB Base de datos de perfiles, almacena todos los datos aprendidos por el monitor de perfiles.

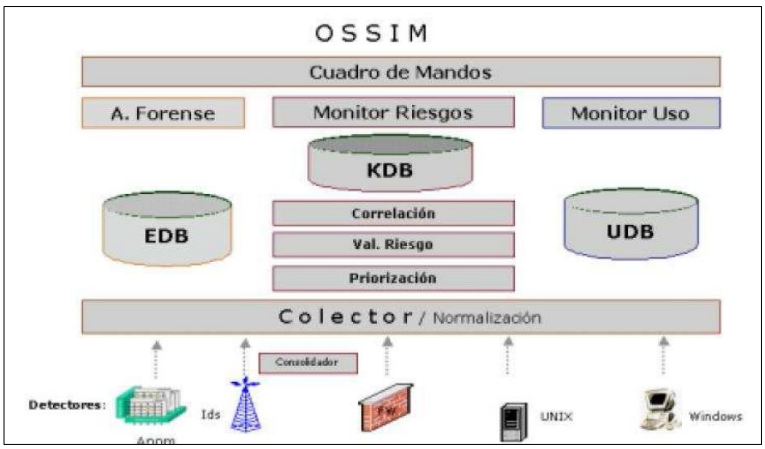


Figura N° 16. Arquitectura de OSSIM
Fuente: (Puchades Olmos, 2008).

2.2.2.5.2 Capas de OSSIM

Según el informe de Chanaluisa Viera, Meza Castillo, & Tasipanta Chicaiza (2012) los componentes de OSSIM son módulos autónomos y pueden ser configurados como el administrador necesite. Todos estos componentes pueden disponerse en distinto hardware, separando todos los componentes o colocando todos ellos juntos en una sola máquina.

OSSIM puede recibir eventos de dispositivos comerciales o aplicaciones propietarias gracias a plugins específicos y genéricos configurables.

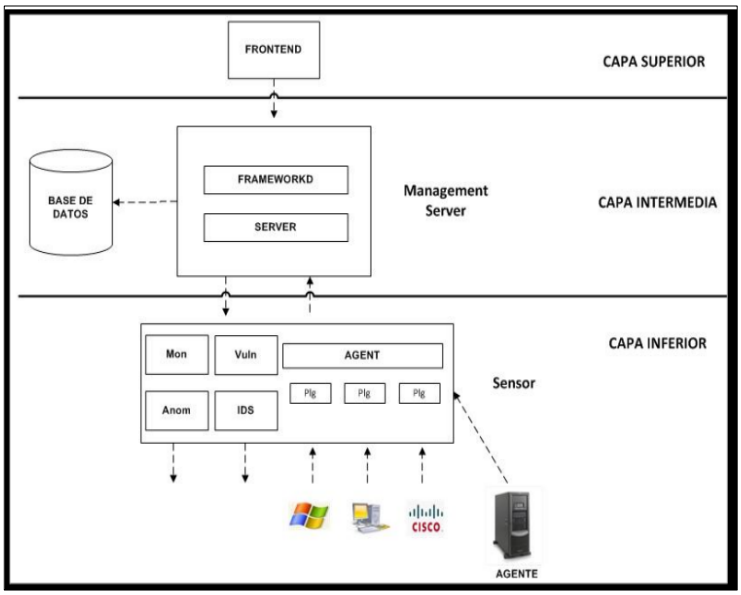


Figura N° 17. Capas del sistema OSSIM
Fuente: (Chanaluisa Viera, Meza Castillo, & Tasipanta Chicaiza, 2012).

Configuraciones avanzadas permiten el montaje de una arquitectura distribuida de servidores como muestra a continuación:

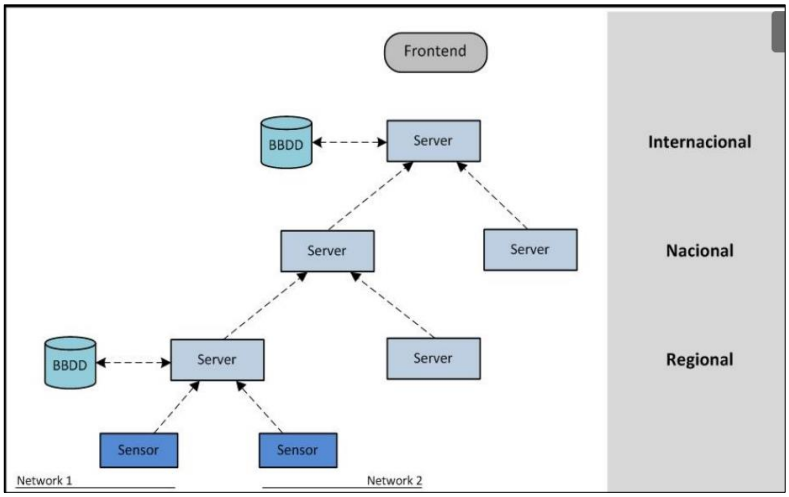


Figura N° 18. Capas del sistema OSSIM en una arquitectura distribuida
Fuente: (Chanaluisa Viera, Meza Castillo, & Tasipanta Chicaiza, 2012).

Es posible instalar motores de correlación en sensores, permitiendo correlación y filtrado a bajo nivel implementar políticas de Consolidación (para ahorrar ancho de banda).

Capa Inferior

Es el nivel más bajo "preprocesado", se compone por un número de detectores, monitores dispersados por la red. Se encargan de realizar la detección y generación de alertas que posteriormente enviarán la información al sistema central para la colección y correlación de los diferentes eventos. Los sensores se despliegan en la red para monitorizar actividad de red.

Normalmente incluyen: monitores y detectores pasivos de bajo nivel que colectan datos buscando patrones y analizadores que de forma activa buscan vulnerabilidades en la red.

Agente de OSSIM que reciben datos desde equipos de red (routers, firewalls, etc), comunican y envían sus eventos al servidor padre.

Una configuración de sensor típica de OSSIM tendrá las siguientes funciones:

- IDS (Snort)
- Analizador de Vulnerabilidades (Nessus)
- Detector de Anomalías (Spade, P0f, Pads, Arpwatch, RRD ab Behaviour)
- Monitorización y Perfil de red (Ntop)
- Colección de eventos de routers locales, firewalls, IDS's, etc.

Capa intermedia

En el nivel intermedio se realiza el post procesado, donde se desarrolla un proceso de abstracción en el que millones de pequeños eventos incompresibles se convierten en singulares alarmas comprensibles, este proceso se lleva a cabo principalmente en el motor de correlación, donde el administrador crea directivas de correlación para unir diferentes eventos de bajo nivel en una única alarma de alto nivel, cuyo objetivo es aumentar la sensibilidad y la confiabilidad de la red. Servidor de Gestión normalmente incluye los siguientes componentes:

Framework: Es el demonio de control que mantiene unidas algunas partes.

OSSIM Server: Centraliza la información recibida de los sensores.

El Server de Gestión cumple al menos las siguientes funciones:

- Las principales tareas del server son Normalización, Priorización, Colección, Valoración de Riesgos y Motores de Correlación
- Tareas de mantenimientos y externas como backups, Backups planificados, inventario de activo o ejecución de análisis.
- Base de Datos almacena eventos e información útil para la gestión del sistema, base de datos SQL.

Capa Superior: Por último, en el nivel más alto "Front-End" se ubica una herramienta de gestión, capaz de configurar y visualizar tanto los módulos externos como los propios del framework, mediante ella podremos crear la topología de la red, inventariar activos, crear las políticas de seguridad, definir las reglas de correlación y enlazar las diferentes herramientas integradas.

El Front-End o Consola es la aplicación de visualización en este caso es una consola web.

2.2.2.5.3 Proceso de detección

La capacidad de detección

Consiste en el descubrimiento de anomalías, vulnerabilidades mediante el uso de técnicas de recopilación de datos provenientes de los detectores y monitores de la red.

Reforzar la seguridad de la red dependerá de los dispositivos que se utilicen y la capacidad de detección que tengan estos para detectar los ataques o amenazas.
La capacidad de un detector se define mediante 2 variables:

Sensibilidad: Definida como la capacidad de análisis que posee el detector al momento de localizar un posible ataque.

Fiabilidad: Definida como el grado de certeza que ofrece el detector ante el aviso de un posible evento (Yagual Del Valle & Chilán Rodríguez, 2014).

La incapacidad de detección

Los detectores en la actualidad tienen 2 principales problemáticas:

Falsos Positivos: La falta de fiabilidad en los detectores es el causante del mayor problema actual, es decir alertas que realmente no corresponden con ataques reales.

Falsos Negativos: La incapacidad de detección implicaría que un ataque es pasado por alto (Chanaluisa Viera, Meza Castillo, & Tasipanta Chicaiza, 2012)**.**

Tabla N° 3: Capacidad de los detectores

	Propiedad	Efecto ante su ausencia
FIABILIDAD	El grado de certeza que nos ofrece nuestro detector ante el aviso de un posible evento.	Falsos Positivos
SENSIBILIDAD	La capacidad de análisis, en profundidad y complejidad, que posee nuestro detector a la hora de localizar un posible ataque.	Falsos Negativos

Fuente: Capacidad de los detectores (Karg, Muñoz, Gil, González, & Casal, 2003).

2.2.2.5.4 Funcionalidad

OSSIM cumple las siguientes funciones:

Detector de patrones

Son aplicaciones capaces de monitorizar el tráfico de la red, en busca de patrones malignos definidos a través de firmas o reglas, estas aplicaciones producen eventos de seguridad.

Las aplicaciones más comunes son los sistemas de detección de intrusos, se basan en el análisis detallado de tráfico de la red, comparando el tráfico con las firmas de ataques conocidos o reglas de comportamientos sospechosos. Estos sistemas analizan tanto el tipo de tráfico como el contenido y el comportamiento de los paquetes de la red, tienen la capacidad de detectar patrones en la red como puede ser un escaneo de puertos, intentos de spoofing o posibles ataques por fragmentación, cada uno de ellos tiene su propio log de seguridad capaz de alertar posibles problemas de red.

Ossim integra varios detectores de patrones de código abierto como Snort (NIDS), Snare y Osiris (HIDS), integrados en el sistema (Chanaluisa Viera, Meza Castillo, & Tasipanta Chicaiza, 2012).

Detector de anomalías

Los detectores de anomalías tienen una capacidad de detección mucho más compleja que la de los detectores de patrones. En este caso al sistema de detección de anomalías no se le tiene que especificar patrones de seguridad mediante reglas, ya que es capaz de identificar si un comportamiento difiere del comportamiento normal.

Funcionalidad de los detectores de anomalías:

- Detecta nuevos ataques que aún no están registrados por los detectores de patrones.
- Detecta gusanos introducidos desde la red interna o ataque de spam, que pueden generar un número de conexiones anómalas.
- Detecta uso de servicios con origen y destino anormales.
- Detecta uso de activos en horarios anormales.
- Detecta exceso de tráfico o de conexiones.
- Detecta cambios de sistemas operativos, IP, MAC.

Ossim integra una amplia gama de detectores de anomalías:

- Aberrant Behaviour plugin para Ntop examina parámetros y alerta cuando dichos parámetros se salen de los valores esperados.
- ArpWatch utilizado para detectar cambios de MAC.
- P0f utilizado para detección de cambios de sistema operativo.
- Nmap utilizado para detectar anomalías en los servicios de red.

Colección y la normalización de registros

El proceso de colección y normalización se encarga de unificar todos los eventos de seguridad provenientes de cualquier sistema de la red en una única consola y formato (Puchades Olmos, 2008)**.**

Según (Alamanni, 2014) podemos recoger los registros de los dispositivos de la red de dos formas:

Instalación de un agente de software (como Caja o SysLogAgent) en la máquina de origen y se configura para leer ciertos tipos de registros y enviarlos a componente del sensor.

Configurar la máquina de origen para enviar los registros a petición del Sensor adecuado plugins (por ejemplo, a través de WMI para máquinas Windows). Una vez que el sensor almacena los registros, el Agente OSSIM realiza el análisis y los convierte en un formato único (normalización). Cada registro representa un evento que se envía al servidor de análisis.

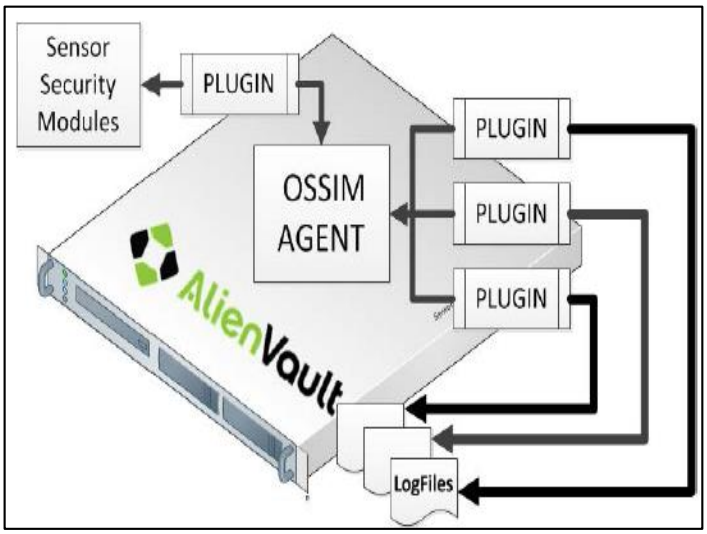


Figura N° 19. Colección de registros y normalización
Fuente: (Alamanni, 2014).

La normalización implica la existencia de un intérprete que conozca los tipos de formatos de alertas de los diferentes detectores, capaz de estandarizar el tratamiento y almacenar todos los eventos de seguridad en una única base de datos "EDB". Para luego visualizar en la misma pantalla y con el mismo formato los eventos de seguridad de un momento específico ya sean del Router, firewall, IDS o de cualquier host (Yagual Del Valle & Chilán Rodríguez, 2014).

Priorización de eventos y evaluación de riesgos

El proceso de priorización consiste en asignar los valores de prioridad a los eventos grabados, que se realiza en el componente de servidor. Depende de la estructura de la red y que necesita, como requisito previo, la definición de las políticas de seguridad y el inventario de los activos de información en la red, que puede ser administrado en la Web panel de administración. Establece la prioridad de un evento en función de la máquina que lo generó y el tipo de evento al que pertenece.

La evaluación del riesgo de eventos se calcula en tiempo real y se basa en tres factores principales:

- El valor o nivel de importancia de la máquina que generó el evento.
- El tipo de amenaza que presenta el caso.
- La probabilidad de que se produce este evento.

La fórmula utilizada para calcular el riesgo es la siguiente:

Riesgo = valor * (fiabilidad * Prioridad / 25)

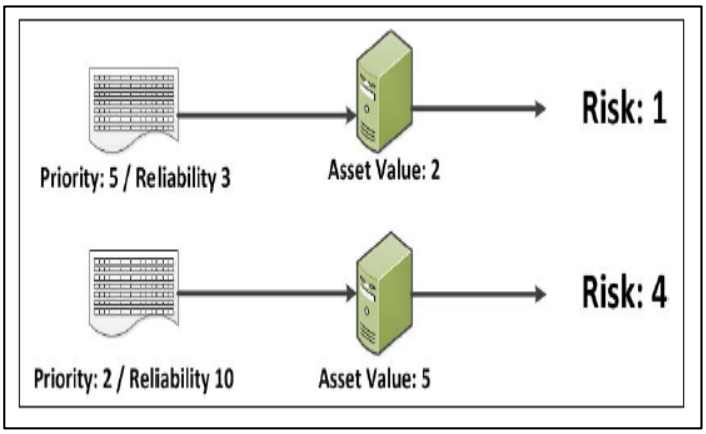


Figura N° 20. Como calcular el riesgo asociado a un evento
Fuente: (Alamanni, 2014).

Análisis y correlación de eventos

La correlación de eventos se refiere fundamentalmente a eventos que se relacionan entre si para obtener una visión global de la seguridad de la red y detectar posibles ataques o anomalías.

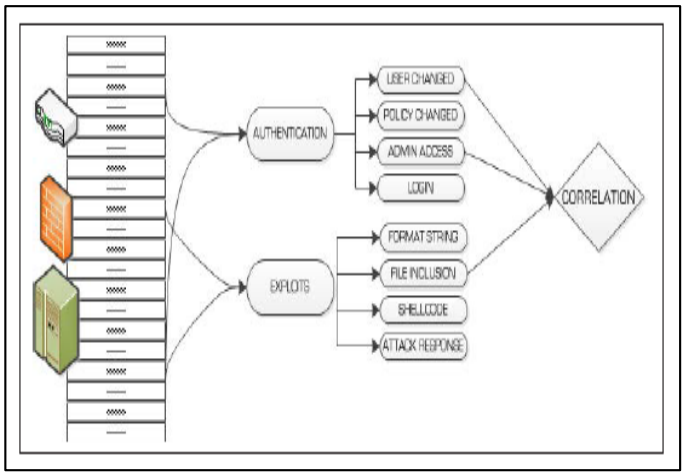


Figura N° 21. Ejemplo de análisis y correlación de eventos
Fuente: (Alamanni, 2014).

El proceso de correlación se realiza a través de dos métodos:

1. **Correlación siguiendo la secuencia de los eventos**, mediante directivas, integrado por un conjunto de normas que se relacionan los eventos de patrones de ataques conocidos. Este método es similar a utilizar Snort para la detección de intrusiones (detección basada en firmas).

2. **La correlación usando algoritmos heurísticos** puede ser detectado por estas situaciones anómalas que no detectan las reglas anteriores y que pueden o no ser ataques (detección de anomalías).

   Las directivas se especifican en XML con etiquetas como Id, Nombre, Prioridad, Tipo, fiabilidad, frecuencia, tiempo de espera, el origen, el destino, puerto de origen, puerto de destino, el protocolo PluginSid y el sensor. La confiabilidad es una medida de la probabilidad de que el evento representa verdaderamente el ataque a las que se refiere la directiva y generalmente se basa en el número de ocurrencias del evento.

   (Alamanni, 2014).

   La directiva asigna un valor de fiabilidad igual a 3 (30% de probabilidad) cuando el número de ocurrencias del evento detectado por el sensor (SSH

error de autenticación) es igual a 1, entonces incrementa en 1 en la tercera aparición del evento, por 2 en la quinta aparición, y por una cantidad adicional de 2 en el décimo, logrando así una fiabilidad de 8 (80% de probabilidad) cuando los intentos de autentificación incorrectos 10. OSSIM también tiene la capacidad de relacionar entre sí los distintos tipos de logs generados por distintos plugins (cross-correlation). La correlación cruzada permite cambiar el evento fiabilidad y la evaluación de los riesgos. Por ejemplo, supongamos que Nessus, OpenVas ha identificado una vulnerabilidad en el servidor. Si Snort detecta un evento que indica un posible ataque en ese servidor, el motor de correlación aumenta el nivel de riesgo asociado con el evento (Alamanni, 2014).

Puchades Olmos (2008), Considera otro tipo de correlación aparte de los dos mencionados anteriormente como es:

3. **Correlación mediante inventariado:** Todo ataque tiene como objetivo un determinado sistema operativo o servicio especificado. La correlación de inventario comprueba si el sistema atacado usa ese sistema operativo o servicio objetivo del ataque. Si lo usa, podremos determinar que existe riesgo, por lo contrario, se puede confirmar que el evento para dicha maquina es un falso positivo.

   Este tipo de correlación depende de la fiabilidad del inventario, Ossim incorpora además del inventario manual, un método de inventario automático.

Niveles de correlación:

A causa de la recursividad que el modelo de correlación de Ossim ofrece se puede crear una jerarquía de niveles casi infinita.

Figura N° 22. Representación con 3 niveles de correlación
Fuente: (Chanaluisa Viera, Meza Castillo, & Tasipanta Chicaiza, 2012)**.**

Chanaluisa Viera, Meza Castillo, & Tasipanta Chicaiza (2012), explican el nivel 2 y 3 de la figura anterior de la siguiente manera:

Nivel 2:

Ataque específico. El motor de correlación es alimentado por los detectores de patrones y es capaz de procesar estos eventos para detectar nuevas alarmas. Además, puede detectar nuevos eventos a causa de una actividad específica en la red, proporcionando alarmas con una determinada prioridad y confiabilidad. Esta correlación limita falsos positivos y prioriza ataques reales en el motor de correlación.

Ataque General. La localización de ataques no conocidos se realiza a causa de la generación de actividades anómalas por parte de un intruso. Se almacena parámetros como puertos, servicios, tráfico e incluso el horario para detectar comportamientos sospechosos.

Nivel 3:

Comportamiento del Ataque. El tercer nivel se alimenta de alertas generadas por la correlación de varios ataques específicos o actividades anómalas. La determinación de cada nivel localiza patrones de comportamiento que caractericen el objetivo, el camino trazado y el comportamiento del atacante.

Generación de alarmas acciones de respuesta

Las directivas pueden crear alarmas, las que son generadas por un único evento o por una secuencia específica de eventos bajo ciertas condiciones. Las alarmas se pueden mostrar en el Web panel de administración, en la opción de menú Análisis→Alarma. Además, las alarmas pueden activar acciones de respuesta, como por ejemplo, enviar una alerta por correo electrónico al administrador del sistema y/o la ejecución de scripts adecuados (Alamanni, 2014)**.**

Otras funcionalidades de Ossim según (Chanaluisa Viera, Meza Castillo, & Tasipanta Chicaiza, 2012)**:**

Monitores

OSSIM realiza una monitorización de la red esencial para un sistema de seguridad, ya que sin ella un administrador de seguridad estará ciego cuando ocurran eventos, sin poder distinguir la actividad anómala de la normal.

Ossim realiza diferentes tipos de monitorización:

- **Monitor de Riesgos (RiskMeter).** Representa los valore producidos por el algoritmo CALM, valores que miden el nivel de riesgo de compromiso "C" y el de ataque "A" procedentes de la recepción de alertas que indican que una determinada maquina ha sido comprometido o está siendo atacada.

- **Monitor de Uso.** Ofrece datos generales de la máquina, como el número de bytes que transmite al día.

- **Monitor de Perfiles**. Ofrece datos específicos del uso realizado por el usuario y permite establecer un perfil, (ej: uso de correo, pop y http, perfil de usuario normal), estos datos se obtienen de la base de datos de perfiles "UDB".

- **Monitor de Sesión**. Permite ver en tiempo real las sesiones que está realizando el usuario. Ofrece una foto instantánea de la actividad de una maquina en la red.

- **Monitor de Caminos.** Ofrece una representación en tiempo real de los caminos trazados en la red entre las diferentes máquinas que interactúan entre ellas en un intervalo de tiempo. El monitor obtiene sus datos de dos de los

monitores descritos anteriormente, el de sesiones le proporciona uno de los enlaces del momento, y el monitor de riesgo le proporciona el nivel de riesgo de cada máquina para representar cada camino con un color diferente y calcular el riesgo agregado. La monitorización se puede realizar únicamente dibujando las sesiones TCP o dibujando tanto UDP como TCP e ICMP lo que puede implicar un mapa de red enredado.

- **Monitor de Disponibilidad**. La información de disponibilidad es importante para detectar ataques de denegación de servicios. Ossim incluye el plugin "Nagios" capaz de chequear y mostrar la disponibilidad o no de servicios y equipos en la red.

- **Monitorización Personalizada**. Existe un plugin parametrizable que permite crear monitores personalizados, que extraen cualquier parámetro que se quiera recopilar, filtrar y enviar al motor de correlación para ser procesado.

Consola forense

La consola forense es un frontal Web que permite la consulta a toda la información almacenada en el colector.

Esta consola es un buscador que ataca a la base de datos de eventos "EDB", y permite al administrador analizar a posteriori y de una forma centralizada los eventos de seguridad de todos los elementos críticos de la red.

Al contrario que el monitor de riesgos, esta consola permite profundizar al máximo detalle sobre cada uno de los eventos ocurridos en el sistema.

Cuadros de mando

La última de las funcionalidades ofrecidas por Ossim es el Cuadro de Mandos, donde se podrá configurar una visión a alto nivel del estado de seguridad de la red.

El cuadro de mandos monitorizará una serie de indicadores definidos que medirán el estado de seguridad de la organización, definiendo umbrales que debe cumplir la organización.

Es la principal herramienta para saber en todo momento que ocurre en la red, mostrando la información más concisa y simple posible. A través de él se enlazara con cada una de las de monitorización para profundizar sobre cualquier problema localizado.

2.2.2.5.5 Herramientas que integra OSSIM

OSSIM incluye muchas herramientas muy útiles, que también son de código abierto y que se encuentran entre los más conocidos y utilizados para la detección de intrusiones, análisis de vulnerabilidad y supervisión y gestión de red:

- **ArpWatch:** se utiliza para la supervisión ARP tráfico en la LAN y de detección de ataques.
- **P0f:** se utiliza para el sistema operativo identificación y análisis.
- **Pads:** se utiliza para detectar anomalías de los servicios que se ejecutan en un host.
- **Nessus y OpenVas:** los más utilizados y populares escáneres de vulnerabilidad.
- **Nmap:** el más famoso y potente escáner de red.
- **Snort:** el más popular sistema de detección de intrusos (IDS).
- **Tcptrack:** utilizado para conexión TCP.
- **Nagios y Ntop:** se utiliza para supervisar el estado de la red, los hosts y la disponibilidad de los servicios.
- **Osiris y OSSEC:** software de detección de intrusiones en hosts individuales (HIDS- Host-Based IDS).
- **Snare:** un agente de software para recopilar los registros en los sistemas Windows.

Estas herramientas pueden ser:

Activas.- Generan tráfico dentro de la red en que se encuentran.

Pasivas.- Analizan el tráfico de la red sin generar tráfico dentro de ella.

Tabla N° 4: Herramientas integradas en OSSIM

HERRAMIENTA	TIPO	DEFINICIÓN Y UTILIDAD EN OSSIM
SNORT	PASIVA	NIDS (Detección de intrusos a nivel de red) Snort analiza todo el tráfico de red Mediante el uso de firmas genera eventos de seguridad Utilidad en OSSIM: - Escaneos de puertos - Gusanos - Malware -Violaciones de política (P2P,Mensajería, pornografía)
NTOP	PASIVA	Monitor de red y de uso Ntop analiza todo el tráfico de red Ntop ofrece datos (En tiempo real e histórico) del uso que estamos dando a nuestra red Utilidad en OSSIM: - Estadísticas de uso de red - Información sobre activos -Matrices de tiempo y de actividad -Información sobre sesiones activas en la red -Detección de abuso de la red
NFSEN / NFDUMP	PASIVA	NFDump recoge y procesa netflows desde la línea de comandos. NFSen es una interfaz gráfica que permite gestionar y mostrar la información recogida por NFDump. Netflows es un protocolo de red desarrollado por Cisco que permite recoger información referida al tráfico analizado Un gran número de dispositivos soportan hoy día Netflow.
OCS	ACTIVA (AGENTES)	Gestión de inventario Mediante un sistema de agentes distribuidos, se recoge información para el inventario de cada máquina. OCS requiere de un agente instalado en cada máquina a inventariar. Utilidad en OSSIM: -Gestión de inventario (Software y Hardware) -Gestión de vulnerabilidades -Violaciones de política -Control del hardware
NAGIOS	ACTIVA	Monitor de disponibilidad Nagios monitoriza la disponibilidad de los activos y servicios Podemos monitorizar un servicio de diferentes modos: (Ejemplo: Servidor MySQL) Comprobar que el equipo está levantado Comprobar que el puerto de MySQL está levantado Comprobar si en el puerto realmente escucha un servidor MySQL Realizar una consulta al servidor y comprobar el resultado Utilidad en OSSIM -Disponibilidad de los activos Nagios puede realizar comprobaciones en remoto o disponiendo de un agente en la máquina monitorizada Nagios dispone de un gran número de plugins para diferentes entornos y herramientas
OPENVAS	ACTIVA	Escaneo de vulnerabilidades OpenVas realiza escaneos de vulnerabilidades utilizando una serie de firmas Utilidad en OSSIM -Prevención de ataques -¿Se cumple la política de la organización? -Algunas vulnerabilidades solo pueden ser probadas explotando la vulnerabilidad(ejemplo: DOS)

		-OpenVas permite definir la agresividad de los escaneos que realiza -Un escaneo mal configurado puede acarrear caídas en servicios de nuestra red. Los primeros escaneos siempre deberán supervisarse con atención. -OpenVas tiene la capacidad de realizar escaneos en remoto conectándose a la maquina escaneada si le facilitamos las credenciales para ello. -De este modo OpenVas conoce exactamente el software instalado en cada máquina y si este tiene alguna vulnerabilidad o no -OpenVas dispone de un lenguaje propio de escritura de firmas.
OSVDB	ACTIVA	Base de datos de vulnerabilidades Utilidad en OSSIM: -Creación de reglas de correlación -Relaciona identificadores de cada vulnerabilidad -Completa la información ofrecida por OpenVas.
OSSEC	ACTIVA (AGENTES)	HIDS (IDS a nivel de host) OSSEC requiere de un agente instalado en cada máquina a monitorizar(Excepto sistemas UNIX) OSSEC realiza análisis de logs, comprueba la integridad del sistema, monitoriza el registro de Windows e incluye un sistema de detección de sistemas rootkit. OSSEC utiliza una arquitectura agente → servidor, en OSSIM recogeremos los eventos recolectados en el servidor de OSSEC. OSSEC dispone de su propio sistema de plugins para analizar los eventos de herramientas en Windows y UNIX. Utilidad en OSSIM -Recogida de eventos de sistemas Windows y UNIX -Recogida de eventos de aplicaciones -Monitorización de ficheros, carpetas y registros (DLP)
KISMET	PASIVA	Sniffer y detector de intrusos en redes Wireless Kismet requiere de una tarjeta WiFi que soporte el modo de monitorización raw y puede rastrear trafico 802.11b, 802.11ª y 802.11g Utilidad en OSSIM -Securización de redes inalámbricas -Detección de rogue AP -Cumplimiento de normativa (PCI)
NMAP	ACTIVA	Nmap escanea redes y equipos mediante un escaneo configurable (precisión, velocidad, grado de intrusión …) Utilidad en OSSIM -Descubrimiento de activos -Identifica puertos abiertos -Determina qué servicios se están ejecutando -Determinar qué S.O y versión se utiliza -Obtiene algunas características del hardware de red de los activos escaneados
P0F	PASIVA	Detección de anomalías en S.O A partir del análisis del tráfico generado por los activos de la red,P0f identifica el S.O que está utilizando Utilidad en OSSIM: -Cambios de S.O -Gestión de inventario -Accesos no autorizados a la red.
PADS	PASIVA	Detección de anomalías en servicios A partir del análisis del tráfico generado por los activos de la red, Pads identifica los servicios que está ejecutando cada activo Utilidad en OSSIM: -Gestión del inventario

		-Cambios en los servicios -Violaciones de política -Correlación de inventario
ARPWATCH	PASIVA	Detección de anomalías en las direcciones MAC A partir del análisis del tráfico generado por los activos de la red, Arpwatch identifica cambios en las direcciones MAC asociadas a cada dirección IP. Utilidad en OSSIM: -Gestión del inventario -Cambios de dirección IP -ARP Spoofing.
TCPTRACK	PASIVA	Monitor de sesiones(red) Tcptrack muestra información acerca de las conexiones TCP activas en la red Utilidad en OSSIM: -Información de sesiones durante la correlación
NEPENTHES	PASIVA	Honeypot Nepenthes emula servicios y vulnerabilidades conocidas con el objeto de recoger información de los atacantes (patrones de ataque, ficheros…) Utilidad en OSSIM: -Conocer que equipos están infectados -Creación de firmas y directivas en base a los ataques identificados -Colección de malware

Fuente: (Lorenzo, 2010)

2.2.2.5.6 Flujo de datos

Para entender la integración de cada uno de las herramientas se va a describir el proceso desde la generación de un evento.

La siguiente figura, muestra el flujo de los datos del sistema. Posteriormente se definen paso a paso la secuencia de los eventos

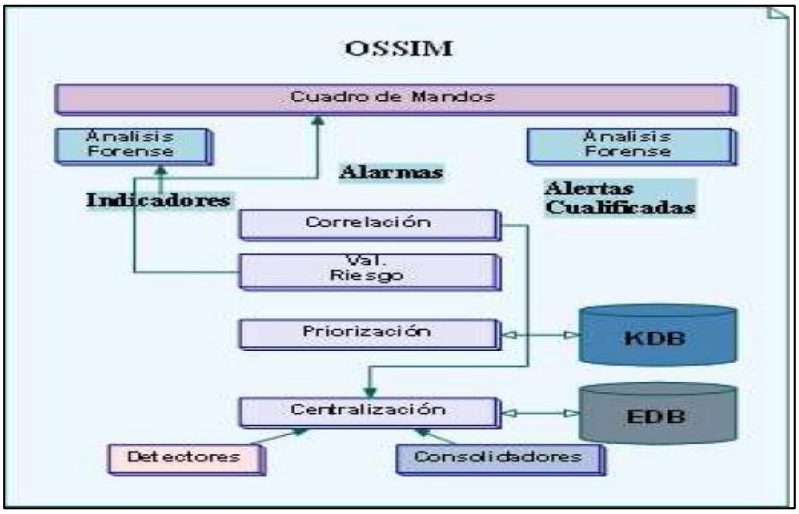


Figura N° 23. Flujo de datos OSSIM
Fuente: (Giménez García, 2008).

1. Los eventos son generados por los detectores o monitores, ya sea por la detección de un patrón o una anomalía.

2. Los eventos son procesados en caso necesario por los consolidadores antes de ser enviados (encargados de enviar la información agrupada para ocupar el mínimo ancho de banda).

3. Los eventos son recibidos por el colector a través de diferentes protocolos abiertos de comunicación.

4. El parser se encarga de normalizarlas y guardarlas si procede en la base de datos de eventos "EDB".

5. El parser se encarga de cualificar los eventos determinando su prioridad según la política de seguridad definida y los datos sobre el sistema atacado localizados en el inventario de sistemas.

6. El parser valora el riesgo instantáneo que implica la alerta y en caso de ser necesario envía una alarma al Cuadro de Mandos.

7. Los eventos son procesados por el motor de correlación para generar alarmas, que a su vez lanzará nuevos eventos con una información más completa y fiable al parser.

8. El monitor de riesgos visualizará la situación de cada uno de los índices de riesgo según han sido calculados por el algoritmo CALM.

9. El cuadro de mandos mostrará las alarmas más recientes.

10. El administrador podrá desde el cuadro de mandos enlazar y visualizar a través de la consola forense todos los eventos ocurridos en el momento de la alarma.

11. Podrá además comprobar el estado instantáneo de la máquina a través de los monitores de uso, perfiles y sesiones.

2.2.2.5.7 Uso de OSSIM en una empresa distribuida

Cuando OSSIM se implementa en una empresa distribuida es necesario colocar agentes OSSIM en diferentes lugares de toda la empresa. Muchos de estos sensores tienen que ser instalados en host que ejecutan algún tipo de software de monitoreo/sensor como Nagios, donde los otros pueden ser genéricamente instalados sobre host de sensor dedicadas (Karg, 2006).

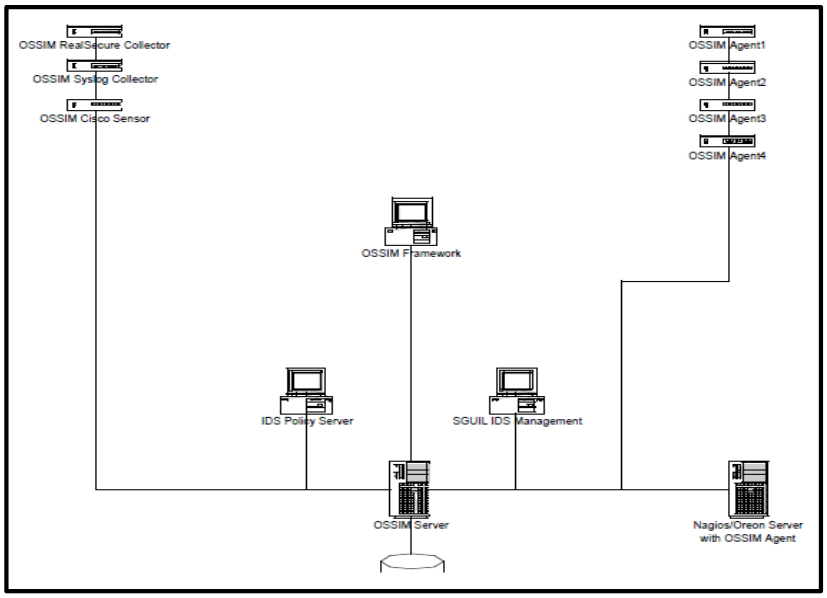


Figura N° 24. OSSIM Infrastructure
Fuente: (Karg, 2006).

Los agentes OSSIM se dividen en dos grupos:

Agente de Especialidad: es un agente que es instalado sólo para cumplir con el objetivo de recoger los datos.

Los agentes de especialidad son:

- Realsecure Collector
- Syslog Collector (servidor)
- Cisco Collector
- Nagios Collector
- Ntsyslog Collector
- IIS Collector
- Apache Collector

Agente genérico: el agente genérico es un tipo de agente que puede instalarse en su propio servidor y distribuido en toda la empresa. Este agente incluye los siguientes:

- Snort
- TcpTrack
- P0f
- Pads
- RRD
- Ntop
- Arpwatch
- Nessus
- Nmap
- Syslog (local)

2.2.2.5.8 Cumplimiento de las normas de seguridad

De acuerdo a Araújo da Silva, Magalhães Silva, & Serique Junior (2012) el sistema OSSIM tiene un módulo de cumplimiento de normas de seguridad de la información como son:

- **SOx:** Ley estadounidense que responsabiliza a la dirección de la empresa por la mala administración, destaca el papel fundamental de control interno que es un proceso dirigido por la Junta Directiva y el Consejo de administración.

- **PCI-DSS:** Requisitos de seguridad para la empresa con transacciones financieras a través de tarjeta, describe los 12 requisitos del patrón de seguridad de datos para el sector de tarjetas de pago.

- **ISO 27001:** Requisitos de seguridad para implementar un SGSI; recomienda establecer, implementar, operar, monitorear, analizar críticamente, mantener y mejorar un Sistema de Seguridad de Información.

- **ISO 27002:** código de prácticas para la gestión de la seguridad información, establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización.

2.2.2.6 Gestión de la seguridad a través de métricas e indicadores

"Lo que no puede ser medido no puede ser gestionado". La necesidad de gestionar la seguridad de los sistemas de información obliga a la utilización de métricas e indicadores que permitan evaluar la situación real. Las métricas seguridad son necesarias para saber el estado de un sistema de información y tienen por finalidad conocer, evaluar y gestionar la seguridad de los sistemas de información. Si una organización no usa métricas de seguridad para la toma de decisiones, las elecciones serán motivadas por aspectos puramente subjetivos, presiones externas o por motivaciones puramente comerciales (Sanchez, Luis & Piattini, Mario, 2015).

El empleo de métricas para medir, monitorear y reportar la efectividad y eficiencia de los controles de seguridad de información, así como las políticas se seguridad de información es una tarea continua que debe ser desarrollada por el administrador de seguridad de información en una organización. Por lo expuesto, la herramienta más efectiva para gestionar el programa de seguridad es el empleo de métricas. El administrador de seguridad de información debe contar con una metodología formal para medir la efectividad del programa de seguridad.

En el diseño de métricas, una buena base debe ser establecida. Las buenas métricas deben ser específicas, medibles, alcanzables, repetitivas y dependientes del tiempo. Luego las métricas pueden ser usadas para medir el progreso (Villena, 2006).

Las métricas de seguridad facilitan el cumplimiento de los objetivos, cuantificando la implantación de los controles de seguridad y la eficacia y eficiencia de los mismos, analizando la adecuación de los procesos de seguridad e identificando posibles acciones de mejora. Las métricas deben proporcionar información cuantitativa (porcentajes, medias, números).

Los procesos de definición de métricas deben tener en cuenta la naturaleza del negocio y organización para poder adecuarse a cada tipo de negocio. En la definición de métricas es habitual encontrarse con numerosos problemas, siendo los más relevantes los siguientes:

- Las métricas no están definidas en un contexto donde el objetivo o interés industrial que se pretende alcanzar mediante su utilización es explícito.
- En ocasiones, aunque el objetivo sea explícito, las hipótesis experimentales a menudo no están hechas de forma explícita.
- Las definiciones de métricas no siempre tienen en cuenta el entorno o el contexto en el cual serán aplicadas.

- A menudo, no es posible realizar una adecuada validación teórica de las métricas porque el atributo que una métrica pretende cuantificar no está bien definido.
- Un gran número de métricas no han sido nunca el objeto de validación empírica.
- (Sanchez, Luis & Piattini, Mario, 2015)

Hablando sobre las características que deberían cumplir los indicadores, así como las métricas de seguridad, Sanchez, Luis & Piattini, Mario (2015), resumen los siguientes puntos:

- Establecer los objetivos de las métricas automatizables para desarrollar una herramienta eficaz y óptima en su aplicación.
- Filtrar la selección de los indicadores a aplicar de acuerdo a su nivel en el ciclo de nuestro modelo en espiral, reflejando el nivel a partir del que se puede aplicar la métrica.
- Evaluación del impacto del proceso de obtención del valor del indicador en la organización, analizando las áreas funcionales de la organización y evaluando la aplicación de las métricas adecuadas a cada una.
- Optimización de costos temporales y económicos de los procesos de aplicación de nuestro modelo de madurez.

2.2.2.6.1 Framework COBIT

COBIT son las siglas para definir Control Objectives for Information and Related Technology (Objetivos de Control para la información y tecnología relacionada), el cual es un marco de referencia creado por ISACA (Information Systems Audit and Control Association) (Asociación de Control y Auditoria de Sistemas de Información) para la gestión de la TI y el Gobierno de TI. Es un conjunto de herramientas de soporte que permite a la gerencia de las organizaciones el cerrar la brecha entre los requerimientos de control, problemas técnicos y los riesgos del negocio (Martínez Estébanes & García Cano, 2011).

En Pasquini & Galiè (2013) encontramos que ISACA fue fundada en 1967, por un grupo de industrias individuales que trabajaban en el mismo campo. En 1969 se incorporaron como Electronic Data Processing (EDP) Auditors Association. Los miembros de ISACA trabajaron juntos para desarrollar y crear mejores prácticas, una de ellas fue el marco COBIT. La primera versión de este marco fue lanzado en 1996 y fue llamado "Objetivos de Control para Información y Tecnologías Relacionadas", que cubre el área de auditoría. La segunda edición con mejoras en

materia de evaluación de control fue lanzado en 1998. La tercera edición fue liberada dos años más tarde, y de acuerdo con (Kadam, 2012)"El gran cambio se produjo con la publicación de la tercera edición de COBIT, con su orientación hacia los objetivos de negocio. En este tiempo, COBIT se denominaba como un marco de gestión de TI. La tercera edición identificó que una organización necesitaba de TI no sólo para el procesamiento de la información, sino también para lograr objetivos del negocio". En 2005 ISACA introdujo la cuarta versión de COBIT, con un enfoque sobre la gobernanza de TI. Una versión más de este marco es COBIT 4.1, lanzado en 2007, versión que tuvo la aceptación por ser congruente y podía hibridarse con otros marcos como: IT Infrastructure Library (ITIL), la serie ISO 27000 y Capability Maturity Model® Integration (CMMI). La versión actual del marco, COBIT 5, fue lanzada en 2012. Se basa en la versión anterior del marco y dos marcos complementarios de ISACA, como son Val IT y Risk IT; y está alineado con las mejores prácticas actuales, tales como ITIL y TOGAF.

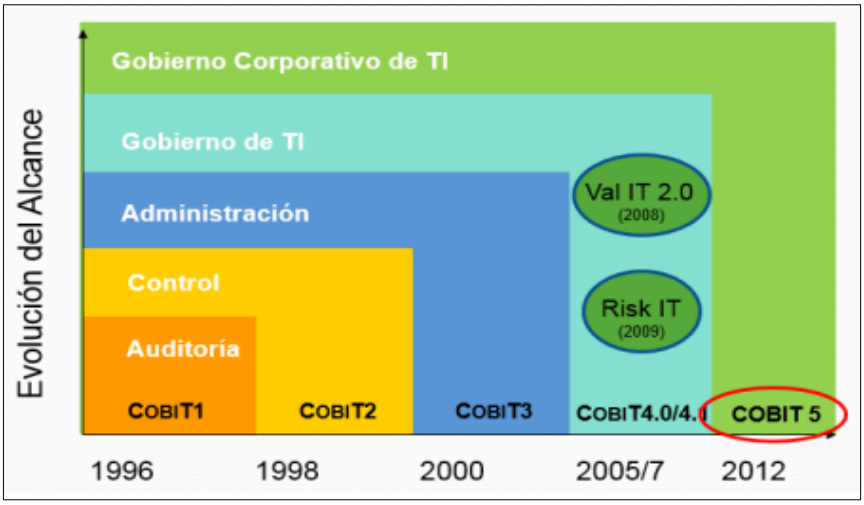


Figura N° 25. Evolución del marco de referencia COBIT
Fuente: (ISACA, 2012) (Mera Balseca, 2014).

Sheikhpour & Modiri (2012) mencionan que los Administradores, auditores, y los usuarios se benefician del desarrollo de COBIT porque ayuda a entender sus sistemas de TI y decidir el nivel de seguridad y control que es necesario para proteger sus activos de la organización a través del desarrollo de un modelo de gobernanza. COBIT puede ser ampliamente aplicado a diversos fines. COBIT abarca la seguridad además de todos los otros riesgos que pueden ocurrir con el uso de las TI.

2.2.2.6.2 COBIT 5.0

COBIT 5 ayuda a las empresas a crear valor óptimo de TI el mantenimiento de un equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y el uso de recursos (Alramahi, Barakat, & Haddad, 2014).

Proporciona un modelo de referencia de procesos de gobernanza y gestión de TI. Además COBIT 5 ha sido alineado y armonizado con otros estándares y mejores prácticas y actúa como un integrador de todos estos materiales guía, resumiendo los objetivos clave bajo un mismo marco de trabajo integral que también se alinea con los requerimientos de gobernanza y de negocios (Carrillo Verdún & Rubio Casallas, 2012).

Solares Soto (2014) comenta que COBIT 5.0 es un marco de referencia único e integrado porque:

- Se alinea con otros estándares y marcos de referencia lo que permite usarlo como el marco integrador general de gestión y gobierno.
- Es completo en la cobertura de la empresa, ofreciendo una base para integrar de manera efectiva otros marcos, estándares y prácticas utilizadas.
- Proporciona una arquitectura simple para estructurar los materiales de guía y producir un conjunto consistente.
- Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA.

En la misma fuente encontramos COBIT 5 tiene la característica de ser adaptado a todos los modelos de negocio, entornos tecnológicos, sectores, geografías y culturas corporativas y que es factible de aplicarse a:

- La seguridad de la información.
- La gestión del riesgo.
- El gobierno corporativo y la gestión de las TI de la empresa.
- Las actividades de revisión y garantía.
- La conformidad legal y regulatoria.
- El tratamiento de datos financieros o de información sobre RSC

Según Ramírez Castro (2012) COBIT 5 toma la gestión de riesgos como un objetivo de gobernanza para la creación de valor, buscando la optimización de riesgos, haciendo el mapeo de estos junto a la optimización de recursos y el realce

de beneficios a las metas organizacionales de información y tecnología. La finalidad es cumplir con procesos, capacidad en servicios, habilidades, competencias, principios y políticas, información, estructura organizacional, además del ambiente ético y cultural requerido.

Objetivos

De acuerdo con ISACA (2012) las empresas existen para crear valor para sus accionistas. En consecuencia, cualquier empresa, comercial o no, tendrá como objetivo de Gobierno la creación de valor. Creación de valor significa conseguir beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo. La Figura N° 26 muestra esta propuesta. Los beneficios pueden tomar muchas formas, como financieros para las empresas comerciales o de servicio público para entidades gubernamentales.

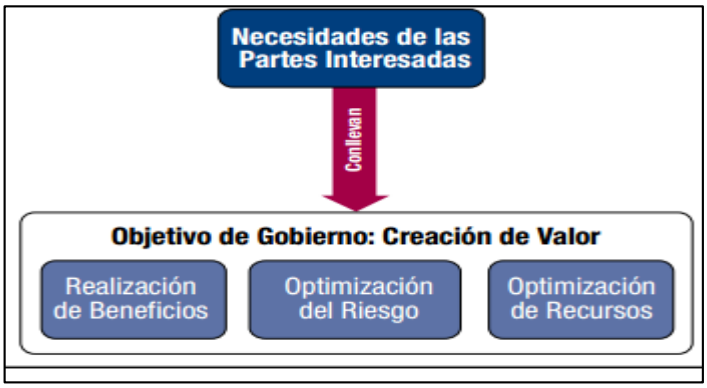


Figura N° 26. El objetivo de Gobierno " Creación de valor"
Fuente: (ISACA, 2012).

Las empresas tienen muchas partes interesadas, y 'crear valor' significa cosas diferentes y a veces contradictorias para cada uno de ellos. Las actividades de gobierno tratan sobre negociar y decidir entre los diferentes intereses en el valor de las partes interesadas. En consecuencia, el sistema de gobierno debe considerar a todas las partes interesadas al tomar decisiones sobre beneficios, evaluación de riesgos y recursos. Para cada decisión, las siguientes preguntas pueden y deben hacerse: ¿Para quién son los beneficios? ¿Quién asume el riesgo? ¿Qué recursos se requieren?

Cascada de metas

En los comentarios de **Francavilla (2014)** encontramos que la cascada de metas de COBIT 5, traslada las necesidades de los interesados en:

- Objetivos específicos
- Acciones concretas y personalizadas dentro del contexto de la empresa
- Objetivos relacionados de TI
- Objetivos facilitadores o activadores de las metas.

Figura N° 27. Visión General de la Cascada de Metas de COBIT 5
Fuente: (ISACA, 2012).

Catalizadores

Los catalizadores son factores que, individual y colectivamente, influyen sobre si algo funcionará – en este caso, el gobierno y la gestión de la empresa TI. Los catalizadores son guiados por la cascada de metas, es decir, objetivos de alto nivel relacionados con TI definen lo que los diferentes catalizadores deberían conseguir. El marco de referencia COBIT 5 describe siete categorías de catalizadores:

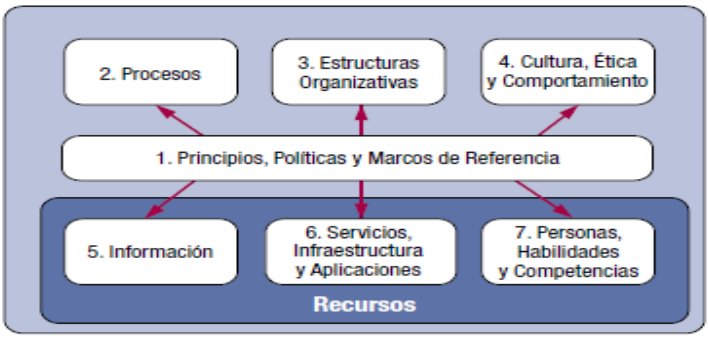


Figura N° 28. Catalizadores Corporativos COBIT 5
Fuente: (ISACA, 2012).

- Principios, políticas y marcos de referencia son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.
- Los procesos describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.
- Las estructuras organizativas son las entidades de toma de decisiones clave en una organización.
- La Cultura, ética y comportamiento de los individuos y de la empresa son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.
- La información impregna toda la organización e incluye toda la información producida y utilizada por la empresa. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.
- Los servicios, infraestructuras y aplicaciones incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.
- Las personas, habilidades y competencias están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctiva.
- Algunos de los catalizadores definidos previamente son también recursos corporativos que también necesitan ser gestionados y gobernados. Esto aplica a:
- La información, que necesita ser gestionada como un recurso. Alguna información, tal como informes de gestión y de inteligencia de negocio son importantes catalizadores para el gobierno y la gestión de la empresa.
- Servicios, infraestructura y aplicaciones.
- Personas, habilidades y competencias.

Todos los catalizadores tienen un conjunto de dimensiones comunes. Este conjunto de dimensiones comunes (figura N° 29):

- Proporciona una manera común, simple y estructurada de tratar con los catalizadores
- Permite a una entidad manejar sus complejas interacciones

- Facilita resultados exitosos de los catalizadores

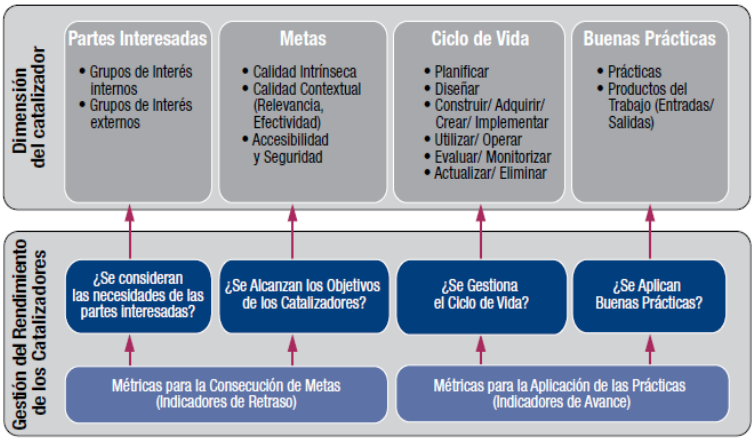


Figura N° 29. Catalizadores COBIT 5: Genéricos
Fuente: (ISACA, 2012).

Procesos

Una empresa puede organizar sus procesos como crea conveniente, siempre y cuando las metas de gobierno y gestión queden cubiertas. Empresas más pequeñas pueden tener pocos procesos; empresas más grandes y complejas pueden tener numerosos procesos, pero todos con el ánimo de cubrir las mismas metas.

COBIT 5 incluye un *modelo de referencia de procesos* que define y describe en detalle varios procesos de gobierno y de gestión. Dicho modelo representa todos los procesos que normalmente encontramos en una empresa relacionados con las actividades de TI, proporciona un modelo de referencia común entendible para las operaciones de TI y los responsables de negocio. El modelo de proceso propuesto es un modelo completo e integral, pero no constituye el único modelo de procesos posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación particular.

La incorporación de un modelo operacional y un lenguaje común para todas las partes de la empresa involucradas en las actividades de TI, es uno de los pasos más importantes y críticos hacia el buen gobierno. Adicionalmente proporciona un marco para medir y vigilar el rendimiento de TI, proporcionar garantía de TI, comunicarse con los proveedores de servicio e integrar las mejores prácticas de gestión.

Según ISACA (2012), de los procesos del modelo de referencia COBIT, los que serán tomados en cuenta en la presente investigación son los que a continuación se detallan:

Gestionar la Disponibilidad y la Capacidad (BAI04)

Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados. Dentro de sus metas de TI figuran: *la entrega de servicios de TI de acuerdo a los requisitos del negocio, la optimización de activos, recursos y capacidades de TI y la disponibilidad de información útil y relevante para la toma de decisiones*.

Gestionar los Activos (BAI09)

Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia. Dentro de sus metas de TI figuran: *la transparencia de los costos, beneficios y riesgo de las TI y la optimización de activos, recursos y capacidades de TI*.

Gestionar la Configuración (BAI10)

Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoria de la información de configuración y la actualización del repositorio de configuración. Dentro de sus metas de TI figuran: *el cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas, la optimización de activos, recursos y capacidades de TI y la disponibilidad de información útil y relevante para la toma de decisiones*.

Gestionar las Operaciones (DSS01)

Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas. Dentro de sus metas de TI figuran: *los riesgos de negocio relacionados con las TI gestionados, la entrega de TI de acuerdo a los requisitos del negocio y la optimización de activos recursos y capacidades de TI*.

Gestionar las Peticiones y los Incidentes de Seguridad (DSS02)

Proponer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal, registrar y completar las peticiones de usuario y registrar, investigar, diagnosticar, escalar y resolver incidentes. Dentro de sus metas de TI figuran: *los riesgos de negocio relacionados con las TI gestionados y la entrega de servicios de TI de acuerdo a los requisitos del negocio*.

Gestionar Servicios de Seguridad (DSS05)

Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad. Dentro de las metas de TI figuran: *el cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas, los riesgos de negocio relacionados con las TI gestionados y la seguridad de la información, infraestructura de procesamiento y aplicaciones*.

2.2.3 Glosario

Como parte de la situación problemática y la solución se definen los siguientes conceptos.

- **Activo. -** Es todo aquello que posea valor para la organización, por tanto, debe protegerse. Ejemplo: Información física y digital, Software, Hardware, Servicios de información, Servicios de Comunicaciones, Servicios de almacenamiento, Personas.

- **Amenaza**. - Evento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos.

- **COBIT**. - Objetivos de Control para Tecnologías de Información o Relacionadas es un marco completo, internacionalmente aceptado, para el gobierno y la gestión de la información de la empresa y la tecnología de la información (TI) que soporta a los ejecutivos de la empresa y los gestores en la definición y consecución de las metas de negocio y las metas de TI relacionadas.

- **Confidencialidad**. - Se refiere a tener la información restringida a aquellos sujetos que no tiene autorización, solo para usuarios definidos por la dirección de la empresa tendrán acceso.

- **Correlación**. - identifica posibles amenazas potenciales de seguridad mediante la detección de patrones de comportamiento que ocurren en diferentes tipos de control de activos.

- **Creación de valor. -** El objetivo principal del gobierno de una empresa, conseguido cuando los tres objetivos subyacentes (consecución de beneficios, optimización de riesgo y optimización de recursos) están en equilibrio

- **Cuadrante mágico de Gartner. -** Dichos cuadros son una invención de la consultora Gartner que investiga exclusivamente las industrias de las TI, analiza las tendencias de mercado y elabora el ranking de soluciones tecnológicas para facilitar la selección de soluciones y productos. El cuadrante mágico le ayuda a determinar rápidamente cómo los proveedores de tecnología están ejecutando sus visiones indicados y qué tan bien lo está realizando contra la visión de mercado de Gartner.

- **Disponibilidad. -** Es muy importante que la información de los sistemas esté disponible en cualquier momento que lo necesiten los usuarios designados o procesos autorizados.

- **Empresa distribuida. -** Una empresa distribuida es aquella que organiza el trabajo de sus miembros de manera que pueda ser realizado a distancia. Es decir, una empresa distribuida podría tener decenas de miembros, distribuidos por todo el mundo (y quizás sin conocerse personalmente entre ellos) y aun así funcionar correcta y exitosamente**.**

- **IDS. -** Sistema de detección de intrusos es una herramienta de software que monitorea el tráfico de una red y los sistemas de una organización en busca de señales de

intrusión, actividades de usuarios no autorizados y la ocurrencia de malas prácticas, como en el caso de los usuarios autorizados que intentan sobrepasar sus límites de restricción de acceso a la información.

- **Integridad. -** Para la empresa es muy importante que su información se mantenga sin modificación y que las personas que estén autorizados para hacerlo trabajen bajo estrictas normas de operación

- **Open Source. -** Software de código abierto es software cuyo código fuente está disponible para la modificación o mejora por cualquier persona.

- **OSSIM**. - Gestión de la Seguridad de la Información Open Source es una colección de herramientas bajo la licencia GPL, diseñadas para ayudar a los administradores de red en la seguridad de las computadoras, detección de intrusos y prevención.

- **Parte interesada. -** Cualquiera que tiene una responsabilidad, expectativa o cualquier otro interés en la empresa –por ejemplo, accionistas, usuarios, el gobierno, proveedores, clientes y el público en general.

- **Plugin. -** es un software de complemento que se instala en un programa, lo que le permite realizar funciones adicionales.

- **Política de seguridad. -** Conjunto de directivas y normas emitidas por la gerencia que escriben los objetivos de la organización respecto a la protección de sus activos de información.

- **Riesgo. -** Posibilidad de que una amenaza se materialice.

- **Seguridad de la información. -** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

- **SEM. -** Gestión de eventos de seguridad realiza la monitorización y la gestión de eventos a tiempo real. Recoge información de todos los sistemas y los equipos a tiempo real. Mediante un monitor se puede visualizar, monitorizar y gestionar los eventos utilizando reglas para detectar situaciones anómalas.

- **SIEM. -** Gestión de Información y Eventos de Seguridad es un sistema que ofrece una funcionalidad añadida a SIM y SEM, es decir, recoge los registros de actividad de todos los dispositivos a largo plazo y agregan en tiempo real toda la información que ha sido recibida para facilitar la detección y actuación sobre los eventos, generando alertas, respuestas automáticas, informes, etc.

- **SIM. -** Gestión de la Información de Seguridad es un sistema de supervisión que persigue la función de recolección, correlación y análisis de la información de seguridad, por lo que se generan documentos que están adjuntos a los datos que se han obtenido de los dispositivos supervisados.

CAPÍTULO 3. DESARROLLO DEL MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: OSSIM-COBIT

SECCION A: Análisis del caso de estudio.

La presente sección, está enfocada en explicar el entorno del caso de estudio relacionado con el campo de la gestión de la seguridad de la información. Se describirá la situación actual, los servicios brindados y las normas o políticas que regulan dichos servicios. Se analizarán algunas herramientas de gestión actuales, así como la forma en la que se toman las decisiones en el entorno universitario según los lineamientos actuales.

3.1 Situación actual del caso de estudio

De acuerdo a su sitio oficial en internet[4], la Universidad Nacional Pedro Ruiz Gallo (UNPRG), es una organización académico-administrativa, orientada a la formación personal y académica integral, que gestiona la cultura y el conocimiento de acuerdo a las exigencias de la globalización. Se considera, además, una comunidad integrada por docentes, estudiantes y graduados, inspirada en principios científicos, democráticos y éticos. Brinda una formación integral, centrada en la investigación, docencia, extensión cultural y proyección social; en base al Modelo de Gestión por Procesos, que orienta el desarrollo de competencias, para estimular un desempeño eficiente en los mundos profesional, académico, laboral e investigativo.

Por otro lado, la Universidad Nacional Pedro Ruiz Gallo, cuenta con un órgano de apoyo a la Alta Dirección: La Oficina General de Sistemas Informáticos (OGSI), cuyo objetivo es brindar servicios de procesamiento de información a los órganos internos de la Universidad.
Según el estatuto vigente, aprobado con fecha del 8 de febrero de 2017, la Oficina General de Sistemas Informáticos es el órgano encargado de gestionar los sistemas informáticos académicos, investigativos y administración de la universidad.
Dentro de su misión se incluyen: Planificar, desarrollar, evaluar y dar soporte técnico a los servicios tanto académicos como administrativos que se dan en todas las dependencias de la universidad, utilizando tecnologías de la información y comunicaciones (TICs) para el logro de los objetivos buscados por la Alta Dirección, dentro del Plan Estratégico Institucional.

[4] Sitio oficial en internet: www.unprg.edu.pe

Tal como se especificó en el capítulo 1, las principales funciones de la Oficina General de Sistemas Informáticos se cuentan las siguientes:

- Diseñar, planificar, ejecutar, actualizar y supervisar los procesos informáticos académicos, administrativos y de investigación de la Universidad.
- Desarrollar, actualizar y mantener el software y el hardware institucional.
- Asesorar a las diferentes dependencias en asuntos de sistemas informáticos y de comunicación.
- Apoyar las actividades de actualización institucional en el avance de las tecnologías de información y la comunicación (TICs).
- Prestar servicios a terceros, funcionando en este caso como un órgano generador de ingresos propios.

Además, cuenta con servicios considerados principales, dentro de los que figuran: servicios web, de correo, FTP (servidores de archivos), SIAF (Sistema Integrado de Administración Financiera) del MEF, GESTAC, SIGA (Sistema integrado de Gestión Académica), Sistema de Proyección Social, Sistema de Biblioteca, Sistema de Investigación, Sistema de Personal, Sistema de Tesorería, Sistema de Presupuesto, Sistema de Trámite Documentario, Sistema de Abastecimiento y Almacén, etc.; así como otros considerados secundarios: Telefonía por Voz IP, Aula Virtual, Blog de docentes universitarios, bolsa de empleo, etc.

Esta diversidad de servicios se fusiona con el crecimiento continuo de la infraestructura tecnológica de la universidad y con los grandes volúmenes de información sensible manejados diariamente, que hacen que la gestión de la seguridad de la información sea un pilar fundamental en el total monitoreo de toda la Red. Pero, ¿sobre qué estructura tecnológica se soportan todas ellas?

3.2 Análisis de la infraestructura de la red de comunicación de datos

La infraestructura de red Telemática se soporta sobre los siguientes componentes:

- Sistema de cableado estructurado con backbone de fibra óptica bajo el estándar 802.3ae con un soporte de tasa de transferencia máxima de 10Gbps y subsistema de cableado horizontal con medio de transmisión que soporta 1Gbps en la capa de acceso, cumpliendo los estándares internacionales para sistemas de cableado estructurado, lo que garantiza el uso de múltiples aplicaciones sobre la misma infraestructura de telecomunicaciones.
- Sistema activo de comunicaciones, con tecnología de conmutación de datos distribuida en un sistema jerárquico en 2 capas preparada para actualizarse a 3 capas. Implementan una

red escalable y con capacidades de redundancia, disponibilidad y administración. No utiliza el 100% de la capacidad de tráfico que puede soportar los enlaces inalámbricos con 3 dependencias importantes externas al Campus Universitario, son de banda ancha.

- Sistema Activo de comunicaciones con equipos de enrutamiento de alta confiabilidad, redundancia, disponibilidad y administración.

- Sistema de seguridad con hardware y software de protección en la frontera de la red pública y privada, así como la disponibilidad de herramientas de seguridad en todos los niveles del modelo de red TCP/IP de la red privada de la Universidad.

- Data Center con capacidad de soportar hardware de servidores adicional para el procesamiento y almacenamiento de nuevas aplicaciones.

- Sistemas de refrigeración y control de temperatura, protección y sistema de suministro eléctrico con backups de UPS's y generador de energía en condiciones operativas.

- Personal técnico capacitado y dedicado a la administración permanente de la red de comunicación IP.

Para un análisis detallado de los equipos de comunicación existentes en la Red Telemática, consulte el Apéndice A.
En dicha sección, se describen los equipos que conforman el gabinete de servidores y el gabinete de comunicaciones con algunas de sus especificaciones técnicas de acuerdo a la situación real.

3.3 Análisis de las herramientas de monitorización actuales

En la actualidad, la monitorización de la infraestructura de red se realiza a nivel de hardware dedicado (CISCO IDS, CISCO PIX) y de algunas herramientas Open Source implementadas, que si bien es cierto proporcionan un grado razonable de seguridad de la información, estas se encuentran aisladas y trabajando de forma independiente, lo que hace que la administración sea tediosa y muchas veces confusa (debido al gran caudal de información de reportería). La toma de decisiones en estas circunstancias se torna engorrosa y afecta considerablemente a los principales procesos que brinda la universidad como: matriculas, registro de notas, admisión, etc.

3.4 Selección de entorno aislado para pruebas

Debido a la complejidad de la infraestructura tecnológica de toda la universidad y de acuerdo a los objetivos propuestos en la presente investigación, creemos conveniente seleccionar solo un tramo de red y crear un entorno cerrado y controlado de monitorización mediante OSSIM y todas sus herramientas integradas.

La selección del tramo de red, cumple con los requerimientos de hardware y software apropiados (según las especificaciones técnicas de OSSIM) para la correcta implementación de la primera prueba piloto. Este tramo, fue seleccionado y aprobado por el administrador de la Red, quien hizo seguimiento de todo el proceso y analizó, junto con los autores de la presente investigación, toda la información recopilada, filtrada y analizada con el fin de tomar las primeras decisiones importantes de seguridad en base a políticas y normas establecidas teniendo como marco de referencia lo propuesto por COBIT 5. Todos estos puntos, se analizarán con detalle en los capítulos siguientes.

A continuación, se muestra el diseño de red seleccionado para la presente investigación:

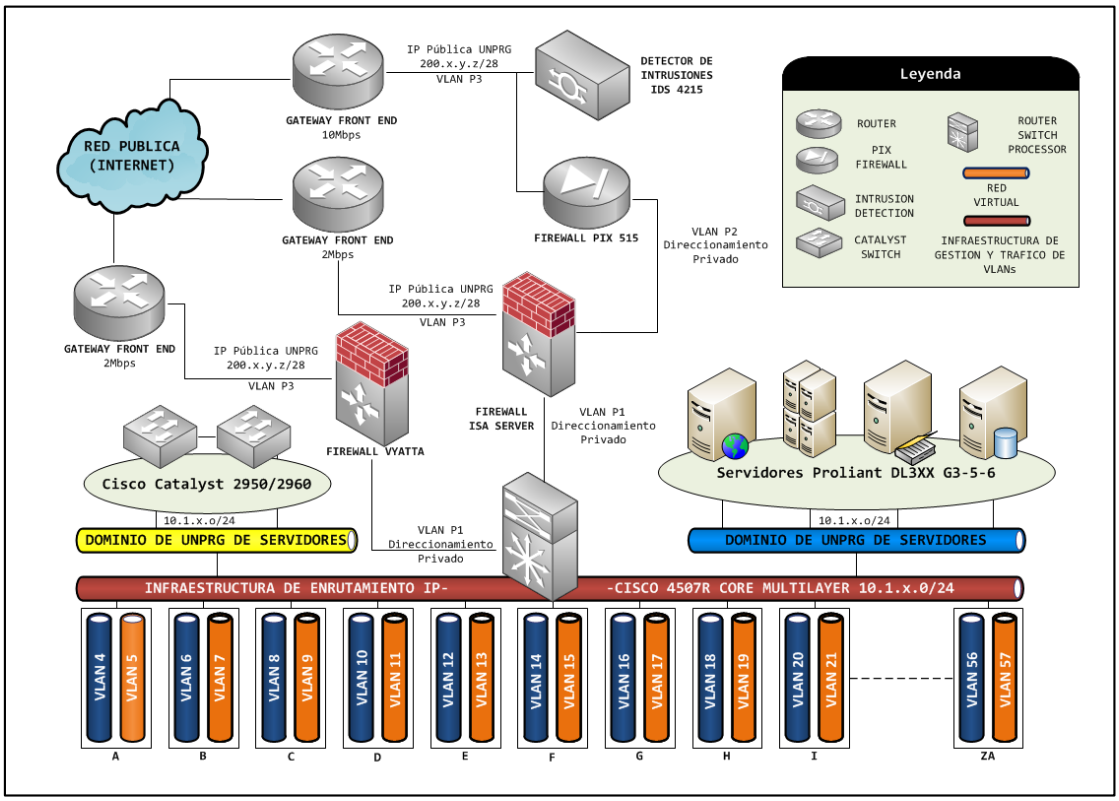


Figura N° 30. Diseño de red para la presente investigación

SECCION B: Identificación de objetivos e indicadores según COBIT

Esta sección desarrollará el mapeo de los objetivos que persigue nuestro caso de estudio con la relación de los objetivos propuestos por el marco de referencia COBIT 5.0, con el propósito de aplicar la cascada de metas de COBIT y determinar los objetivos de control de TI relacionados, así como sus procesos habilitadores alineados de acuerdo a nuestro modelo.

3.5 Mapeo de objetivos: caso de estudio - COBIT 5.0

A continuación, se muestran los objetivos organizacionales para el caso de estudio. Es importante mencionar, que estos han sido definidos y aprobados teniendo en cuenta las normas y políticas internas de la Universidad Nacional Pedro Ruiz Gallo, así como de los objetivos internos que define y persigue el Área de Red Telemática para el desarrollo de sus funciones.

OBJETIVO A: Lograr una expansión estratégica de los procesos de la universidad.
OBJETIVO B: Lograr el reconocimiento a la excelencia en cuanto a la atención y servicios brindados en la universidad.
OBJETIVO C: Asegurar el cumplimiento de las políticas y normas internas.
OBJETIVO D: Asegurar el cumplimiento de las políticas y normas externas que rijan los procesos de TI aplicados.
OBJETIVO E: Asegurar la optimización y funcionalidad de los procesos implementados en la universidad.
OBJETIVO F: Asegurar el resguardo de los activos mediante la gestión de riesgos.
OBJETIVO G: Mantener la continuidad y disponibilidad de los servicios brindados.
OBJETIVO H: Tomas de decisiones estratégicas en base a información confiable.
OBJETIVO I: Asegurar la capacitación al personal para el logro de los objetivos establecidos.

Definiendo lo anterior, se procede a mapear los objetivos del caso de estudio con los objetivos de control propuestos por COBIT 5, logrando una adaptación efectiva:

Tabla N° 5: Correspondencia entre los objetivos de la organización y los objetivos propuestos por COBIT

OBJETIVOS DEL CASO DE ESTUDIO	OBJETIVOS DE COBIT 5.0
OBJETIVO A	Cartera de productos y servicios competitivos.
OBJETIVO B	Cultura de servicio orientada al cliente.
OBJETIVO C	Cumplimiento con las políticas internas.
OBJETIVO D	Cumplimiento de leyes y regulaciones externas.
OBJETIVO E	Optimización de la funcionalidad de los procesos de negocio.
OBJETIVO F	Riesgos de negocio gestionados (salvaguarda de activo).
OBJETIVO G	Continuidad y disponibilidad del servicio de negocio.
OBJETIVO H	Toma estratégica de Decisiones basadas en información.
OBJETIVO I	Personas preparadas y motivadas.

Fuente: Los autores

El resumen de los objetivos mapeados se define a continuación:

Tabla N° 6: Cuadro resumen de los objetivos mapeados

OBJETIVOS DEL CASO DE ESTUDIO	OBJETIVOS DE COBIT 5.0
Lograr una expansión estratégica de los procesos de la universidad.	Cartera de productos y servicios competitivos.
Lograr el reconocimiento a la excelencia en cuanto a la atención y servicios brindados en la universidad	Cultura de servicio orientada al cliente.
Asegurar el cumplimiento de las políticas y normas internas.	Cumplimiento con las políticas internas.
Asegurar el cumplimiento de las políticas y normas externas que rijan los procesos de TI aplicados.	Cumplimiento de leyes y regulaciones externas.
Asegurar la optimización y funcionalidad de los procesos implementados en la universidad.	Optimización de la funcionalidad de los procesos de negocio.
Asegurar el resguardo de los activos mediante la gestión de riesgos.	Riesgos de negocio gestionados (salvaguarda de activo).
Mantener la continuidad y disponibilidad de los servicios brindados.	Continuidad y disponibilidad del servicio de negocio.
Tomas decisiones estratégicas en base a información confiable.	Toma estratégica de Decisiones basadas en información.
Asegurar la capacitación al personal para el logro de los objetivos establecidos.	Personas preparadas y motivadas.

Fuente: Los autores

3.5.1 Justificación del mapeo: Objetivo Organizacional – Objetivo de TI/COBIT

Objetivo "A" a objetivo 2

Tal como refiere el primer objetivo, es importante la expansión estratégica mediante el uso de TI para el beneficio de la gestión de la información, así como para los usuarios finales. De acuerdo a COBIT, mantener un portafolio de servicios competitivos logrará un alto nivel estratégico.

Objetivo "B" a objetivo 6

El reconocimiento por la excelencia de los servicios brindados es otro de los objetivos principales de la universidad de ahí que la cultura organizacional, propuesta por COBIT, se oriente al cliente con la entrega de mejores servicios. Por lo tanto, existe una relación directa.

Objetivo "C" a objetivo 15

Pensando en que el cumplimiento de las políticas internas de TI da como resultado que estas sean respetadas y reconocidas, se ve la necesidad de asegurar su aplicación comprometiendo a toda la organización a fin de tomar decisiones acordes con ellas. Este objetivo es abarcado por COBIT y su relación es directa.

Objetivo "D" a objetivo 4

El cumplimiento regulatorio de las políticas o normas externas favorecen la correcta evaluación de los niveles de madurez de la universidad en cuanto a las TI implementadas. Las NTP, así como algunos estándares ISO se relacionan directamente con este objetivo. COBIT, por su parte, relaciona de forma directa el cumplimiento de este objetivo.

Objetivo "E" a objetivo 11

Este objetivo está relacionado con contar con procesos eficientes, óptimos y funcionales para el beneficio de la universidad y específicamente hablando de TI para la gestión de la información y satisfacción de usuarios finales. Esta es la razón por la que se mapea con este objetivo de COBIT.

Objetivo "F" a objetivo 3

Con este objetivo se pretende garantizar que la gestión de riesgos de TI no exceda el nivel aceptado y sea gestionado por el cumplimiento de las leyes internas de la universidad, asegurando así el resguardo de los activos. El objetivo 3 que propone COBIT se relaciona directamente.

Objetivo "G" a objetivo 7

Este es una de las principales iniciativas estratégicas de la universidad en relación a TI debido a los costos y consecuencias del tiempo en que los servicios podrían quedar inoperativos, de ahí que mantener la continuidad y disponibilidad de los servicios sea un factor clave que COBIT, en su objetivo 7, también abarca y define.

Objetivo "H" a objetivo 9

A fin de tomar decisiones acertadas y eficientes que favorezcan a la universidad, se busca como objetivo que las herramientas de TI capturen, procesen, almacenen y distribuyan información confiable, además de ayudar a los encargados a analizar problemas y dar soluciones efectivas de acuerdo a las políticas internas. El objetivo 9 de COBIT aborda este enfoque.

Objetivo "I" a objetivo 16

Se reconoce, mediante este objetivo, la necesidad de contar con personal capacitado para cumplir con las necesidades de la organización, brindando una mejor atención en las labores desempeñadas. Esta es la razón por que se alinea con el objetivo 16 que propone COBIT.

3.6 Objetivos de TI identificados a partir de la cascada de objetivos

A través de la cascada de objetivos propuestas por COBIT 5 se tiene para cada objetivo de la organización una relación principal ("P") y una secundaria ("S") con los objetivos de TI relacionados.

Este detalle se muestra a continuación:

Tabla N° 7: Objetivo de TI Nº 02

FINANCIERA	1	Alineamiento de TI y la estrategia de negocio	**P**
	3	compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	**S**
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	**P**
CLIENTE	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	**P**
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	**S**

INTERNA	9	Agilidad de las TI	P
	11	Optimización de activos, recursos y capacidades de las TI	S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	P
	13	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	S
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S
APRENDIZAJE Y CRECIMIENTO	16	Personal del negocio y de las TI competente y motivado	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	P

Fuente: Los autores

Tabla N° 8: Objetivo de TI Nº 03

FINANCIERA	1	Alineamiento de TI y la estrategia de negocio	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	S
	3	compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	S
	4	Riesgos de negocio relacionados con las TI gestionados	P
	6	Transparencia de los costos, beneficios y riesgos de TI	S
CLIENTE	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S
INTERNA	9	Agilidad de las TI	S
	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones	P
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S
	13	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	S
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S
	15	Cumplimiento de TI con las políticas internas	S
APRENDIZAJE Y CRECIMIENTO	16	Personal del negocio y de las TI competente y motivado	P

Fuente: Los autores

Tabla N° 9: Objetivo de TI Nº 04

FINANCIERA	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	**P**
	4	Riesgos de negocio relacionados con las TI gestionados	**S**
CLIENTE	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	**S**
INTERNA	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones	**P**
	14	Disponibilidad de información útil y relevante para la toma de decisiones	**S**
	15	Cumplimiento de TI con las políticas internas	**S**

Fuente: Los autores

Tabla N° 10: Objetivo de TI Nº 06

FINANCIERA	1	Alineamiento de TI y la estrategia de negocio	**P**
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	**S**
CLIENTE	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	**P**
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	**S**
INTERNA	9	Agilidad de las TI	**S**
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	**S**
	13	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	**S**
APRENDIZAJE Y CRECIMIENTO	16	Personal del negocio y de las TI competente y motivado	**S**
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	**S**

Fuente: Los autores

Tabla N° 11: Objetivo de TI Nº 07

FINANCIERA	1	Alineamiento de TI y la estrategia de negocio	**S**
	4	Riesgos de negocio relacionados con las TI gestionados	**P**
CLIENTE	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	**S**

	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S
INTERNA	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones	P
	14	Disponibilidad de información útil y relevante para la toma de decisiones	P

Fuente: Los autores

Tabla N° 12: Objetivo de TI Nº 09

FINANCIERA	1	Alineamiento de TI y la estrategia de negocio	P
	3	compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	S
	6	Transparencia de los costos, beneficios y riesgos de TI	S
CLIENTE	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S
INTERNA	14	Disponibilidad de información útil y relevante para la toma de decisiones	P
APRENDIZAJE Y CRECIMIENTO	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S

Fuente: Los autores

Tabla N° 13: Objetivo de TI Nº 11

FINANCIERA	1	Alineamiento de TI y la estrategia de negocio	P
	3	compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	S
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	S
CLIENTE	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	P
INTERNA	9	Agilidad de las TI	P
	11	Optimización de activos, recursos y capacidades de las TI	S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	P
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S
APRENDIZAJE Y CRECIMIENTO	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S

Fuente: Los autores

Tabla N° 14: Objetivo de TI Nº 15

FINANCIERA	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	P

	4	Riesgos de negocio relacionados con las TI gestionados	S
INTERNA	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones	P
	15	Cumplimiento de TI con las políticas internas	P

Fuente: Los autores

Tabla N° 15: Objetivo de TI Nº 16

FINANCIERA	1	Alineamiento de TI y la estrategia de negocio	S
	3	compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	S
	4	Riesgos de negocio relacionados con las TI gestionados	S
CLIENTE	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S
INTERNA	9	Agilidad de las TI	S
APRENDIZAJE Y CRECIMIENTO	16	Personal del negocio y de las TI competente y motivado	P
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S

Fuente: Los autores

A fin de lograr el cumplimiento de los objetivos de nuestro caso de estudio planteados y alineados al marco de referencia COBIT 5, se identifican en resumen los siguientes objetivos de TI, los cuales se ajustan a las necesidades reales de la organización para posteriormente identificar las métricas y procesos habilitadores según el enfoque de la seguridad de la información:

Tabla N° 16: Objetivo de TI que se ajustan a las necesidades de la organización.

Perspectiva	Objetivos de TI
Financiera	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	Riesgos de negocio relacionados con las TI gestionados
Cliente	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	Agilidad de las TI
	Seguridad de la información, infraestructuras de procesamiento y aplicaciones
	Optimización de activos, recursos y capacidades de las TI
	Disponibilidad de información útil y relevante para la toma de decisiones

	Cumplimiento de TI con las políticas internas
Aprendizaje y crecimiento	Conocimiento, experiencia e iniciativas para la innovación de negocio

Fuente: Los autores – COBIT5

3.6.1 Justificación de los objetivos de TI seleccionados

Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas

Debido a que las normas externas regulan el uso de las tecnologías de información en las organizaciones, se debe garantizar el cumplimiento y soporte de la TI a todo nivel con el fin de llevar a cabo análisis futuros en los niveles de madurez de acuerdo a los enfoques establecidos por dichas normas.

Riesgos de negocio relacionados con las TI gestionados

En la actualidad, las organizaciones se ven afectadas por riesgos en materia de seguridad de la información y protección de datos relacionadas con la gestión de las TI. Conocer las vulnerabilidades asociadas, ayudará a evitar una falla tecnológica que pudiera convertirse en un riesgo a nivel organizacional. De ahí la importancia de tomar este objetivo.

Entrega de servicios de TI de acuerdo a los requisitos del negocio

La entrega de servicios de acuerdo a las políticas, requerimientos y normas internas de la organización es fundamental para el cumplimiento de estos mismos y, además, garantiza la satisfacción de las partes interesadas y el correcto desempeño de sus funciones.

Uso adecuado de aplicaciones, información y soluciones tecnológicas

Considerando que las tecnologías de información constituyen un factor crítico y estratégico que permiten tomar decisiones eficientes, se considera que estas deben gestionarse de forma adecuada, mediante el buen uso de la información y la implementación de soluciones ágiles con amplio alcance y beneficios inmediatos.

Agilidad de las TI

De acuerdo al crecimiento tecnológico surgido durante los últimos años, la universidad requiere la adopción de nuevas herramientas que permitan integrar aplicaciones actuales como nuevas de forma tal que se agilicen los procesos relacionados, brindando servicios oportunos que beneficien a todas las partes interesadas y permitan una fácil administración.

Seguridad de la información, infraestructuras de procesamiento y aplicaciones

Actualmente, la información es uno de los activos más preciados para una organización de ahí que brindarle seguridad sea una misión fundamental para los encargados de su administración. Para ello, deben estar en la capacidad de identificar, proteger y supervisar las acciones sobre la información sensible o confidencial. La importancia para este objetivo se ve reforzada por la ley de protección de datos personales (Ley Nº 29733).

Optimización de activos, recursos y capacidades de las TI

Unas de las razones por la que se debe considerar este objetivo es que la eficiencia de los servicios brindados en una organización depende en gran medida de la optimización de las tecnologías de TI. Así se mantendrá una ventaja competitiva dando cumplimiento a las normativas y buenas prácticas vigentes. Una buena gestión del riesgo, la satisfacción de las expectativas de los interesados y los buenos niveles de servicio, son aportes adicionales en consecuencia.

Disponibilidad de información útil y relevante para la toma de decisiones

Se dice que las mejores decisiones son aquellas basadas en información relevante. El tener acceso a este tipo de información centralizada, permite monitorear lo que está pasando tanto dentro como fuera de la organización a fin de tomar las medidas necesarias y oportunas que favorezcan al logro de los objetivos propuestos. Este es un factor clave que viene como consecuencia de la adecuada gestión de la información.

Cumplimiento de TI con las políticas internas

Tal como se mencionó anteriormente, el cumplimiento de las políticas internas de TI da como resultado que estas sean respetadas y reconocidas; por eso, asegurar su cumplimiento será de importancia a fin de tomar decisiones acordes con ellas.

Conocimiento, experiencia e iniciativas para la innovación de negocio

Este objetivo está relacionado con en gran medida con el grado de satisfacción de las partes interesadas y el cumplimiento de las políticas internas. Esto apuntará a alcanzar la excelencia estratégica a través del conocimiento, experiencia e iniciativas para la innovación en proyectos de TI a futuro.

3.7 Identificación de métricas para los objetivos de TI

Se identifican para cada objetivo de TI las métricas o indicadores que verifican el cumplimiento de las mismas. Esta es parte de la cascada de objetivos de COBIT 5.

Tabla N° 17: Métricas relacionadas con los objetivos de TI según COBIT 5

Perspectiva	Objetivos de TI	MÉTRICAS
Financiera	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Número de incumplimientos de TI reportados al Consejo de Administración o causantes de comentarios o vergüenzas públicos
		Número de incumplimientos relacionados con proveedores de servicios de TI
	Riesgos de negocio relacionados con las TI gestionados	Porcentaje de servicios de TI y programas de negocio habilitados por TI cubiertas por evoluciones de riesgo
		Número de incidentes TI significativos que no fueron identificados en evaluaciones de riesgos
		Porcentaje de evaluaciones de riesgo corporativas que incluyen riesgo de TI
Cliente	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Número de interrupciones de negocio debidas a incidentes de servicios de TI
		Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados
		Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios de TI
		Nivel de entendimiento de los usuarios del negocio sobre cómo las soluciones tecnológicas apoyan sus procesos
		Valor presente neto (NPV) mostrando el nivel de satisfacción del negocio con la calidad y utilidad de las soluciones tecnológicas
Interna	Agilidad de las TI	Nivel de satisfacción de la alta dirección del negocio con la capacidad de respuesta de TI a nuevos requerimientos.
		Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas
	Seguridad de la información, infraestructuras de procesamiento y aplicaciones	Número de incidentes de seguridad causantes de interrupción del negocio o vergüenza pública
		Tiempo de concesión, cambio y eliminación de privilegios de acceso comparado con los niveles de servicio acordados
		Frecuencia de las evaluaciones de seguridad en relación a los últimos estándares y guías
	Optimización de activos, recursos y capacidades de las TI	Niveles de satisfacción de la alta dirección del negocio y de TI con las capacidades TI
	Disponibilidad de información útil y relevante para la toma de decisiones	Nivel de satisfacción del usuario del negocio con la calidad y la puntualidad (o disponibilidad) de la información de gestión
		Número de incidentes de procesos de negocio causados por la indisponibilidad de la información
		Relación y alcance de decisiones de negocio erróneas donde la información errónea o no disponible fue un factor clave
	Cumplimiento de TI con las políticas internas	Número de incidentes relacionados con el incumplimiento de políticas
		Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivas
Aprendizaje y crecimiento	Conocimiento, experiencia e iniciativas para la innovación de	Nivel de concienciación y comprensión de la alta dirección del negocio sobre las posibilidades de innovación TI

	negocio	Nivel de satisfacción de los interesados con los niveles de experiencia e ideas de innovación de TI

Fuente: Los autores – COBIT 5 Procesos Habilitadores

Con referencia a lo anterior, los objetivos de TI mapeados serán empleados para llegar a los procesos habilitadores de COBIT 5 según el enfoque de la seguridad de la información a fin de alcanzar los objetivos organizacionales propuestos. Esto se evidenciará en los resultados de la evaluación de las métricas definidas.

SECCION C: Análisis de procesos de COBIT aplicables

Durante el desarrollo de esta sección, se llegarán a los procesos habilitadores mediante la última parte de la cascada de objetivos de control definida por COBIT 5, teniendo en cuenta los objetivos relacionados de TI definidos en el capítulo anterior.

De acuerdo a lo propuesto por COBIT 5, para cada objetivo de TI le corresponden procesos habilitadores que serán analizados minuciosamente a fin de realizar un primer filtro que determinará su correcta aplicabilidad de acuerdo al caso de estudio definido. A partir del correcto análisis y justificación, se procederá a realizar un segundo filtro donde todos los procesos habilitadores (según el dominio), relacionados a seguridad de la información, sean seleccionados y justifiquen el logro final de los objetivos del caso estudio.

3.8 Aplicación de los procesos habilitadores

Teniendo en cuenta los objetivos relacionados con TI definidos en el capítulo anterior, se procederá a relacionarlos con sus respectivos procesos habilitadores que conllevan a su cumplimiento. COBIT define dos tipos de relaciones: principal (“P”) y secundaria (“S”) de acuerdo a la influencia sobre dicho objetivo.

A continuación, se presentan los objetivos de TI identificados y su relación con los procesos habilitadores propuestos por COBIT:

Objetivo de TI: Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas

Tabla N° 18: Procesos habilitadores según el objetivo de TI 2

DOMINIO	PROCESO	RELACIÓN
Evaluar, Dirigir y Monitorear (EDM)	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	S
	Asegurar la Optimización del Riesgo	S
	Asegurar la Transparencia hacia las partes interesadas	S

Alinear, Planear y Organizar (APO)	Gestionar el Marco de Gestión de TI	**P**
	Gestionar los Recursos Humanos	**S**
	Gestionar los Proveedores	**S**
	Gestionar la Calidad	**S**
	Gestionar el Riesgo	**P**
	Gestionar la Seguridad	**P**
Construir, Adquirir e Implementar (BAI)	Gestionar la Definición de Requisitos	**S**
	Gestionar los Activos	**S**
	Gestionar la Configuración	**P**
Entregar, dar Servicio y Soporte (DSS)	Gestionar las Operaciones	**S**
	Gestionar los Problemas	**S**
	Gestionar la Continuidad	**S**
	Gestionar los Servicios de Seguridad	**P**
	Gestionar los Controles de los Procesos del Negocio	**S**
Monitorear, Evaluar y Asegurar (MEA)	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	**S**
	Supervisar, Evaluar y Valorar el Sistema de Control Interno	**P**
	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	**P**

Fuente: Los autores

Objetivo de TI: Riesgos de negocio relacionados con las TI gestionados

Tabla N° 19: Procesos habilitadores según el objetivo de TI 4

DOMINIO	PROCESO	RELACIÓN
Evaluar, Dirigir y Monitorear (EDM)	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	**S**
	Asegurar la Optimización del Riesgo	**P**
	Asegurar la Optimización de los Recursos	**S**
Alinear, Planear y Organizar (APO)	Gestionar el Marco de Gestión de TI	**S**
	Gestionar la Estrategia	**S**
	Gestionar la Arquitectura Empresarial	**S**
	Gestionar la Innovación	**S**
	Gestionar el portafolio	**S**
	Gestionar el Presupuesto y los Costes	**S**
	Gestionar los Recursos Humanos	**S**
	Gestionar las Relaciones	**S**
	Gestionar los Acuerdos de Servicio	**S**
	Gestionar los Proveedores	**P**
	Gestionar la Calidad	**S**
	Gestionar el Riesgo	**P**
	Gestionar la Seguridad	**P**
Construir, Adquirir e Implementar (BAI)	Gestionar los Programas y Proyectos	**P**
	Gestionar la Definición de Requisitos	**S**
	Gestionar la Identificación y la Construcción de Soluciones	**S**
	Gestionar la Disponibilidad y la Capacidad	**S**
	Gestionar los Cambios	**P**
	Gestionar la Aceptación del Cambio y de la	**S**

	Transición	
	Gestionar los Activos	S
	Gestionar la Configuración	S
Entregar, dar Servicio y Soporte (DSS)	Gestionar las Operaciones	P
	Gestionar las Peticiones y los Incidentes del Servicio	P
	Gestionar los Problemas	P
	Gestionar la Continuidad	P
	Gestionar los Servicios de Seguridad	P
	Gestionar los Controles de los Procesos del Negocio	P
Monitorear, Evaluar y Asegurar (MEA)	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	P
	Supervisar, Evaluar y Valorar el Sistema de Control Interno	P
	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	P

Fuente: Los autores

Objetivo de TI: Entrega de servicios de TI de acuerdo a los requisitos del negocio

Tabla N° 20: Procesos habilitadores según el objetivo de TI 7

DOMINIO	PROCESO	RELACIÓN
Evaluar, Dirigir y Monitorear (EDM)	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P
	Asegurar la Entrega de Beneficios	P
	Asegurar la Optimización del Riesgo	S
	Asegurar la Optimización de los Recursos	S
	Asegurar la Transparencia hacia las partes interesadas	P
Alinear, Planear y Organizar (APO)	Gestionar el Marco de Gestión de TI	S
	Gestionar la Estrategia	P
	Gestionar la Arquitectura Empresarial	S
	Gestionar el portafolio	S
	Gestionar el Presupuesto y los Costes	S
	Gestionar los Recursos Humanos	S
	Gestionar las Relaciones	P
	Gestionar los Acuerdos de Servicio	P
	Gestionar los Proveedores	P
	Gestionar la Calidad	P
	Gestionar el Riesgo	S
	Gestionar la Seguridad	S
Construir, Adquirir e Implementar (BAI)	Gestionar los Programas y Proyectos	S
	Gestionar la Definición de Requisitos	P
	Gestionar la Identificación y la Construcción de Soluciones	P
	Gestionar la Disponibilidad y la Capacidad	P
	Gestionar la introducción de Cambios Organizativos	S
	Gestionar los Cambios	P
	Gestionar la Aceptación del Cambio y de la Transición	S
	Gestionar el Conocimiento	S

	Gestionar los Activos	S
Entregar, dar Servicio y Soporte (DSS)	Gestionar las Operaciones	P
	Gestionar las Peticiones y los Incidentes del Servicio	P
	Gestionar los Problemas	P
	Gestionar la Continuidad	P
	Gestionar los Servicios de Seguridad	S
	Gestionar los Controles de los Procesos del Negocio	P
Monitorear, Evaluar y Asegurar (MEA)	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	P
	Supervisar, Evaluar y Valorar el Sistema de Control Interno	S
	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	S

Fuente: Los autores

Objetivo de TI: Uso adecuado de aplicaciones, información y soluciones tecnológicas

Tabla N° 21: Procesos habilitadores según el objetivo de TI 8

DOMINIO	PROCESO	RELACIÓN
Evaluar, Dirigir y Monitorear (EDM)	Asegurar la Entrega de Beneficios	S
	Asegurar la Optimización del Riesgo	S
	Asegurar la Optimización de los Recursos	S
Alinear, Planear y Organizar (APO)	Gestionar la Estrategia	S
	Gestionar la Arquitectura Empresarial	S
	Gestionar la Innovación	P
	Gestionar el portafolio	S
	Gestionar el Presupuesto y los Costes	S
	Gestionar las Relaciones	S
	Gestionar los Acuerdos de Servicio	S
	Gestionar los Proveedores	S
	Gestionar la Calidad	S
	Gestionar el Riesgo	S
	Gestionar la Seguridad	S
Construir, Adquirir e Implementar (BAI)	Gestionar los Programas y Proyectos	S
	Gestionar la Definición de Requisitos	S
	Gestionar la Identificación y la Construcción de Soluciones	S
	Gestionar la Disponibilidad y la Capacidad	S
	Gestionar la introducción de Cambios Organizativos	P
	Gestionar los Cambios	S
	Gestionar la Aceptación del Cambio y de la Transición	P
	Gestionar el Conocimiento	S
	Gestionar la Configuración	S
Entregar, dar Servicio y Soporte (DSS)	Gestionar las Operaciones	S
	Gestionar las Peticiones y los Incidentes del Servicio	S
	Gestionar los Problemas	S
	Gestionar la Continuidad	S
	Gestionar los Servicios de Seguridad	S

	Gestionar los Controles de los Procesos del Negocio	S
Monitorear, Evaluar y Asegurar (MEA)	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S
	Supervisar, Evaluar y Valorar el Sistema de Control Interno	S

Fuente: Los autores

Objetivo de TI: Agilidad de las TI

Tabla N° 22: Procesos habilitadores según el objetivo de TI 9

DOMINIO	PROCESO	RELACIÓN
Evaluar, Dirigir y Monitorear (EDM)	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	S
	Asegurar la Optimización de los Recursos	P
Alinear, Planear y Organizar (APO)	Gestionar el Marco de Gestión de TI	P
	Gestionar la Estrategia	S
	Gestionar la Arquitectura Empresarial	P
	Gestionar la Innovación	P
	Gestionar el portafolio	S
	Gestionar los Recursos Humanos	S
	Gestionar los Acuerdos de Servicio	S
	Gestionar los Proveedores	P
	Gestionar la Calidad	S
	Gestionar el Riesgo	S
Construir, Adquirir e Implementar (BAI)	Gestionar la Definición de Requisitos	S
	Gestionar la Disponibilidad y la Capacidad	S
	Gestionar la introducción de Cambios Organizativos	S
	Gestionar los Cambios	S
	Gestionar la Aceptación del Cambio y de la Transición	S
	Gestionar el Conocimiento	P
	Gestionar los Activos	S
	Gestionar la Configuración	S
Entregar, dar Servicio y Soporte (DSS)	Gestionar las Operaciones	S
	Gestionar los Problemas	S
	Gestionar la Continuidad	S
Monitorear, Evaluar y Asegurar (MEA)	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S

Fuente: Los autores

Objetivo de TI: Seguridad de la información, infraestructuras de procesamiento y aplicaciones

Tabla N° 23: Procesos habilitadores según el objetivo de TI 10

DOMINIO	PROCESO	RELACIÓN
Evaluar, Dirigir y Monitorear (EDM)	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	S
	Asegurar la Optimización del Riesgo	P
Alinear, Planear y Organizar (APO)	Gestionar el Marco de Gestión de TI	S
	Gestionar la Arquitectura Empresarial	S
	Gestionar los Recursos Humanos	S
	Gestionar los Acuerdos de Servicio	S

	Gestionar los Proveedores	S
	Gestionar el Riesgo	P
	Gestionar la Seguridad	P
Construir, Adquirir e Implementar (BAI)	Gestionar la Definición de Requisitos	S
	Gestionar los Cambios	P
	Gestionar el Conocimiento	S
	Gestionar los Activos	S
	Gestionar la Configuración	S
Entregar, dar Servicio y Soporte (DSS)	Gestionar las Operaciones	S
	Gestionar las Peticiones y los Incidentes del Servicio	S
	Gestionar la Continuidad	S
	Gestionar los Servicios de Seguridad	P
	Gestionar los Controles de los Procesos del Negocio	S
Monitorear, Evaluar y Asegurar (MEA)	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S
	Supervisar, Evaluar y Valorar el Sistema de Control Interno	S
	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	S

Fuente: Los autores

Objetivo de TI: Optimización de activos, recursos y capacidades de las TI

Tabla N° 24: Procesos habilitadores según el objetivo de TI 11

DOMINIO	PROCESO	RELACIÓN
Evaluar, Dirigir y Monitorear (EDM)	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	S
	Asegurar la Entrega de Beneficios	S
	Asegurar la Optimización de los Recursos	P
Alinear, Planear y Organizar (APO)	Gestionar el Marco de Gestión de TI	P
	Gestionar la Estrategia	S
	Gestionar la Arquitectura Empresarial	P
	Gestionar la Innovación	P
	Gestionar el portafolio	S
	Gestionar el Presupuesto y los Costes	S
	Gestionar los Recursos Humanos	P
	Gestionar las Relaciones	S
	Gestionar los Acuerdos de Servicio	S
	Gestionar los Proveedores	S
	Gestionar la Calidad	S
Construir, Adquirir e Implementar (BAI)	Gestionar los Programas y Proyectos	S
	Gestionar la Definición de Requisitos	S
	Gestionar la Identificación y la Construcción de Soluciones	S
	Gestionar la Disponibilidad y la Capacidad	P
	Gestionar la introducción de Cambios Organizativos	S
	Gestionar los Cambios	S
	Gestionar el Conocimiento	S
	Gestionar los Activos	P
	Gestionar la Configuración	P

Entregar, dar Servicio y Soporte (DSS)	Gestionar las Operaciones	**P**
	Gestionar los Problemas	**P**
	Gestionar la Continuidad	**S**
	Gestionar los Servicios de Seguridad	**S**
	Gestionar los Controles de los Procesos del Negocio	**S**
Monitorear, Evaluar y Asegurar (MEA)	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	**P**

Fuente: Los autores

Objetivo de TI: Disponibilidad de información útil y relevante para la toma de decisiones

Tabla N° 25: Procesos habilitadores según el objetivo de TI 14

DOMINIO	PROCESO	RELACIÓN
Evaluar, Dirigir y Monitorear (EDM)	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	**S**
	Asegurar la Entrega de Beneficios	**S**
	Asegurar la Optimización del Riesgo	**S**
	Asegurar la Transparencia hacia las partes interesadas	**S**
Alinear, Planear y Organizar (APO)	Gestionar el Marco de Gestión de TI	**S**
	Gestionar la Estrategia	**S**
	Gestionar la Arquitectura Empresarial	**S**
	Gestionar la Innovación	**S**
	Gestionar los Acuerdos de Servicio	**P**
	Gestionar los Proveedores	**S**
	Gestionar la Calidad	**S**
	Gestionar el Riesgo	**S**
	Gestionar la Seguridad	**P**
Construir, Adquirir e Implementar (BAI)	Gestionar la Definición de Requisitos	**S**
	Gestionar la Identificación y la Construcción de Soluciones	**S**
	Gestionar la Disponibilidad y la Capacidad	**P**
	Gestionar los Cambios	**S**
	Gestionar la Aceptación del Cambio y de la Transición	**S**
	Gestionar el Conocimiento	**S**
	Gestionar los Activos	**S**
	Gestionar la Configuración	**P**
Entregar, dar Servicio y Soporte (DSS)	Gestionar las Operaciones	**S**
	Gestionar las Peticiones y los Incidentes del Servicio	**S**
	Gestionar los Problemas	**P**
	Gestionar la Continuidad	**P**
	Gestionar los Servicios de Seguridad	**S**
	Gestionar los Controles de los Procesos del Negocio	**S**
Monitorear, Evaluar y Asegurar (MEA)	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	**S**

Fuente: Los autores

Objetivo de TI: Cumplimiento de TI con las políticas internas

Tabla N° 26: Procesos habilitadores según el objetivo de TI 15

DOMINIO	PROCESO	RELACIÓN
Evaluar, Dirigir y Monitorear (EDM)	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	S
	Asegurar la Optimización del Riesgo	P
	Asegurar la Transparencia hacia las partes interesadas	S
Alinear, Planear y Organizar (APO)	Gestionar el Marco de Gestión de TI	P
	Gestionar la Estrategia	S
	Gestionar los Recursos Humanos	S
	Gestionar las Relaciones	S
	Gestionar los Acuerdos de Servicio	S
	Gestionar los Proveedores	S
	Gestionar la Calidad	S
	Gestionar el Riesgo	S
Construir, Adquirir e Implementar (BAI)	Gestionar los Cambios	S
	Gestionar la Aceptación del Cambio y de la Transición	S
	Gestionar los Activos	S
	Gestionar la Configuración	S
Entregar, dar Servicio y Soporte (DSS)	Gestionar las Operaciones	S
	Gestionar las Peticiones y los Incidentes del Servicio	S
	Gestionar los Problemas	S
	Gestionar la Continuidad	S
	Gestionar los Servicios de Seguridad	S
	Gestionar los Controles de los Procesos del Negocio	S
Monitorear, Evaluar y Asegurar (MEA)	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	P
	Supervisar, Evaluar y Valorar el Sistema de Control Interno	P
	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	S

Fuente: Los autores

Objetivo de TI: Conocimiento, experiencia e iniciativas para la innovación de negocio

Tabla N° 27: Procesos habilitadores según el objetivo de TI 17

DOMINIO	PROCESO	RELACIÓN
Evaluar, Dirigir y Monitorear (EDM)	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	S
	Asegurar la Entrega de Beneficios	P
	Asegurar la Optimización del Riesgo	S
	Asegurar la Optimización de los Recursos	S
	Asegurar la Transparencia hacia las partes interesadas	S
Alinear, Planear y Organizar (APO)	Gestionar el Marco de Gestión de TI	P
	Gestionar la Estrategia	P
	Gestionar la Arquitectura Empresarial	S
	Gestionar la Innovación	P
	Gestionar el portafolio	S
	Gestionar los Recursos Humanos	P
	Gestionar las Relaciones	P
	Gestionar los Proveedores	S

	Gestionar la Calidad	S
	Gestionar el Riesgo	S
Construir, Adquirir e Implementar (BAI)	Gestionar los Programas y Proyectos	S
	Gestionar la Definición de Requisitos	S
	Gestionar la Identificación y la Construcción de Soluciones	S
	Gestionar la Disponibilidad y la Capacidad	S
	Gestionar la introducción de Cambios Organizativos	P
	Gestionar los Cambios	S
	Gestionar la Aceptación del Cambio y de la Transición	S
	Gestionar el Conocimiento	P
Entregar, dar Servicio y Soporte (DSS)	Gestionar las Operaciones	S
	Gestionar las Peticiones y los Incidentes del Servicio	S
	Gestionar los Problemas	S
	Gestionar la Continuidad	S
	Gestionar los Controles de los Procesos del Negocio	S
Monitorear, Evaluar y Asegurar (MEA)	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S
	Supervisar, Evaluar y Valorar el Sistema de Control Interno	S
	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	S

Fuente: Los autores

3.8.1 Justificación de los procesos habilitadores a nivel general

De acuerdo a nuestro caso de estudio, y de manera general, se deberán tomar en cuenta los procesos que únicamente correspondan con el logro de objetivos organizacionales, en otras palabras, con su entorno actual, políticas internas y normativas a las cuales está sujeta.

Por eso, debido a la relación principal y secundaria de cada uno de los objetivos de TI con su respectivo proceso habilitador, se toman en cuenta los siguientes según el marco de COBIT 5.

Tabla N° 28: Relación de procesos habilitadores según los objetivos perseguidos por el caso de estudio

DOMINIO	PROCESO HABILITADOR
Evaluar, Dirigir y Monitorear (EDM)	Asegurar la Optimización del Riesgo
Alinear, Planear y Organizar (APO)	Gestionar el Marco de Gestión de TI
	Gestionar la Innovación
	Gestionar los Proveedores
	Gestionar el Riesgo
	Gestionar la Seguridad
Construir, Adquirir	Gestionar la Disponibilidad y la Capacidad

e Implementar (BAI)	Gestionar los Cambios
	Gestionar los Activos
	Gestionar la configuración
Entregar, dar Servicio y Soporte (DSS)	Gestionar las Operaciones
	Gestionar las Peticiones y los Incidentes del Servicio
	Gestionar los Problemas
	Gestionar la Continuidad
	Gestionar los Servicios de Seguridad
Monitorear, Evaluar y Asegurar (MEA)	Supervisar, Evaluar y Valorar Rendimiento y Conformidad
	Supervisar, Evaluar y Valorar el Sistema de Control Interno

Fuente: Los autores

La tabla anterior, muestran los procesos habilitadores que dan seguimiento a los objetivos de TI asociados para el caso de estudio. Estos procesos definidos por COBIT, tienen la finalidad de dar cumplimiento a los 10 procesos organizacionales definidos en el capítulo anterior, tomados según las normas y políticas internas de la Universidad Nacional Pedro Ruiz Gallo, así como de los objetivos internos que define y persigue el área de Red Telemática para el desarrollo de sus funciones. La justificación según ISACA (2012), para cada proceso se muestra a continuación.

- **Evaluar, Dirigir y Monitorear (EDM)**

De forma general, este dominio contiene 5 procesos principales considerados como los pilares del gobierno de TI. Sin embargo, como parte de nuestro caso de estudio, solo se considera uno de ellos, a saber: Asegurar la Optimización del Riesgo (EDM03). Este proceso, permite asegurar la tolerancia al riesgo de una organización mediante el entendimiento, la articulación y la comunicación. El resultado final será identificar y gestionar los riesgos relacionados con el uso de TI.

Además, está íntimamente relacionado con los objetivos de TI 4 y 6 abordados por COBIT quienes dan cumplimiento final a dos de los objetivos propuestos por el caso de estudio y definidos en el capítulo anterior.

- **Alinear, Planear y Organizar (APO)**

Existen 13 procesos habilitadores descritos en este segundo dominio. Como parte del caso de estudio, se seleccionan 5 procesos, a saber: Gestionar el Marco de Gestión de TI (APO01), Gestionar la Innovación (APO04), Gestionar los Proveedores (APO10), Gestionar el Riesgo (APO12) y Gestionar la seguridad (APO13).

Estos procesos se concentran en implementar y mantener mecanismos para la gestión de la información y uso de TI, para dar cumplimiento a los objetivos de la organización y en consecuencia a las políticas y principios rectores. También, permite mantener un conocimiento de la tecnología de la información y los servicios a fin de influir estratégicamente en las decisiones de la organización.

Administrar todos los servicios de TI para satisfacer las necesidades de la organización minimizando el riesgo, es otro de las maneras como cumplir los objetivos de TI.

Y finalmente, la identificación, evaluación y reducción de los riesgos relacionados con TI y la gestión de la seguridad de la información, serán habilitadores necesarios para dar cumplimiento a las necesidades de la organización.

Estos 5 procesos abordan de forma oportuna 8 objetivos de TI propuestos por COBIT y relacionados con el cumplimiento de los objetivos del caso de estudio.

- **Construir, Adquirir e Implementar (BAI)**

Este tercer dominio, compuesto por 10 procesos, se orienta básicamente a los mecanismos necesarios para adquirir e implementar soluciones de TI, identificando soluciones viables, preparando documentación y formando a los usuarios en las nuevas herramientas de gestión.

Para nuestro caso de estudio, 4 procesos están muy relacionados en el cumplimiento de 5 de los objetivos de TI definidos, a saber: Gestionar la Disponibilidad y la Capacidad (BAI04), Gestionar los Cambios (BAI 06), Gestionar los Activos (BAI09) y Gestionar la Configuración (BAI10).

Estos procesos están enfocados en mantener la disponibilidad de los servicios, la gestión eficiente de recursos y la optimización del rendimiento de los sistemas mediante la predicción del rendimiento futuro. Además, gestiona los cambios en forma controlada con respecto a los activos de TI e infraestructura, administra las licencias de software según los acuerdos pertinentes, y mitiga cualquier riesgo que impacte en forma negativa en la estabilidad de los servicios brindados.

Por otro lado, se ve la necesidad de gestionar los activos de TI para asegurar que su uso aporte valor, sean fiables y estén disponibles. Todo esto hará que haya suficiente

información sobre los activos del servicio a fin de que este pueda gestionarse con eficiencia, evaluar el impacto de los cambios y hacer frente a los incidentes.

- **Entregar, dar Servicio y Soporte (DSS)**

La necesidad de administrar y asegurar que los servicios provistos por terceros cumplan con los requerimientos de la organización es hacia donde se enfoca este cuarto dominio compuesto de 6 procesos habilitadores. Para nuestro caso de estudio, se seleccionan los cinco primeros procesos quienes están íntegramente relacionados con dos objetivos de TI asociados, a saber: Gestionar las Operaciones (DSS01), Gestionar las Peticiones y los incidentes del servicio (DSS02), Gestionar los problemas (DSS03), Gestionar la Continuidad (DSS04) y Gestionar los Servicios de Seguridad (DSS05).

Estos procesos se enfocan principalmente en entregar los resultados de los servicios operativos de TI, incluyendo las actividades de monitorización requeridas. También, de proveer una respuesta oportuna y efectiva a los incidentes de seguridad logrando mayor productividad y minimización de las interrupciones.

Además, Incrementar y mantener la disponibilidad de la información a un nivel aceptable, mejorar los niveles de servicio y mejorar la satisfacción de los usuarios finales. Todo esto para minimizar el impacto de las vulnerabilidades e incidentes operativos de seguridad de la información de acuerdo con las políticas de seguridad de la organización, estableciendo roles y privilegios de acceso a la información.

- **Monitorear, Evaluar y Asegurar (MEA)**

Este último dominio, se concentra en dar cumplimiento de los requerimientos de control interno en la organización. Se proponen 3 procesos de los cuales, de acuerdo al caso de estudio, solo se abordarán 2, a saber: Supervisar, Evaluar y Valorar el Rendimiento y Conformidad (MEA01) y Supervisar, Evaluar y Valorar el Sistema de Control Interno (MEA02).

Proporcionar transparencia de rendimiento y conformidad a los objetivos de TI de la organización, así como a las partes interesadas son los principales propósitos por las que considerar dichos procesos.

3.9 Seguridad de la Información según el enfoque de COBIT 5

Según lo realizado hasta el momento, se tiene definidos los procesos habilitadores cuya aplicación garantizará el cumplimiento de los objetivos de TI y, por lo tanto, los perseguidos por la Universidad como marco general de nuestro caso de estudio.

Sin embargo, dentro de los procesos definidos, se deben tomar en cuenta los que guarden relación con el enfoque de la seguridad de la Información, pues estos serán aplicados de forma particular a la Red Telemática como parte de nuestro modelo que finalmente favorezca la toma efectiva de decisiones dentro de la gestión de dicha información.
Seguir los lineamientos de la Ley de protección de datos personales, así como de lo contemplado por las normas internacionales ISO 27001 e ISO 27002, ayudarán a seleccionar los procesos que se ajusten a nuestro caso específico de estudio.

Es digno de mención que, para este caso en particular, no existe alguna regulación que exija su cumplimiento y aplicación.

Tabla N° 29: Resumen de la relación de procesos habilitadores según los objetivos

DOMINIO	PROCESO HABILITADOR
Construir, Adquirir e Implementar (BAI)	Gestionar la Disponibilidad y la Capacidad
	Gestionar los Activos
	Gestionar la configuración
Entregar, dar Servicio y Soporte (DSS)	Gestionar las Operaciones
	Gestionar las Peticiones y los Incidentes del Servicio
	Gestionar los Servicios de Seguridad

Fuente: Los autores

3.9.1 Justificación de los procesos habilitadores seleccionados

Los procesos definidos en el apartado anterior son considerados importantes dentro de la gestión de la seguridad de la información a nivel técnico de acuerdo a la normativa externa y lineamientos contemplados internacionalmente como estándares, así como, de las políticas internas que plantea el área de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

La selección de los mismos, también surge de la intención de relacionar una herramienta software de soporte (base) que sirva de ejecutor en el cumplimiento de los procesos habilitadores definidos, dando seguimiento a los objetivos relacionados a TI asociados y finalmente cumpliendo con los objetivos principales (a nivel de gestión de la seguridad de la información) perseguidos por la universidad. La herramienta de software, así como la relación con el marco de referencia de COBIT 5 (en los procesos habilitadores definidos) se explicarán con más detalles en los capítulos siguientes.

La justificación técnica, de acuerdo a ISACA (2012) para cada proceso definido se da a continuación:

- **Gestionar la disponibilidad y la capacidad de la información y servicios.**

Se considera este proceso por la necesidad de evaluar la previsión de necesidades futuras en base a los requerimientos de la red telemática, el análisis del impacto y la evaluación del riesgo a fin de planificar e implementar acciones correctivas.
Por otro lado, mantener los servicios disponibles, gestionar eficientemente los recursos y optimizar el rendimiento de los sistemas, son actividades vitales para toda organización en cuanto a la gestión de la información y servicios.

Sus procesos de TI relacionados son:

- Entrega de servicios de TI de acuerdo a los requerimientos.
- Optimización de activos, recursos y capacidades de TI.
- Disponibilidad de información útil y relevante para la toma de decisiones.

- **Gestionar los activos de TI**

Este proceso sugiere la gestión de los activos de TI (mediante la contabilización de estos) a fin de asegurar de que aporten valor a la universidad, manteniendo su funcionamiento de acuerdo a las políticas internas. También, la justificación y la protección física para activos fundamentales permitirán que los servicios brindados por estos, sean fiables y estén siempre disponibles.

Además, la administración de licencias de software logrará que se asegure la cantidad óptima de ellas y que a la vez cumplan con los acuerdos establecidos por el proveedor.

Sus procesos de TI relacionados son:

- Transparencia de los costos, beneficios y riesgos de TI.
- Optimización de activos, recursos y capacidades de TI.

- **Gestionar la configuración de los activos de TI**

Implica el poder definir las relaciones entre los recursos y las capacidades necesarias para proporcionar servicios de TI incluyendo la recopilación de información de configuración. Si se tiene suficiente información sobre los activos, se logrará gestionar

los servicios brindados de forma eficiente, evaluando el impacto de los cambios y haciendo frente a los incidentes del servicio.

Sus procesos de TI relacionados son:

- Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas.
- Optimización de activos, recursos y capacidades de TI.
- Disponibilidad de información útil y relevante para la toma de decisiones.

- **Gestionar las operaciones realizadas por los servicios de TI**

Considerar este proceso ayudará a gestionar la entrega de los resultados del servicio operativo de TI, según los acuerdos planificados, para la monitorización requerida.

Sus procesos de TI relacionados son:

- Riesgos de negocio relacionado con las TI gestionados.
- Entrega de servicios de TI de acuerdo a los requisitos del negocio.
- Optimización de activos recursos y capacidades de TI.

- **Gestionar los incidentes de los servicios de TI**

La importancia de este proceso radica en poder dar una respuesta oportuna y efectiva a los incidentes de seguridad generados por los servicios, así como lograr una mayor productividad dentro de la universidad.

Sus procesos de TI relacionados son:

- Riesgos de negocio relacionados con las TI gestionados.
- Entrega de servicios de TI de acuerdo a los requisitos del negocio.

- **Gestionar los servicios de seguridad**

Implica la protección de la información de la empresa para mantener un nivel aceptable del riesgo de seguridad de la información de acuerdo con las políticas establecidas.

Por otro lado, se deberán establecer y mantener los roles de seguridad y los privilegios de acceso a la información realizando las supervisiones necesarias. Todo ello logrará minimizar el impacto de las vulnerabilidades e incidentes operativos en la información.

Sus procesos de TI relacionados son:

- Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas.
- Riesgos de negocio relacionados con las TI gestionadas.
- Seguridad de la información, infraestructura de procesamiento y aplicaciones.

Cada proceso habilitador seleccionado, tiene un conjunto de indicadores que miden su desempeño y correcta aplicación. Estos serán tomados en cuenta en el próximo capítulo para determinar el grado de relación existente entre la herramienta de gestión (OSSIM) y el marco de referencia COBIT.

Tabla N° 30: Procesos habilitadores seleccionados y sus respectivos indicadores

Gestión de la disponibilidad y capacidad	Número de picos de transacciones donde se excede la meta de rendimiento
	Número de incidentes de disponibilidad
	Número de eventos donde la capacidad ha excedido los límites planificados
Gestión de los activos	Numero de activos no utilizados
	Número de activos obsoletos
Gestión de la configuración	Numero de desviaciones entre el repositorio de configuración y la configuración real
Gestión las peticiones y los incidentes de servicio	Número y porcentaje de incidentes que causan interrupción en los procesos críticos de negocio
	Porcentaje de incidentes resueltos dentro de un periodo acordado/aceptable
	Nivel de satisfacción del usuario con la resolución de las peticiones de servicio
Gestión de los servicios de seguridad	Número de vulnerabilidades descubiertas
	Número de rupturas de cortafuegos
	Número de incidentes que impliquen dispositivos de usuario final
	Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno
	Promedio de tiempo entre los cambios y las actualizaciones de cuentas
	Número de cuentas
	Número de incidentes relacionados con seguridad física

	Número de incidentes relacionados con accesos no autorizados a la información
Gestión de operaciones	Número de incidentes causados por problemas operativos
	Tasa de eventos comparada con el número de incidentes
	Porcentaje de tipos de eventos críticos cubiertos por sistemas de detección automática

Fuente: Los autores y COBIT 5 Procesos Habilitadores

SECCION D: Análisis de la herramienta Open Source como plataforma de Gestión de Seguridad de la Información.

Esta sección desarrolla la descripción de las herramientas Open Source que integra la SIEM de OSSIM como plataforma de gestión de la seguridad de la información seleccionada. Se analizarán las funciones esenciales de seguridad que brinda como consola única, así como también, la utilidad de cada una de ellas.

3.10 Framework de OSSIM

La plataforma OSSIM de AlienVault, integra un conjunto de herramientas Open Source en un mismo framework eficiente, capaz de recolectar toda la información de los diferentes Plugin asociados a cada herramienta a fin de integrarlos e interrelacionarlos entre sí, obteniendo una visualización única del estado de la red bajo un formato estándar preestablecido cuyo propósito es el de aumentar la capacidad de detección de anomalías, priorizar los eventos según el contexto en el que se producen y mejorar la visibilidad de la monitorización del estado en la red actual.

A diferencia de otras suites de seguridad tanto libres como propietarias, OSSIM de AlienVault supera el clásico problema del exceso de alertas y de información ya que opera a diferentes niveles, de modo que evita recibir demasiadas alertas poco fiables –falsos positivos-, al mismo tiempo que es altamente efectiva para identificar ataques con comportamientos más complejos - falsos negativos.

La siguiente imagen, muestra los componentes asociados a sus diferentes capas, así como también, su funcionalidad y relaciones.

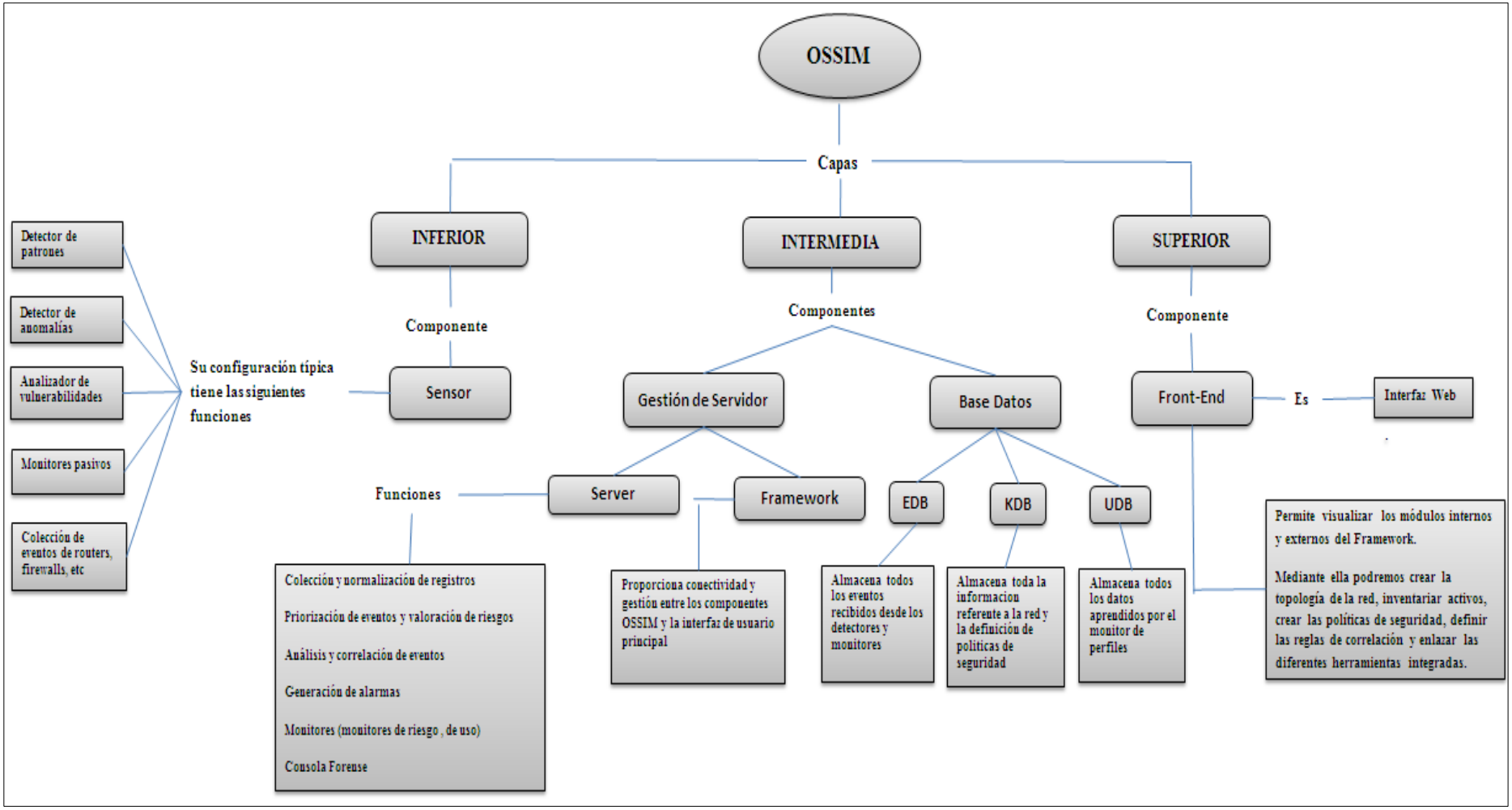


Figura N° 31. Ossim, capas y sus componentes
Fuente: Los autores

3.11 Herramientas integradas en la plataforma OSSIM

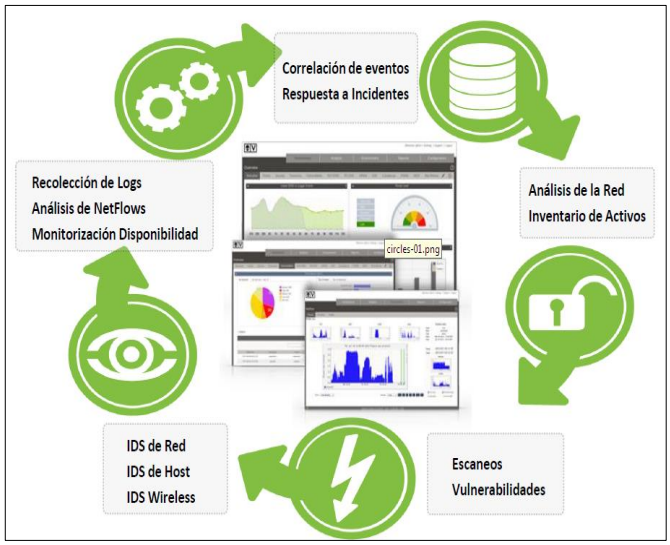


Figura N° 32. Ossim y sus funciones esenciales de seguridad
Fuente: (A3Sec, 2014)

OSSIM proporciona una plataforma unificada que cumple con las siguientes funciones de seguridad:

- Descubrimiento de activos
- Evaluación de vulnerabilidades
- Detección de intrusiones
- Monitoreo del comportamiento
- SIEM

Además, OSSIM aprovecha el poder del intercambio abierto de amenazas de AlienVault, permitiendo a los usuarios contribuir y recibir información en tiempo real sobre los hosts maliciosos.

A continuación, se detallan las herramientas que se utilizan para alguna de las funciones de seguridad:

3.11.1 Descubrimiento de activos

El descubrimiento de activos nos permite crear un inventario de los activos desplegados, logrando con ello dar un primer paso para la evaluación de vulnerabilidades, detección de amenazas, apreciación del comportamiento de la red y de los servicios para detectar violaciones en las políticas corporativas (A3Sec, 2014).

NMAP (Mapeador de redes)

NMAP es una herramienta usada para ejecutar la auditoría de las seguridades de las redes, con la cual se realiza análisis de cada paquete IP, por lo general los administradores de las redes llevan adelante inventarios de las mismas ya que NMAP trabaja con información DNS, en la cual se considera el tipo de puerto, protocolos, estados de los puertos y las direcciones Mac que están vinculados a dichos puertos.

Un puerto puede tener tres tipos de estado: estado abierto o estado de escucha, cerrado o estado de no escucha y en estado de filtrado donde el estado del puerto es indeterminado (Tandazo Jimenez & Rueda Salgado, 2013).

NMAP tiene las siguientes características:

- Identifica Host dentro de una red con el uso del ping.
- Lista los puertos por estado y tipo de protocolo.
- Determina el tipo de sistema operativo.
- Determina la aplicación que corre sobre cada puerto.
- Lista características de Hardware del computador.
- Usado para no ser detectado por IDS.
- Es compatible con sistemas operativos como: Windows, Linux, Solaris, Mac OS, BSD.
- Trabajo bajo línea de comandos y también de forma gráfica como: Zen NMAP.
- Es usada como herramienta de administración para encontrar fallas de seguridad en la red y como herramienta de ataque para encontrar vulnerabilidades en las redes como medio de ataque.
- Sirve para determinar el tipo de Firewalls que se usan.

Utilidad en OSSIM

- Descubrimiento de activos
- Identifica puertos abiertos
- Determina qué servicios se están ejecutando
- Determinar qué S.O y versión se utiliza
- Obtiene algunas características del hardware de red de los activos escaneados

P0F

P0f es una herramienta de identificación pasiva de sistema operativo, permite detectar el sistema y la versión de las maquinas conectadas al sistema, a las que se conecta, a las que se pueden ver a través de su tráfico e incluso a las que no es posible conectarse (DragonJAR).

Utilidad en OSSIM:

- Cambios de S.O
- Gestión de inventario
- Accesos no autorizados a la red

PADS (Sistema pasivo de detección de activos)

Es un motor de detección basado en libpcap para detectar pasivamente activos de la red. Está diseñado para complementar la tecnología IDS proporcionando contexto a las alertas IDS (Shelton, 2005) .

PRADS (Sistema pasivo de detección de activos en tiempo real)

PRADS emplea huellas digitales para reconocer los servicios en el cable, y puede utilizarse para asignar a su red y supervisar los cambios en tiempo real.

El análisis pasivo de tráfico en tiempo real también le permitirá detectar activos que se acaban de conectar a la red durante un corto período de tiempo, ya que Prads puede recoger información útil de cada paquete.

Prads pretende ser una ventanilla única para la detección pasiva de activos, actualmente hace consultas de MAC, identificación de sistema operativo mediante TCP y UDP así como cliente y servicio de la aplicación coincidente y una tabla de estado de conexión.

Varios Plugin de salida incluyen Archivo de registro y FIFO y hacer un Prads útil en reemplazo para P0f, Pads y Sancp.

Prads fue construido desde cero para un diseño compacto y moderno de redes con IPv6 y gigabits de rendimiento (Bjarte Fjellskål & Wysocki).

AlienVault implementa PRADS en OSSIM 4.0 reemplazando a P0f y Arpwatch ya que cumple las mismas funcionalidades que dichas herramientas.

(AlienVault, 2011) indica que su utilidad en OSSIM es la siguiente:

- La gestión de inventario
- Versión de cambios en los servicios
- Violación de políticas
- Inventario de correlación

3.11.2 Evaluación de vulnerabilidades

Se encarga de identificar los sistemas de la red que son vulnerables a ataques, mediante:

- Pruebas de vulnerabilidad de red
- Monitoreo continuo de la vulnerabilidad

OPENVAS

El Sistema de Evaluación de la vulnerabilidad abierto (OpenVas) es un marco de diversos servicios y herramientas que ofrecen una solución completa y potente de análisis de vulnerabilidades y gestión de vulnerabilidades.

OSSIM utiliza OpenVas para la evaluación de las vulnerabilidades y el control de acceso e intrusiones. Al analizar los equipos realiza informes sobre las vulnerabilidades detectadas y trabaja con un motor de correlación con el cual compara todo lo que se ha detectado y buscar soluciones asociadas.

OpenVas funciona con 3 servicios:

Servicio de escaneo (scanner) encargado de realizar el análisis de las vulnerabilidades.

Servicio cliente (interfaz gráfica web) utilizado por el usuario para configurar y presentar los resultados obtenidos (informes).

Servicio manager que mediante el OMP (OpenVas Management Protocol) es el encargado de interactuar con servicios scanner, cliente (Yagual Del Valle & Chilán Rodríguez, 2014).

Utilidad en OSSIM

- Prevención de ataques
- Responde a la pregunta: ¿Se cumple la política de la organización?
- Permite explotar las vulnerabilidades a fin de probarlas (ejemplo: DOS)
- Permite definir la agresividad de los escaneos que realiza
- Evitar el acarreo de caídas en los servicios de red.

- Tiene la capacidad de realizar escaneos en remoto conectándose a la maquina escaneada si se le facilita las credenciales para ello.
- Conoce exactamente el software instalado en cada máquina determinando si tiene alguna vulnerabilidad o no.
- Dispone de un lenguaje propio de escritura de firmas.

3.11.3 Detección de intrusiones

Se encarga de detectar el tráfico malicioso en la red, mediante:

- Sistema de detección de intrusos en una red (NIDS)
- Sistema de detección de intrusos basado en host (HIDS)
- Wireless IDS (WIDS)
- Monitoreo de integridad de archivos (FIM)

SNORT

Es uno de los IDS utilizados por OSSIM. Los IDSs utilizan distintas técnicas de análisis para alertar al administrador en caso de ver acciones sospechosas. Snort en particular es un NIDS que se encarga de analizar el tráfico de red, inspeccionando el contenido de los paquetes para dar alertas, o incluso, cuando detecta tráfico sospechoso.

Snort es el IDS más utilizado mundialmente, y es probablemente el más completo de su tipo, además realiza análisis de protocolo, búsqueda de contenido, y puede detectar una gran variedad de ataques y pruebas, como overflows, escaneo de puertos, ataques CGI.

Snort monitoriza la red y a través de un conjunto de reglas decide si el tráfico es sospechoso. Las reglas contienen la información que debería contener un paquete para considerarlo sospechoso, como ser la IP origen, el puerto origen, la IP destino, el puerto destino y el contenido del paquete (Chanaluisa Viera, Meza Castillo, & Tasipanta Chicaiza, 2012).

Utilidad en OSSIM:

- Escaneos de puertos
- Gusanos
- Malware
- Violaciones de política (P2P, Mensajería, pornografía)

OSSEC

Es un sistema de detección de intrusos basado en el Host que se encarga de analizar los datos del host y detectar a través de ellos si el host está siendo atacado.

OSSEC realiza esta tarea analizando logs, revisando integridad, monitorizando el registro de Windows, detectando rootkits, etc. Los IDS basados en análisis de logs son llamados LIDS porque detectan errores o ataques usando logs como su fuente de información.

OSSEC, está formado por un administrador central de monitoreo, que recibe información desde agentes, syslog y bases de datos (Chanaluisa, Darwin & Meza, Andres & Tasipanta, Jessica, 2012).

Utilidad en OSSIM

- Recogida de eventos de sistemas Windows y UNIX
- Recogida de eventos de aplicaciones
- Monitorización de ficheros, carpetas y registros (DLP)

KISMET

Kismet es un detector de red inalámbrica 802,11, sniffer y sistema de detección de intrusos. Kismet funciona con cualquier tarjeta inalámbrica que soporte modo de monitorización raw y pudiendo sniffear tráfico del tipo 802.11a, b, g, n.

Kismet también ofrece una arquitectura de Plugin que permite adicionar protocolos non-802.11 para ser decodificados.

Kismet identifica redes recolectando pasivamente paquetes, descubriendo redes ocultas y la presencia de redes no señalizadas a través del tráfico de datos (Kershaw, 2016).

Utilidad en OSSIM:

- Securización de redes inalámbricas
- Detección de rogue AP
- Cumplimiento de normativa (PCI Wireless)

3.11.4 Monitoreo del comportamiento

Detectar comportamientos sospechosos y sistemas en riesgo, mediante:

- Análisis netflow
- Supervisión de disponibilidad del servicio
- La captura de paquetes completa

NAGIOS

Es un sistema de supervisión de red y aplicación. Este nos permite observar hosts y servicios que nosotros especifiquemos, además de alertar cuando sucesos inesperados ocurren en los Host y cuando estos están en buen estado. Nagios fue originalmente diseñado para correr bajo LINUX, aunque también debería funcionar en la mayoría de otros UNIX (Tapia Jardinez & Sánchez Ruiz, 2009).

Algunas de las muchas características de Nagios incluyen:

- Seguimiento de los servicios de red (SMTP, POP3, HTTP, FTP, PING, etc.)
- Seguimiento de los recursos de Host (carga del procesador, uso de disco, etc.)
- Diseño simple de plugins que permite a los usuarios desarrollar fácilmente sus propios chequeos de servicios.
- Chequeo de Servicios de red y/o Recursos de Host en paralelo
- Servicio de notificaciones a contactos cuando se producen problemas en los hosts a través del correo electrónico, mensajes a celular vía SMS, o un método definido por el usuario.
- Rotación automática del archivo de registro (Nagios almacena un historial de los eventos en un archivo con extensión .log y para no hacer de este archivo muy grande Nagios elimina los historiales que son muy viejos).
- Soporte para la implementación de la supervisión redundante de hosts.
- Interfaz Web Opcional para ver el estado de los dispositivos de la red desde cualquier punto de la red, así como las alertas y el historial de los sucesos, etc.

Utilidad en OSSIM

- Disponibilidad de los activos
- Nagios puede realizar comprobaciones en remoto o disponiendo de un agente en la máquina monitorizada
- Nagios dispone de un gran número de plugins para diferentes entornos y herramientas

NFSEN / NFDUMP

NFDump recoge y procesa netflows desde la línea de comandos. NFSen es una interfaz gráfica que permite gestionar y mostrar la información recogida por NFDump.

Netflows es un protocolo de red desarrollado por Cisco que permite recoger información referida al tráfico analizado. Un gran número de dispositivos soportan hoy día Netflow (Lorenzo, 2010).

FPROBE

Recoge los datos de tráfico de red y lo distribuye como flujos netflow hacia el colector especificado Libpcap-herramienta.

OSSIM proporciona una consola integrada donde puede ver información de netflow, desde FPROBE, para ayudar con la respuesta a incidente (AlienVault, 2011).

WIRESHARK

Wireshark es una herramienta que actúa directamente sobre la red, analizando el tráfico, es un instrumento de código abierto, que implementa filtros para realizar las búsquedas; soportan aproximadamente 1 100 puertos, posee además una interfaz fácil de usar, esta herramienta corre sobre sistemas operativos como Windows, Linux, Mac Os, presenta una aplicación portable.

Wireshark trabaja en dos versiones por línea de comandos llamada t-shark y gráfica, cabe mencionar que esta herramienta nos permite analizar los protocolos, fue conocido como Ethereal, usado para solucionar problemas en las redes, también es una herramienta didáctica de enseñanza de redes. Wireshark incluye un completo lenguaje para filtrar y la habilidad de mostrar el flujo reconstruido de una sesión de TCP (Tandazo Jimenez & Rueda Salgado, 2013).

Algunas funciones:

- Trabaja en modo promiscuo
- Software Libre
- Utiliza permisos de Administrador
- Utiliza licencia GPL
- Captura datos en tiempo real directo desde la red o lee datos desde un archivo previo
- Utiliza librería PCAP
- Emplea archivos TCPDUMP
- Trabajo con la mayoría de protocolos
- Es utilizado en múltiples plataformas
- Presenta información detallada del análisis de la red
- Mantiene logs de los paquetes capturados
- Realiza filtrado por paquetes de la información analizada
- Búsquedas ordenadas por protocolos
- Permite obtener estadísticas de los resultados

3.11.5 SIEM

Correlacionar y analizar los datos de seguridad de la red, mediante:

- Gestión de logs
- Correlación de Eventos
- Respuesta al incidente
- Presentación de informes y alarmas

Correlación

La correlación es una de las características fundamentales que definen OSSIM como una plataforma de gestión de eventos de seguridad inteligente y la distingue de IDS / IPS. Ayuda a reducir los falsos positivos mediante la transformación de múltiples eventos de entrada y alarmas a una salida más fiable de manera que hay una cantidad manejable de eventos a prestar atención. La función de correlación consta de correlación cruzada y la correlación lógica (Directiva de correlación). La correlación cruzada sólo funciona con los acontecimientos que han definido IP de destino, ya que tiene que revisar el host de destino para determinar si tiene cualquier vulnerabilidad no en la base de datos y cambia el valor de fiabilidad de la prueba en consecuencia. El valor de fiabilidad del evento es uno de los indicadores que se utilizan para calcular el riesgo de OSSIM (INFOSEC INSTITUTE, 2012).

Directivas

Otra característica fundamental de OSSIM es directivas de correlación. OSSIM viene con 200 directivas de correlación y ellos están escritos en sintaxis basada en XML. El principal objetivo de la Directiva es analizar múltiples eventos y decidir si desea o no generar una alarma basada en reglas y directrices. Esta característica puede prevenir los ataques de día cero o vulnerabilidades desconocidas, ya que está generando una alarma por las reglas siguientes, en lugar de comprobar el evento en la lista de vulnerabilidades conocidas. Un ejemplo simple del uso directiva podría ser generar alarma cuando alguien intenta SSH en un servidor web en múltiples ocasiones (INFOSEC INSTITUTE, 2012).

Calculo de riesgo

La gestión de datos OSSIM consiste en registros sin procesar, eventos, alarmas y tickets. Los registros sin procesar son recibidos de varias fuentes de datos al servidor OSSIM y son normalizados. Los registros normalizados se muestran en la interfaz de administración web bajo SIEM como eventos. Los tickets se pueden abrir manualmente o son generadas automáticamente en OSSIM. El uso típico para el manejo de incidentes en OSSIM sería

revisar las alarmas, crear un ticket de incidentes relevantes, y asignarla al personal apropiado. Las alarmas se generan cuando el valor de riesgo del evento es igual o mayor que uno. El riesgo se calcula utilizando la siguiente fórmula:

Valor del activo (0 – 5) * Prioridad (0 - 5) * Fiabilidad (0 – 10) / 25 = riesgo del evento (0 – 10)

Cada activo en OSSIM tiene un valor de activos entre 0-5. Cuanto mayor sea el número es el más valioso activo. Activo puede ser un host, grupos de hosts, redes y grupos de la red. La prioridad mide la importancia del evento. La medida de la fiabilidad es la probabilidad de un ataque; por ejemplo, un valor alto (9 o 10) significa que el ataque es real (INFOSEC INSTITUTE, 2012)

Informes

El reporte de OSSIM es muy escalable y fácil a trabajar que tiene la capacidad de crear un informe previsto y enviarlo por correo electrónico automáticamente (INFOSEC INSTITUTE, 2012).

SECCION E: Integración OSSIM-COBIT 5

En esta sección, se realiza el mapeo de relaciones entre la herramienta de gestión de la seguridad de la información (OSSIM) y los procesos aplicables según lo propuesto por el marco de referencia COBIT 5. Se verificará como las herramientas integradas de la plataforma Open Source cumplen los indicadores de los procesos habilitadores seleccionados según el caso de estudio.

3.12 Procesos habilitadores seleccionados según el caso de estudio

Tal como se describió en las secciones anteriores, 5 de los dominios principales propuestos por COBIT se relacionaban directamente con los objetivos organizacionales de nuestro caso de estudio, en otras palabras, con su entorno actual, políticas internas y normativas a las cuales está sujeta. Sin embargo, de los procesos habilitadores para cada dominio se seleccionaron únicamente los que guardaban estrecha relación con la seguridad de la información, obteniendo solo 2 dominios y 6 procesos habilitadores correspondientes.

Estos dominios son: Construir, Adquirir e Implementar **(BAI)** y Entregar, dar Servicio y Soporte **(DSS)**. Los procesos habilitadores correspondientes son:

- Gestión de la disponibilidad y capacidad
- Gestión de los activos
- Gestión de la configuración

- Gestión de incidentes de servicio
- Gestión de servicios de seguridad
- Gestión de las operaciones

La justificación para cada proceso habilitador seleccionado se podrá consultar en la sección C 3.9.1 de la presente investigación.

3.13 Indicadores según los procesos de COBIT seleccionados

Según ISACA (2012), cada proceso habilitador propuesto en el marco de referencia cuenta con indicadores o métricas relacionadas que facilitan su evaluacion en base a la información del caso de estudio.

Si bien es cierto, para cada proceso habilitador existen más de una metrica relacionada, la selección de las que se muestran a continuación se basan en los objetivos organizacionales y en la herramienta de gestión, quien se encargara de obtener los valores deseados.

- **Gestión de la disponiblidad y capacidad**
  1. Número de picos de transacciones donde se excede la meta de rendimiento.
  2. Número de incidentes de disponibilidad.
  3. Número de eventos donde la capacidad ha excedido los limites planificados.

- **Gestión de los activos**
  1. Número de activos no utilizados.
  2. Número de activos obsoletos.

- **Gestión de la configuración**
  1. Número de desviaciones entre el repositorio de configuración y la configuración real.

- **Gestión de peticiones e incidentes de servicio**
  1. Número y porcentaje de incidentes que causan interrupción en los procesos críticos de negocio.
  2. Porcentaje de incidentes resueltos dentro de un periodo acordado/aceptable.
  3. Nivel de satisfacción del usuario con la resolución de las peticiones de servicio.

- **Gestión de servicios de seguridad**
  1. Número de vulnerabilidades descubiertas.
  2. Número de rupturas de cortafuegos
  3. Número de incidentes que impliquen dispositivos de usuario final.

4. Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno.
5. Promedio de tiempo entre los cambios y las actualizaciones de cuentas.
6. Número de cuentas.
7. Número de incidentes relacionados con seguridad física.
8. Número de incidentes relacionados con accesos no autorizados a la información.

- **Gestión de las operaciones**
  1. Número de incidentes causados por problemas operativos.
  2. Tasa de eventos comparada con el número de incidentes.
  3. Porcentaje de tipos de eventos críticos cubiertos por sistemas de detección automática.

Estos serán los indicadores evaluados durante la fase de implementación siguiente, cuyo seguimiento será cubierto en su totalidad por la plataforma Open Source propuesta.

3.14 Funciones de seguridad y herramientas integradas de soporte de OSSIM

En el capítulo anterior, se describieron las capacidades y algunas herramientas integradas de OSSIM como plataforma de gestión de la seguridad de la información.

- **Descubrimiento de activos**
  - NMAP (Mapeo de redes)
  - P0F (Identificación pasiva de sistema operativo)
  - PADS (Sistema pasivo de detección de activos)
  - PRADS (Sistema pasivo de detección de activos en tiempo real)

- **Evaluación de vulnerabilidades**
  - OPENVAS (Sistema abierto de evaluación de vulnerabilidades)

- **Detección de intrusiones**
  - SNORT (Sistema de detección de intrusiones)
  - OSSEC (Sistema de detección de intrusiones basada en host)
  - KISMET (Detector de redes inalámbricas, Sniffer e IDS)
- **Monitoreo de comportamiento**
  - NAGIOS (Supervisor de redes y aplicaciones)
  - NFSEN/NFDUMP (Recolector y procesador de netflows)
  - FPROBE (Recolector de datos de tráfico de red)
  - WIRESHARK (Analizador de tráfico de red)

- **SIEM**
  - Correlación
  - Directivas
  - Cálculo de riesgo
  - Informes

La correcta implementación y configuración de dichas herramientas sumado al motor de correlación de la plataforma, favorece la información exacta para la toma de decisiones acertadas frente a innumerables casos relacionados con violaciones a las políticas de seguridad de la información.

SECCION F: Diseño de fases para la implementación en tiempo real

En esta sección, se detallan las fases de aplicación e implementación del modelo conceptual desarrollado en la presente investigación. Se describen los requerimientos, procedimientos y resultados obtenidos en cada una de las fases de prueba que asegurarán el correcto funcionamiento de la plataforma de gestión de seguridad OSSIM 5.2.0 y de la evaluación de las normativas propuestas, teniendo como base el marco de referencia COBIT 5.

3.15 Fases de implementación

El siguiente procedimiento desarrollado en 8 fases, será evaluado y aprobado por el administrador de la red quien proporcionará los recursos necesarios para el despliegue de la primera prueba piloto de evaluación de resultados que finalmente servirá como punto de partida para la implementación del proyecto a nivel de toda la universidad. A continuación, se describen:

FASE 1: DEFINICIÓN DEL TRAMO DE RED Y RECOLECCIÓN DE INFORMACIÓN EN BASE A LA TOPOLOGIA LOGICA ACTUAL

Esta fase es de importante consideración ya que, a través de la definición del tramo de red de aplicación, se harán las configuraciones adecuadas en la plataforma de gestión de la seguridad de la información OSSIM 5.2.0

Requerimientos:

- Definición del tramo de red de aplicación.
- Definición de topología lógica y física del tramo asignado en base a la situación actual de la red.

- Información relevante sobre VLANs en el tramo de aplicación (direcciones, total de host disponibles).
- Información relevante sobre equipos de comunicación en el tramo de red de aplicación asignado (switches, routers, APs, etc.).
- Información relevante sobre equipos de seguridad en el tramo de red de aplicación asignado (IDs, Firewalls, etc.).

Procedimientos:

- Analizar la información recopilada y elaborar un diseño de red donde se incorpore los nuevos servicios de gestión de seguridad de la información en base a la plataforma de software OSSIM 5.2.0. dentro del tramo de red asignado.
- La siguiente imagen muestra un ejemplo ideal de diseño de red:

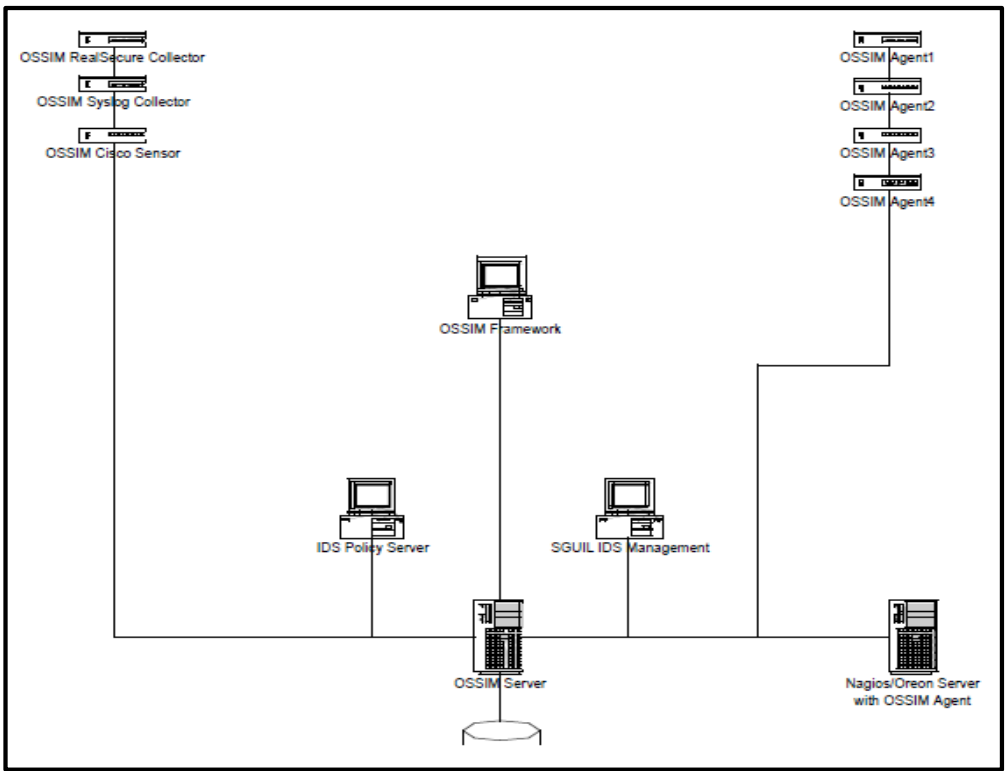


Figura N° 33. Ossim Distribuido
Fuente: (Karg, 2006)

Resultados:

- Diseño de red en base al nuevo servicio de gestión de seguridad de la información OSSIM 5.2.0

FASE 2: PREPARACION DEL ENTORNO DE PRUEBA

La información recopilada en la fase 1 servirá como punto inicial para la instalación de la plataforma de gestión de la seguridad de la información OSSIM así como la configuración de sus agentes, sensores y monitores integrados.

Sin embargo, antes de proceder, es indispensable adecuar un entorno óptimo para el correcto funcionamiento de todas las herramientas de software a usar, a fin de evitar problemas de sobrecargas debido a la falta de recursos de hardware.

Requerimientos:

- 1 **host de prueba** para la instalación de la plataforma OSSIM 5.3.0 que actuará como **servidor** principal.
- 1 **host de interacción** para la administración de la plataforma a través de su interfaz Web
- 1 **host de prueba** para la instalación de **agentes OSSIM** que estarán integrados con el servidor principal (opcional).

El host de prueba que actuará en calidad de servidor, debe contar con las siguientes especificaciones técnicas mínimas:

Tipo de CPU	Intel® Xeon E5620
Tipo de Memoria RAM	DDR3 1333 MHz
Tipo de Disco	SAS 10.000 RPM (204 MB/s)
Rendimiento de la memoria(memcpy)	3310.32 MiB/s
Rendimiento de disco (lectura aleatoria / escritura)	15,97 Mb/s

Según AlienVault (Compañía desarrolladora de los productos OSSIM), es necesario utilizar un hardware similar o mejor para alcanzar un rendimiento óptimo del sistema.

De acuerdo a especificaciones, se hará necesario contar con:

- 4GB de memoria RAM (siendo el recomendado 8GB)
- 1 disco duro de 500 GB (dedicado solo para pruebas)
- Lectora de DVD-ROM SATA 24X (mínimo)
- 2 tarjetas de red (Ethernet e inalámbrica), indispensable para la instalación de herramientas de gestión de seguridad en redes LAN y WLAN.

El host de interacción para la administración de los servicios vía Web, deberá contar con las siguientes especificaciones técnicas mínimas:

Sistema Operativo: Windows 7 o superior (recomendado Windows 10)
Procesador: Intel Core i3 2.8 GHz
Tipo de sistema: Sistema operativo de 64 bits procesador X64
Memoria RAM: 4 GB (Recomendado 8 GB)
Disco Duro: 500 GB

En cuanto al host que actuará como agente integrado al servidor, este contará con especificaciones técnicas similares a la del servidor principal. La utilización del agente solo será necesaria después de evaluar el tamaño del tramo de red de aplicación, ya que, a partir de ello, se podrá decidir si el mismo servidor actuara en función de servidor-sensor o será indispensable su implementación de forma independiente.

Finalmente, todos los equipos de trabajo deberán estar bajo el mismo dominio y tener acceso a Internet con una tasa de transferencia de descarga recomendada.

Procedimiento:

- Adecuar los requerimientos solicitados a los recursos disponibles dentro de la Red Telemática y preparar, junto con el administrador de la red, el entorno necesario para el correcto funcionamiento de todas las herramientas de gestión de la seguridad.
- Realizar las pruebas técnicas de funcionamiento de los equipos a utilizar y verificar el cumplimiento de los requisitos mínimos.

Resultados:

- Informe de aprobación técnica del entorno de red desarrollado para el inicio de pruebas.

FASE 3: INSTALACION DE LA PLATAFORMA OSSIM 5.2.0 Y CONFIGURACIONES INICIALES

Con el entorno listo para ser usado y la información detallada de la topología de red asignada, se procede a realizar la instalación del sistema de gestión de la seguridad de la información Open Source de AlienVault OSSIM en su versión 5.3.0 en el equipo de prueba que actuará como servidor principal, realizando las configuraciones iniciales necesarias para el arranque del mismo.

Requerimientos:

- OSSIM-5.2.0.iso archivo de formato grabado en un DVD y descargado de https://www.alienvault.com/products
- Definición de los parámetros iniciales de configuración de la plataforma (nombre de organización, cuenta de administrador, contraseñas, configuración de dirección IP estática para acceso, configuración de puerta de enlace predeterminada, etc.).

Procedimientos:

- Instalar la plataforma OSSIM 5.2.0 en el servidor de prueba.
- Realizar las configuraciones iniciales de instalación.
- Realizar pruebas iniciales a través del entorno web, a través del equipo de interacción solicitado.
- Realizar las primeras configuraciones de la plataforma a través del entorno web (usuario administrador, contraseñas, etc.).
- Realizar el primer análisis de descubrimiento de activos como prueba de conformidad del correcto funcionamiento de la plataforma.

Entregable:

- Sistema Operativo OSSIM 5.2.0 configurado y testeado según los parámetros establecidos.

FASE 4: INSTALACION Y CONFIGURACION DE SENSORES, AGENTES Y MONITORES

El correcto funcionamiento de la plataforma de gestión de seguridad en el primer análisis de descubrimiento de activos es el paso inicial para realizar el despliegue de esta fase.

El nuevo diseño de red en base a la implementación de OSSIM permite determinar si será indispensable la utilización de sensores especializados en el tramo de red de aplicación, así como la configuración de sus detectores o monitores quienes brindarán información relevante al servidor central.

Si bien el uso de sensores especializados es indispensable en una puesta en marcha real, para nuestro caso de estudio se optará por tener una alternativa adicional: que el servidor principal actué como servidor-sensor; esto para ahorrar problemas en caso de no contar con los equipos necesarios para la instalación.

Requerimientos:

- Información privilegiada sobre equipos de seguridad que serán integradas a la base de datos de OSSIM.
- Información privilegiada sobre equipos de comunicaciones que serán integrados a la base de datos de OSSIM.
- Información privilegiada del controlador de dominio que será útil para la administración del mismo desde la plataforma de gestión de seguridad OSSIM.
- Otra información privilegiada adicional necesaria.

Procedimientos:

- Instalación del sensor en el equipo de prueba 2 y configuración de integración con el servidor principal
- Instalación y configuración de monitores o detectores tanto en el servidor principal como en el sensor (Nagios, OSSEC, Suricata, OpenVas, etc.).
- Pruebas simples de funcionamiento.
- Integración de la plataforma con el servidor de dominio actual para su administración.
- Integración de equipos de comunicaciones con la base de datos.
- Integración de equipos de seguridad con la base de datos.
- Pruebas finales de funcionamiento.

Resultados:

- Plataforma OSSIM 5.2.0 integrada y configurada según topología definida.
- Complementación del diseño de red de aplicación según los avances logrados.

FASE 5: DEFINICIÓN DE POLITICAS Y DIRECTIVAS DE CORRELACIÓN

Todos los sensores y agentes de OSSIM envían sus eventos al servidor principal; para tratar dichos eventos (del mismo servidor o externos) AlienVault permite la creación de políticas de seguridad, las cuales constan de dos partes: condiciones y consecuencias.

Además, OSSIM cuenta con un motor de correlación que permite al administrador de red crear directivas de correlación para unir diferentes eventos de “bajo nivel” en una única alarma de “alto nivel”, cuyo objetivo es aumentar la sensibilidad y la fiabilidad de los eventos de seguridad.
Cabe resaltar que OSSIM cuenta con algunas directivas de correlación integradas en base a normas y estándares internacionales como ISO.

Requerimientos:

- Informes relacionados a políticas de gestión de la información actuales que son aplicadas en la red telemática.
- Información de los activos, grupos de activos, redes y / o grupos de redes
- Información de tipos de eventos, los que pueden ser: Grupo Fuente de datos (documentos Microsoft Office, PDFs, anomalías en la red, datos sensibles detectados en el tráfico de red, etc.) y taxonomía (según el tipo de producto, categoría y subcategoría)
- Información del sensor
- Prioridad del evento

Procedimientos:

- Analizar las políticas básicas aplicables en la actualidad.
- Establecimiento de las políticas de seguridad en base a los procesos definidos por COBIT 5 como marco de referencia.
- Definir y configurar las condiciones de nuevas políticas de gestión como: origen, destino, puerto de origen, tipo de evento, etc.
- Definir y configurar las consecuencias de las nuevas políticas.
- Definir y configurar las reglas de correlación

Resultados:

- Plataforma OSSIM, integrada y configurada con controles de seguridad eficaces en base a requerimientos.
- Informe de aumento de fiabilidad y sensibilidad de alertas producidas.

FASE 6: CONFIGURACION DE TICKETS DE INCIDENCIA Y PRUEBAS DE ENVIO

La definición e implementación de políticas de seguridad en la plataforma OSSIM deja casi al sistema en completo funcionamiento. Sin embargo, las alertas producidas deberán ser escalables hasta el administrador de la red y encargados para su respectivo conocimiento, con el fin de tomar medidas correctivas cuando sea necesario.

OSSIM tiene un sistema interno de incidencias que permite delegar tareas al administrador u otros usuarios y dar seguimiento a los eventos y alarmas, estos son llamados TICKETS.

Por otro lado, permite configurar el servidor de correo (protocolo SMTP) de tal manera que los reportes se puedan enviar a una dirección de correo especificada.

El server Nagios instalado en el Servidor OSSIM, por ejemplo, utiliza este mismo medio para enviar notificaciones al correo electrónico si hay algún inconveniente con la disponibilidad de los servicios.

Requerimientos:

- Información de los usuarios u entidades a quienes se les puede asignar un ticket.
- Prioridad de la incidencia
- Información del tipo de incidencia por ejemplo: anomalía, fallas del sistema, violación de política, virus, etc.
- Definiciones referentes a fechas de inicio y fin de los eventos relacionados.
- Información del servidor SMTP, puerto.
- Información privilegiada de administrador referente a correo para recepción de incidencias.
- Definición de direcciones de correo electrónico hacia donde se reenviará la información.

Procedimientos:

- Creación de tickets manuales en base a información solicitada y requerimientos del administrador.
- Creación de tickets automáticas en base a información solicitada y requerimientos del administrador.
- Configuración en consola del servidor SMTP, direcciones de correo electrónico de origen y destino para el tratamiento de envío de alertas.
- Pruebas de envío de alertas.

Resultados:

- Información detallada de los tickets: status, prioridad, etc.
- Envío de notificaciones al correo electrónico predefinido, envío de reporte a los usuarios que lo requieran.

***FASE 7*:** ANALISIS DE CUADROS DE MANDO INTEGRADOS

En esta fase, se analizarán los resultados obtenidos de forma detallada de la integración de todas las herramientas configuradas en una única consola centralizada. El entendimiento de los cuadros de mando y reportes generados permitirá, a los encargados, tener una visión de alto nivel del estado de seguridad de la red con el fin de tomar decisiones oportunas cuando sean necesarias.

El cuadro de mandos monitorizará una serie de indicadores definidos que medirán el estado de seguridad de la organización, definiendo umbrales que debe cumplir la organización.

Gracias a los cuadros de mando se sabrá en todo momento qué ocurre en la red, mostrando la información más concisa y simple posible.

Requerimientos:

- Haber culminado con éxito las fases anteriores.

Procedimientos:

- Generación de reportes y cuadros de mando.

Resultados:

- Plataforma OSSIM de gestión de la seguridad de la información en correcto funcionamiento en base a políticas establecidas y soportada por los procesos del marco de referencia COBIT 5.

FASE 8: EVALUACION FINAL DEL IMPACTO ALCANZADO

Finalmente, se realizará una evaluación de la situación actual en la red Telemática antes y después de la implementación de la plataforma OSSIM, analizando si las herramientas de seguridad existentes proporcionan información útil y relevante para la toma de decisiones en el momento oportuno.

3.16 Implementación del entorno de prueba

Una vez definido el tramo de red de prueba, así como la secuencia de 8 fases de implementación, se procede a realizar la instalación y configuración de la plataforma OSSIM en su versión 5.3 dentro del entorno de prueba a fin de evaluar los resultados esperados que darán validez al modelo propuesto.

Para este caso, se procedió a realizar un manual “Superusuario” de implementación y configuración detallado, teniendo en cuenta los parámetros establecidos anteriormente. El manual detallado se puede consultar en el Apéndice B.

CAPÍTULO 4. MARCO METODOLÓGICO

4.1 Hipótesis

El uso de una plataforma de Gestión de Seguridad Open Source bajo un entorno de objetivos de control según el enfoque de COBIT tiene un impacto positivo y eficaz en la toma de decisiones de TI en la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

4.2 Mapeo de relación de variables

En el siguiente gráfico, se resume la relación existente entre los procesos habilitadores de COBIT (dentro de sus indicadores correspondientes), así como de las funciones esenciales y herramientas integradas que posee la plataforma de gestión de la seguridad de la información OSSIM. Es a través de esta relación que lograremos la integración de OSSIM bajo el entorno de los objetivos de control de COBIT 5 para la toma de decisiones, en base a información seleccionada y apropiada.

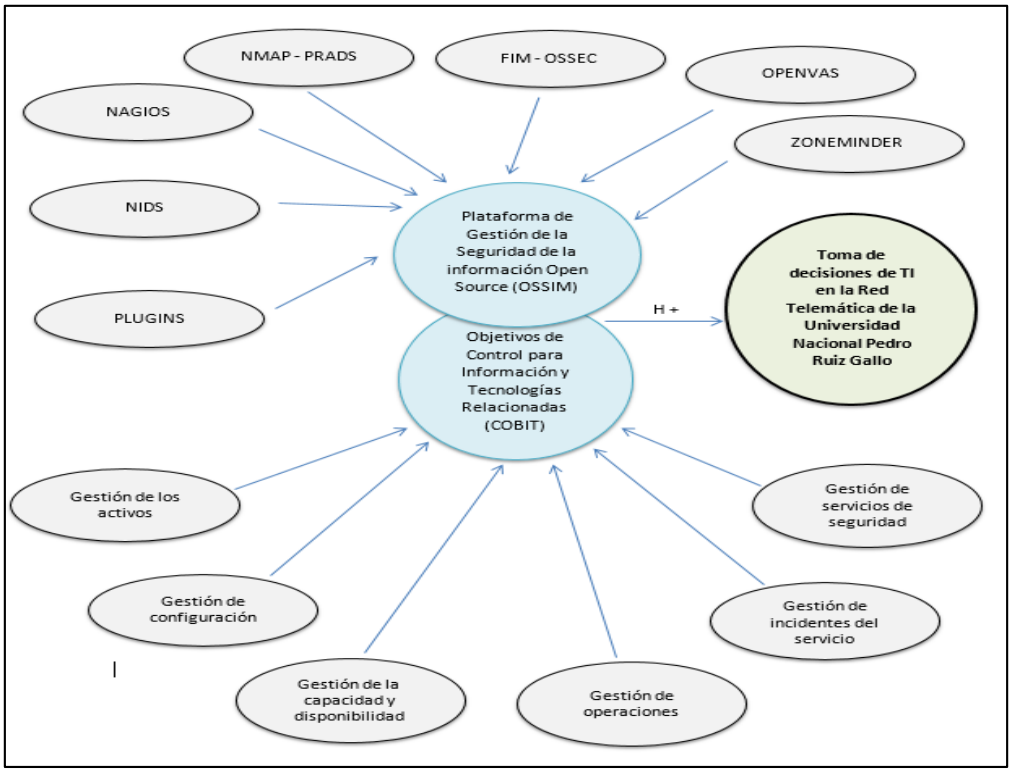


Figura N° 34. Modelo relacional propuesto
Fuente: Los autores

4.3 Operacionalización de variables

A continuación, se mapean los procesos habilitadores de COBIT que se validarán con la herramienta:

Tabla N° 31: Cuadro de operacionalización de variables

PROCESO COBIT 5	INDICADORES
Gestión de la disponibilidad y capacidad	- Número de picos de transacciones donde se excede la meta de rendimiento - Número de incidentes de disponibilidad - Número de eventos donde la capacidad ha excedido los límites planificados
Gestión de los activos	- Numero de activos no utilizados - Número de activos obsoletos
Gestión de la configuración	- Numero de desviaciones entre el repositorio de configuración y la configuración real
Gestión de incidentes de servicio	- Número y porcentaje de incidentes que causan interrupción en los procesos críticos de negocio - Porcentaje de incidentes resueltos dentro de un periodo acordado/aceptable - Nivel de satisfacción del usuario con la resolución de las peticiones de servicio
Gestión de servicios de seguridad	- Número de vulnerabilidades descubiertas - Número de rupturas de cortafuegos - Número de incidentes que impliquen dispositivos de usuario final - Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno - Promedio de tiempo entre los cambios y las actualizaciones de cuentas - Número de cuentas - Número de incidentes relacionados con seguridad física - Número de incidentes relacionados con accesos no autorizados a la información
Gestión de Operaciones	- Número de incidentes causados por problemas operativos - Tasa de eventos comparada con el número de incidentes - Porcentaje de tipos de eventos críticos cubiertos por sistemas de detección automática

Fuente: Los autores

4.4 Contrastación de la hipótesis

4.4.1 Medición de los indicadores de acuerdo a los procesos de COBIT 5 seleccionados para el caso de estudio

A continuación, se describe, para cada proceso aplicable, los resultados obtenidos que sustentan los 20 indicadores de medición del modelo propuesto, referente al uso de COBIT 5. Como se recordará, estos procesos se obtuvieron en el capítulo 3 sección C de acuerdo a los objetivos de TI que persigue el caso de estudio.

<u>Proceso habilitador</u>: GESTIÓN DE LA DISPONIBILIDAD Y CAPACIDAD.

1. Número de picos de transacciones donde se excede la meta de rendimiento

OSSIM permite monitorizar servicios de base de datos como MySQL y visualizar información sobre transacciones que se encuentran en estado de espera o de bloqueo por largo tiempo. El nivel crítico predeterminado, para este evento, es 25 y la alerta es 10.

Figura N° 35. Monitorización de base datos MYSQL
Fuente: Resultados obtenidos por OSSIM

Por otro lado, WEBINJECT es un plugin de Nagios que permite monitorizar el nivel de respuesta de sitios web controlando su funcionalidad a través de 4 fases:

- **Fase 1** - Conectarse a la aplicación
- **Fase 2** - Autenticar a un usuario bajo el sistema de acceso / autenticación de la aplicación web
- **Fase 3** - Verificar que se puede navegar a través de la aplicación mientras se está autenticado.
- **Fase 4** - Hacer una muestra de que tiene acceso a una base de datos para verificar que está disponible para la aplicación web

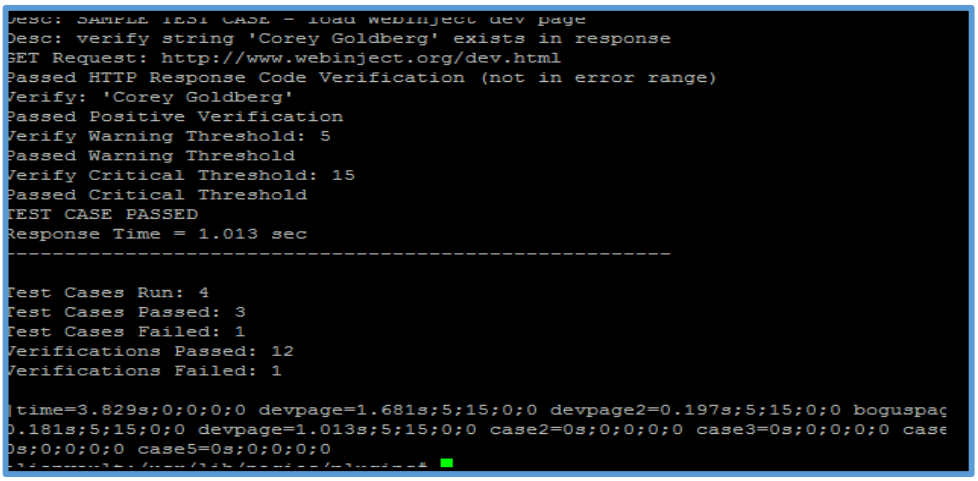


Figura N° 36. Webinject integrado a OSSIM como plugin de Nagios
Fuente: Resultados obtenidos por OSSIM

2. Número de incidentes de disponibilidad

OSSIM tiene la capacidad de integrar el plugin Nagios en su módulo SIEM, logrando visualizarlo en el dashboard del sistema.

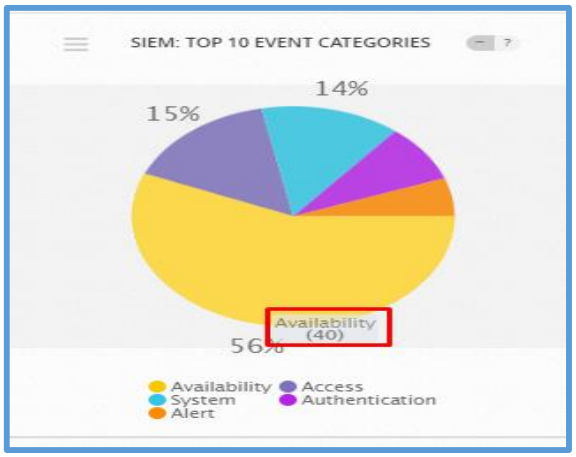


Figura N° 37. Dashboard por categoría de eventos
Fuente: Resultados obtenidos por OSSIM

En este caso podemos apreciar que han ocurrido 40 eventos de disponibilidad en los equipos monitoreados.

3. Número de eventos donde la capacidad ha excedido los límites planificados

Nagios puede monitorear el uso de memoria RAM, uso de espacio de disco, etc. Tener esta información resulta útil para un administrador en el supuesto de que tenga servidores que brindan varios servicios en un mismo equipo. Ver estos datos le ayudará a tomar una decisión acertada para evitar que el equipo se sobrecargue y los servicios dejen de operar.

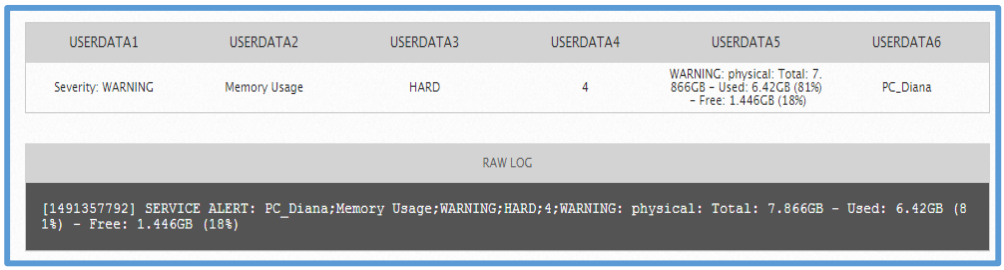


Figura N° 38. Monitoreo del uso de memoria RAM
Fuente: Resultados obtenidos por OSSIM

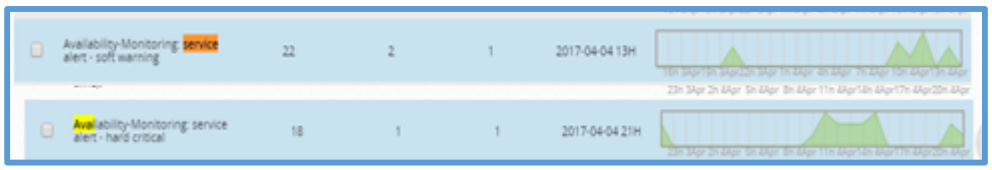


Figura N° 39. Número de eventos de disponibilidad de hardware hay en red
Fuente: Resultados obtenidos por OSSIM

Como apreciamos en las imágenes, un equipo monitorizado genera una advertencia de que el uso de su memoria RAM es superior al 80%. Por otro lado, es posible mostrar también información de manera agrupada sobre cuántos eventos de disponibilidad en hardware han ocurrido en una red.

<u>Proceso habilitador</u>: GESTIÓN DE ACTIVOS.

4. Número de activos no utilizados

OSSIM realiza un inventario de activos y además nos permite habilitar el monitoreo de disponibilidad.

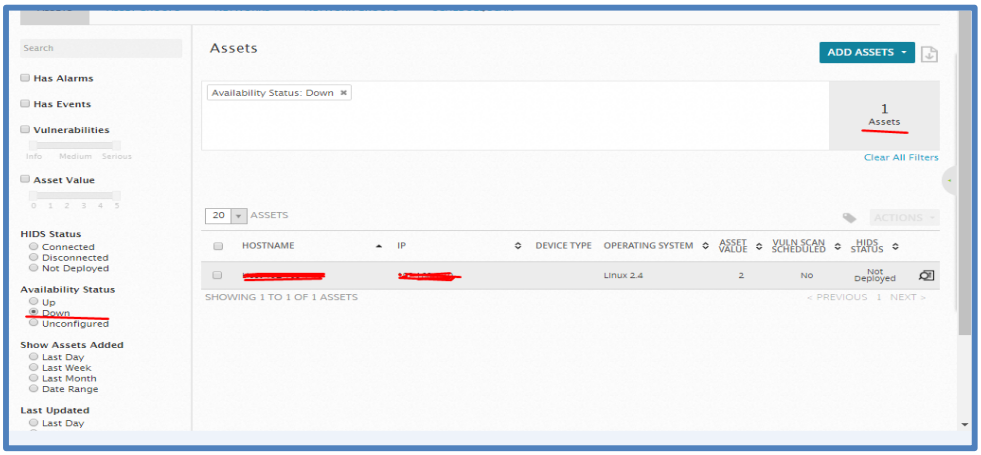


Figura N° 40. Descubrimiento de activos Ossim
Fuente: Resultados obtenidos por OSSIM

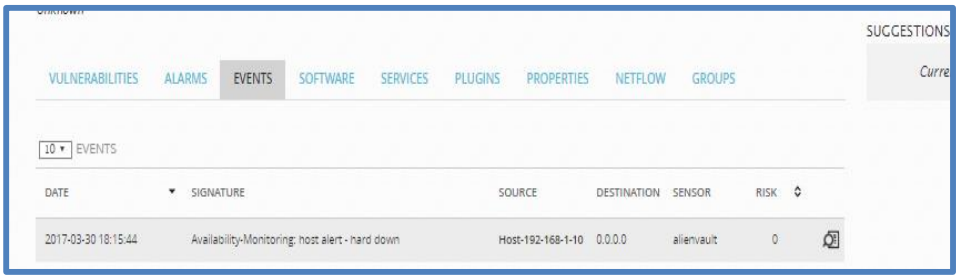


Figura N° 41. Detalle de eventos ocurridos en nuestro equipo
Fuente: Resultados obtenidos por OSSIM

En este caso, podemos filtrar nuestros activos que se encuentran como DOWN y luego de manera independiente visualizar cuándo fue la última vez que estuvieron encendidos.

5. Numero de activos obsoletos

OSSIM puede realizar un escaneo de red para determinar que equipos se encuentran tecnológicamente obsoletos, por ejemplo, al determinar un sistema operativo que actualmente no tiene soporte o al determinar equipos con recursos limitados.

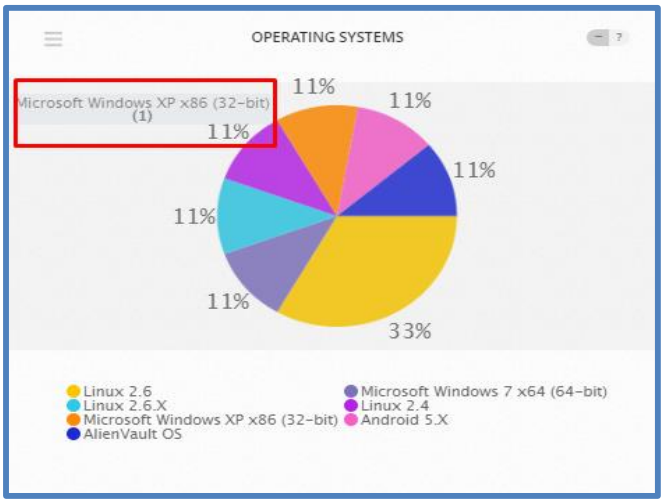


Figura N° 42. Dashboard según sistema operativo de los equipos en red
Fuente: Resultados obtenidos por OSSIM

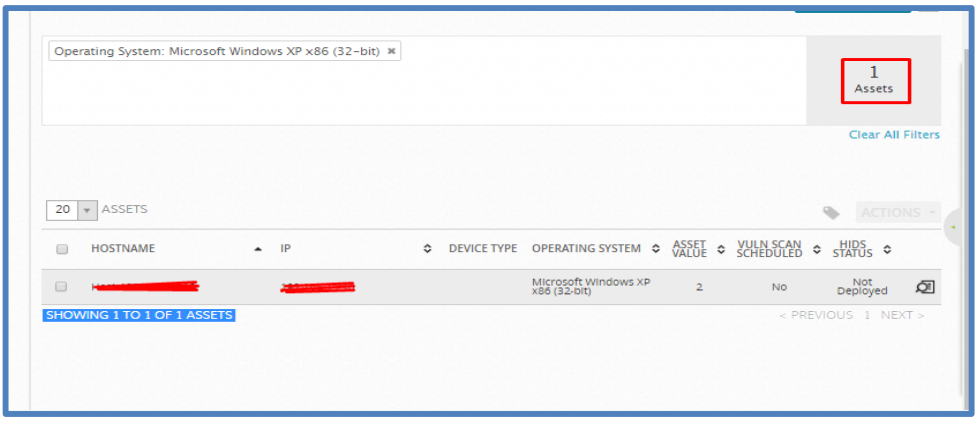


Figura N° 43. Consulta de número de equipos en red según sistema operativo
Fuente: Resultados obtenidos por OSSIM

<u>Proceso habilitador</u>: GESTIÓN DE LA CONFIGURACIÓN.

6. Numero de desviaciones entre el repositorio de configuración y la configuración real

OSSIM integra herramientas como Prads y Arpwatch que permiten ver cambios de S.O, MAC e IP.

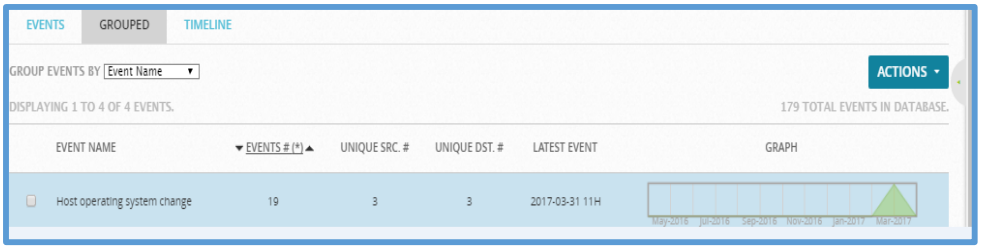


Figura N° 44. Número de eventos de cambio de sistema operativo en los hosts
Fuente: Resultados obtenidos por OSSIM

Esta información permite al administrador visualizar cambios en el sistema operativo o en algún programa monitorizado tanto de manera individual como grupal.

<u>Proceso habilitador</u>: GESTIÓN DE INCIDENTES DE SERVICIO.

7. Número y porcentaje de incidentes que causan interrupción en los procesos críticos de negocio

Podemos considerar aquí los exploits que son utilizados con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

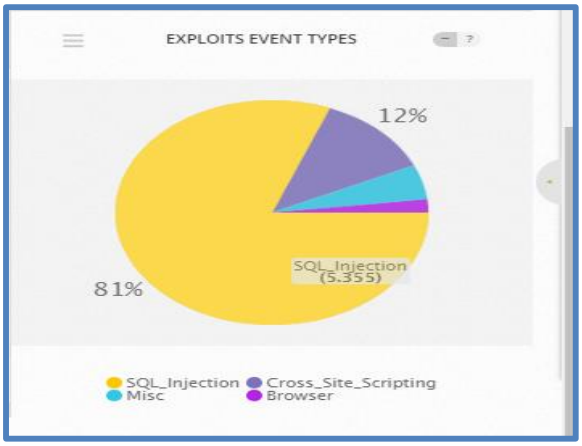


Figura N° 45. Número de eventos de exploits
Fuente: Resultados obtenidos por OSSIM

También podemos considerar: los incidentes de sistema, disponibilidad y programas malware.

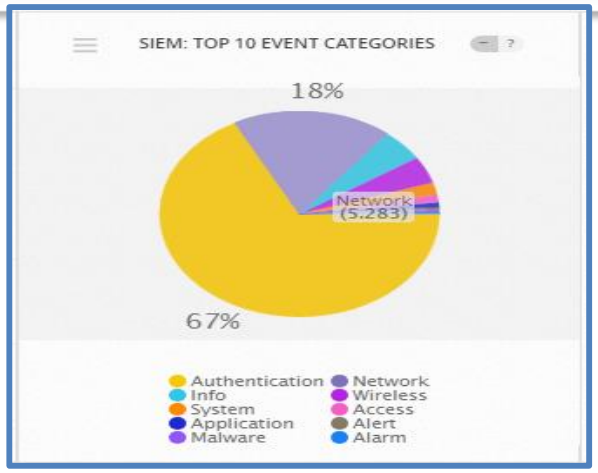


Figura N° 46. Eventos por categorías
Fuente: Resultados obtenidos por OSSIM

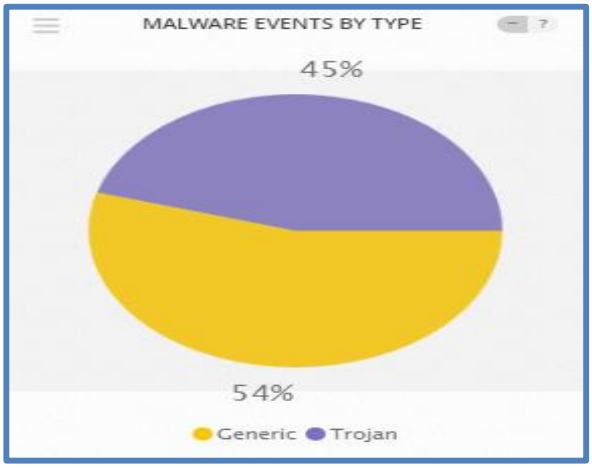


Figura N° 47. Eventos por Malware
Fuente: Resultados obtenidos por OSSIM

8. Porcentaje de incidentes resueltos dentro de un periodo acordado / aceptable

Aunque no exista un nivel de acuerdo de servicio interno documentado, los incidentes son resueltos según la prioridad que tengan.

OSSIM puede generar tickets de las incidencias de forma manual automática, designar un usuario según los incidentes ocurridos y cerrar dicho ticket cuando el personal soluciona el problema.

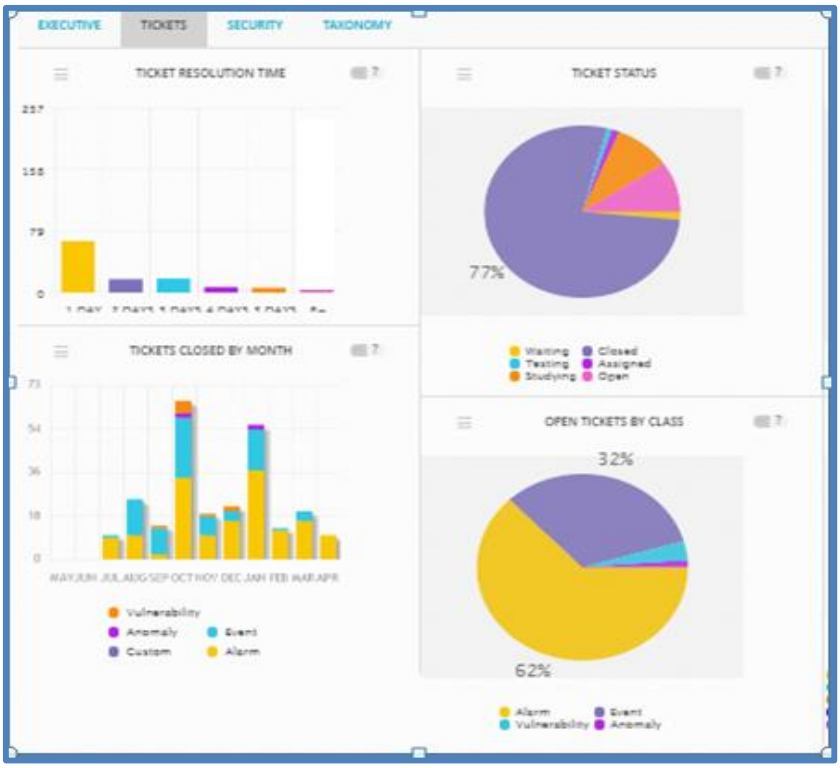


Figura N° 48. Dashboard de tickets de incidencias
Fuente: Resultados obtenidos por OSSIM

Como apreciamos, el 77% de las incidencias han sido solucionadas en un periodo de tiempo aceptable.

9. Nivel de satisfacción del usuario con la resolución de las peticiones de servicio

Al solucionar los incidentes en un periodo aceptable, los usuarios tendrán un nivel de satisfacción alto, ya que el sistema muestra la información confiable y oportuna de los incidentes, a fin de que puedan solucionarse lo más pronto posible.

<u>Proceso habilitador</u>: GESTIÓN DE SERVICIOS DE SEGURIDAD.

10. Número de vulnerabilidades descubiertas

OSSIM realiza escaneo de vulnerabilidades a través de la herramienta OpenVas.

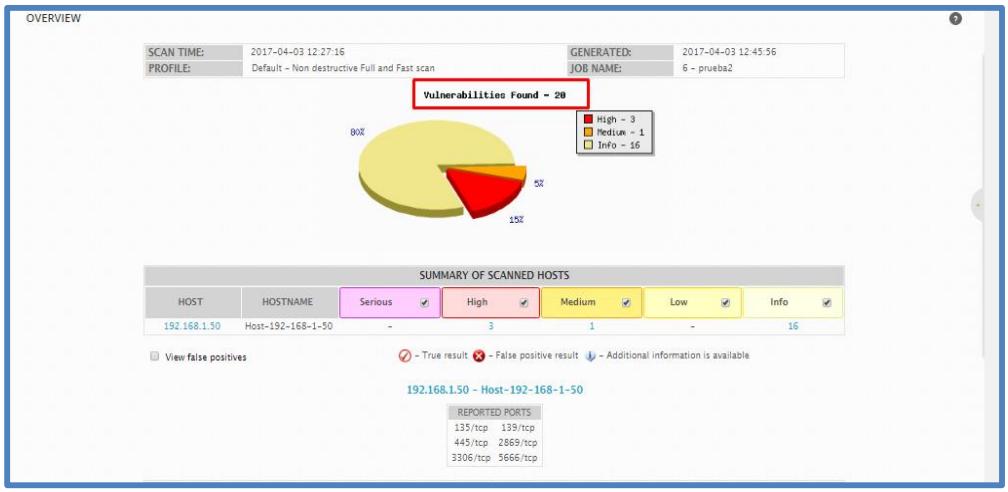


Figura N° 49. Vulnerabilidades detectadas por niveles
Fuente: Resultados obtenidos por OSSIM

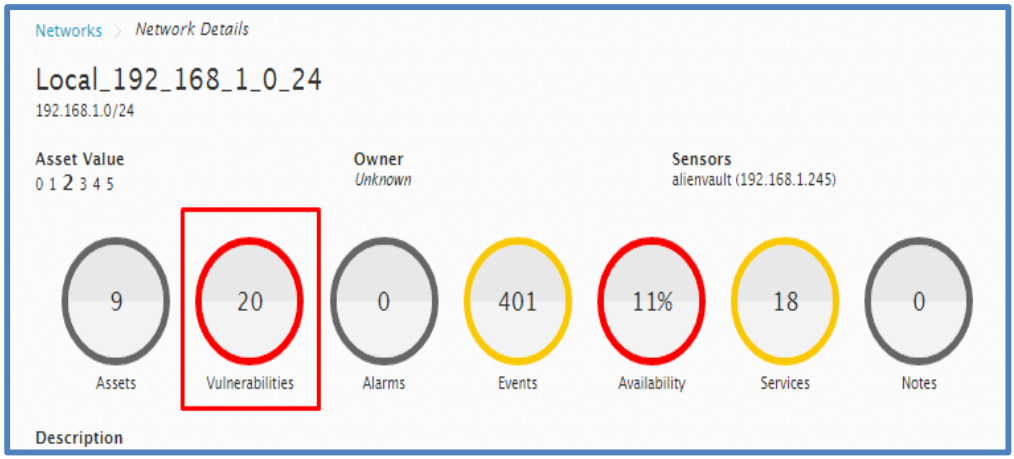


Figura N° 50. Número de vulnerabilidades en red
Fuente: Resultados obtenidos por OSSIM

Como apreciamos en la imagen, al escanear nuestro entorno de red se detectaron 20 vulnerabilidades que deben ser solucionadas.

11. Numero de rupturas de cortafuegos

OSSIM permite la integración con firewalls de diferentes marcas como Cisco ASA, Palo Alto, etc.

En una investigación de Gartner sugiere que, hasta el 2020, el 99% de las brechas de cortafuegos será causado por errores de configuración de servidor de seguridad simples, no defectos.

OSSIM recopila información de los diferentes firewalls que integra y permite la creación de reglas.

7002	2	System	Information	-	AlienVault HIDS: Generic template for all firewall rules.
7002	4100	System	Information	-	AlienVault HIDS: Firewall rules grouped.

Figura N° 51. Eventos de reglas de firewall
Fuente: Resultados obtenidos por OSSIM

Además, recopila información y accesos permitidos y denegados por el firewall como se muestra en las siguientes dos imágenes.

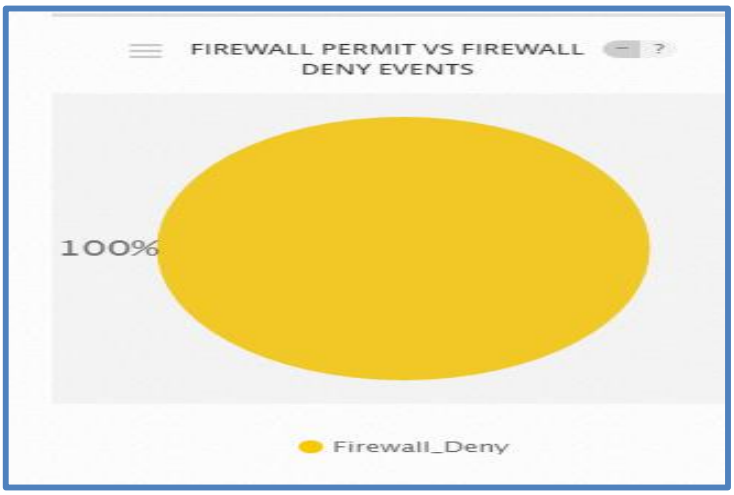


Figura N° 52. Eventos de accesos permitidos y denegados por el firewall
Fuente: Resultados obtenidos por OSSIM

EVENT NAME	EVENTS # (*)	UNIQUE SRC. #	UNIQUE DST. #	LATEST EVENT	GRAPH
ASA: A UDP packet containing a DNS query or response was denied	1.312	1	1.291	1491321600	28 Mar 29 Mar 30 Mar 31 Mar 1 Apr 2 Apr 3 Apr 4 Apr
ASA: ICMP Denied	1.312	1	1	1491321600	28 Mar 29 Mar 30 Mar 31 Mar 1 Apr 2 Apr 3 Apr 4 Apr

Figura N° 53. Denegación del firewall
Fuente: Resultados obtenidos por OSSIM

12. Número de incidentes que impliquen dispositivos de usuario final

Mediante la herramienta, podemos clasificar los activos de la red en grupos, pudiendo así, visualizar sus eventos.

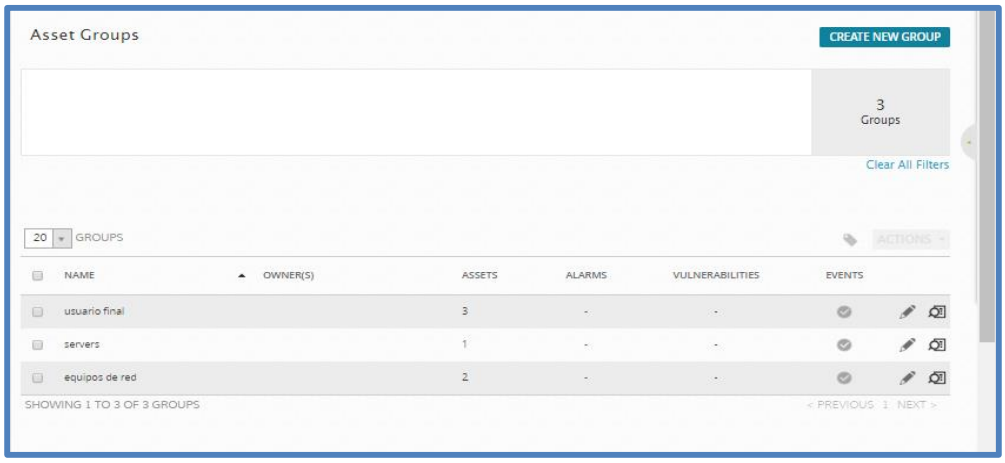


Figura N° 54. Grupos de activos en la red
Fuente: Resultados obtenidos por OSSIM

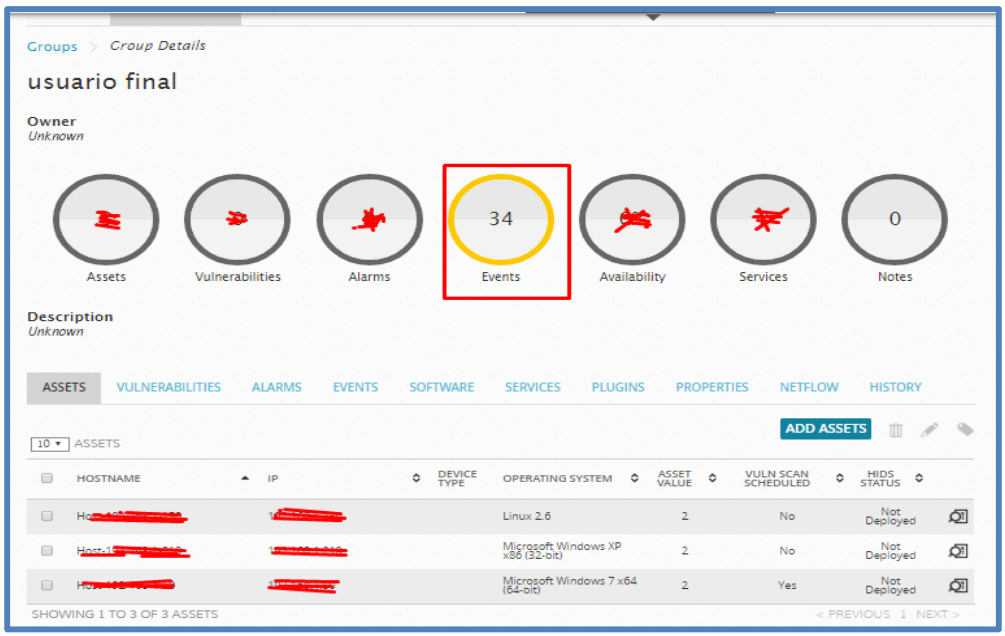


Figura N° 55. Activos de usuario final y eventos ocurridos en ese grupo de activos
Fuente: Resultados obtenidos por OSSIM

Como apreciamos en la imagen anterior el grupo de activos de usuarios presentan 34 incidentes.

13. Numero de dispositivos de usuario final no autorizados detectados en la red o en el entorno

Mediante el escaneo de red, OSSIM puede detectar los nuevos equipos conectados o agregados a la red.

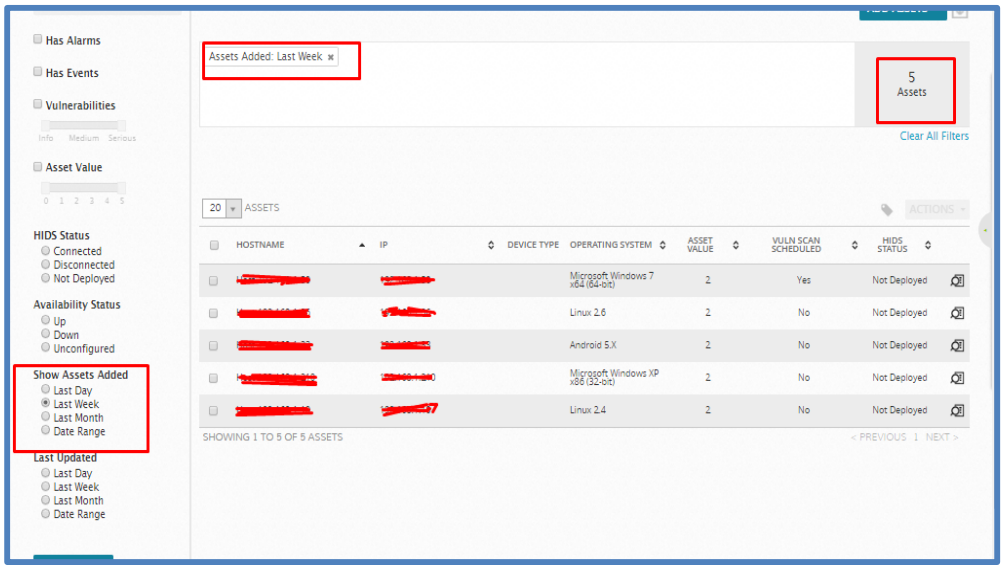


Figura N° 56. Activos agregados a la red últimamente
Fuente: Resultados obtenidos por OSSIM

Podemos clasificar los nuevos activos conectados por semana, mes o por un rango definido por el usuario.

En este caso, detectamos los conectados la última semana con lo que el administrador podrá decidir cuáles serán autorizados para conectarse a la red.

14. Promedio de tiempo entre los cambios y actualizaciones de cuentas

OSSIM muestra información de los cambios y modificaciones en las cuentas usuarios, así como el tiempo en que ocurrieron dichos cambios.

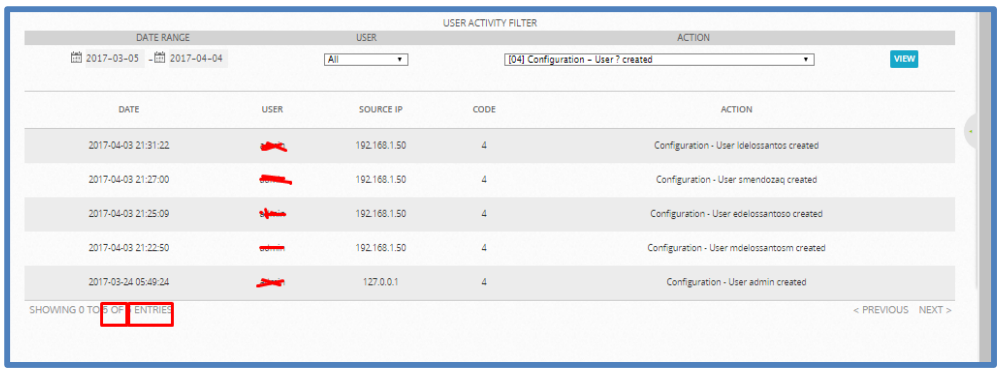


Figura N° 57. Actividad de usuarios
Fuente: Resultados obtenidos por OSSIM

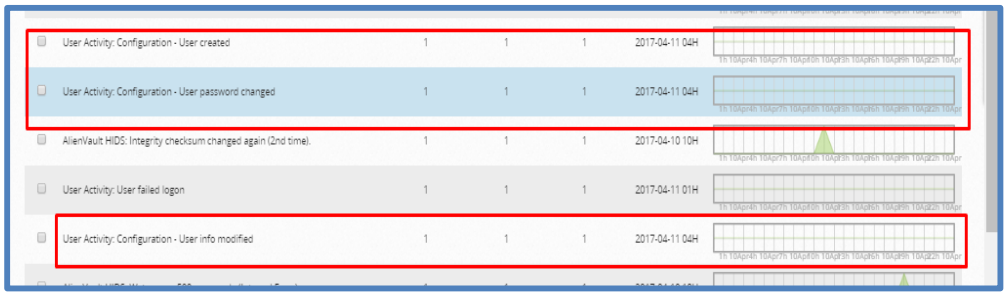


Figura N° 58. Eventos de actividad de usuario por grupos
Fuente: Resultados obtenidos por OSSIM

15. Número de cuentas

OSSIM permite la integración con el controlador Active Directory (Windows Server) mediante la herramienta LDAP, de tal manera que las cuentas de usuario que se creen sean cuentas de dominio.

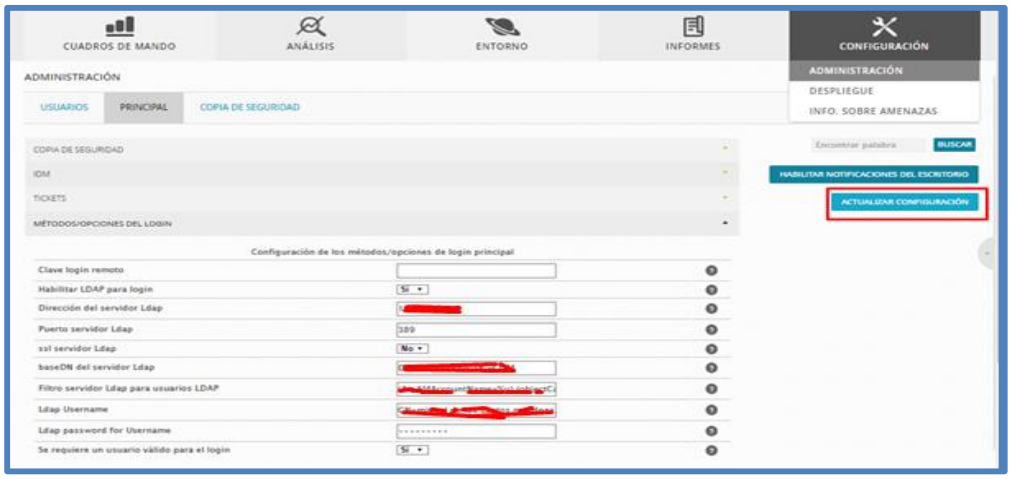


Figura N° 59. Integración OSSIM con LDAP
Fuente: Resultados obtenidos por OSSIM

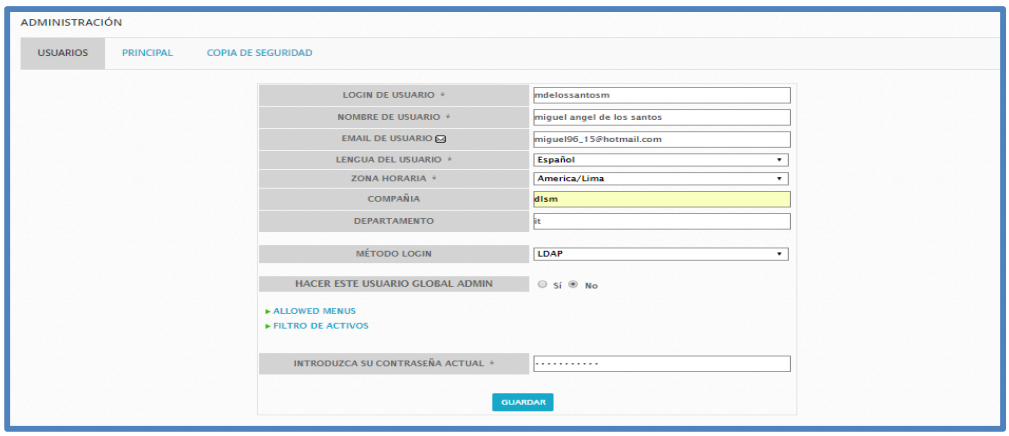


Figura N° 60. Creación de cuentas de usuarios mediante LDAP
Fuente: Resultados obtenidos por OSSIM

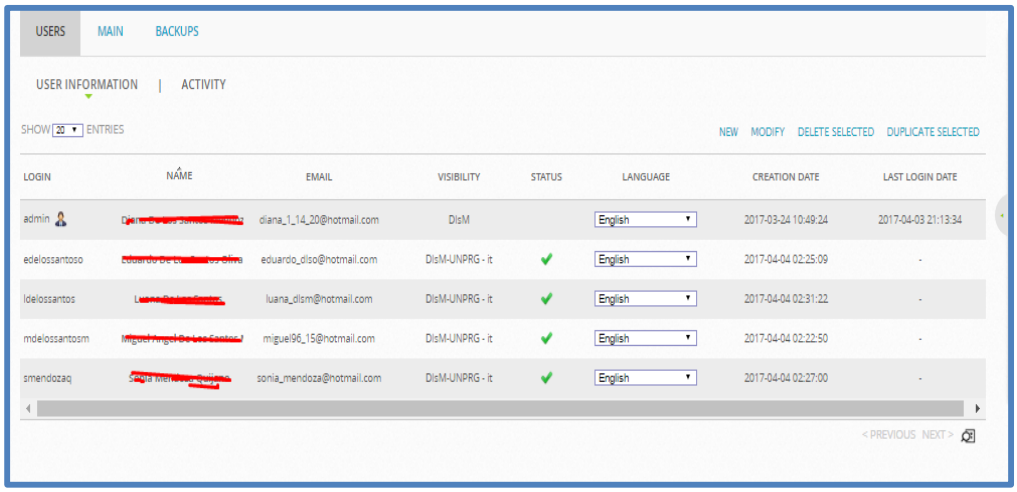


Figura N° 61. Números de cuentas de usuarios
Fuente: Resultados obtenidos por OSSIM

OSSIM muestra la lista de cuentas de usuarios creada. En este caso vemos que se han creado 5 cuentas con usuarios del dominio.

16. Número de incidentes relacionados con seguridad física

OSSIM tiene la capacidad de integrarse con varias herramientas y dispositivos, en este caso específicamente, con dispositivos de seguridad física como el de panel de alarmas de incendio y con cámaras IP de vigilancia. (Osorio Betancur, Cárdenas, Bedoya, Latorre, & Madrid Molina, 2008)

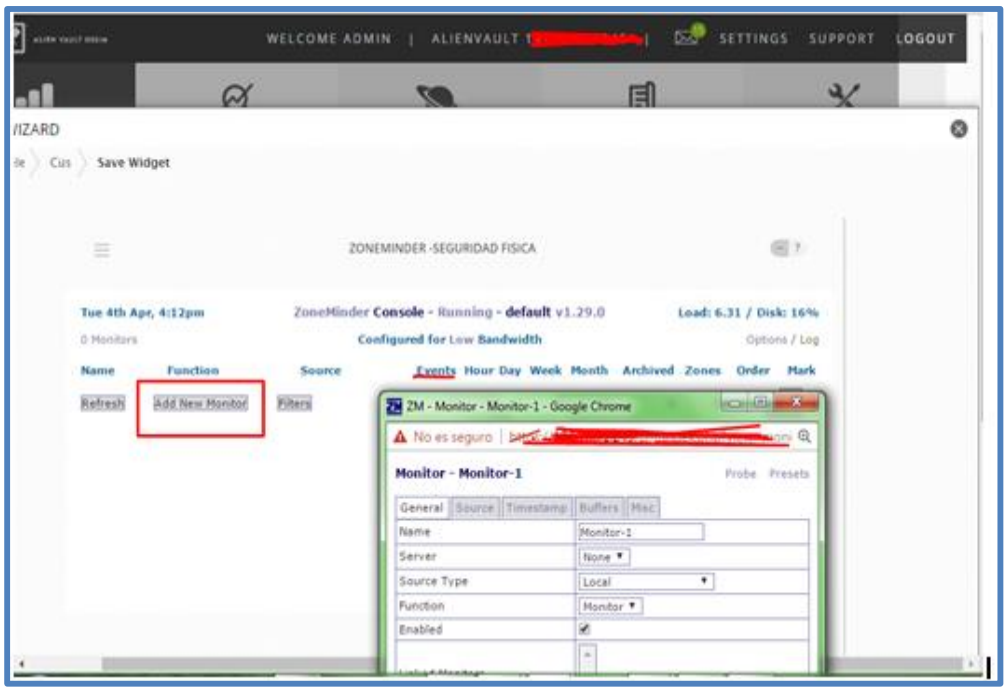


Figura N° 62. Integración ZoneMinder - OSSIM
Fuente: Resultados obtenidos por OSSIM

17. Número de incidentes relacionados con accesos no autorizados a la información

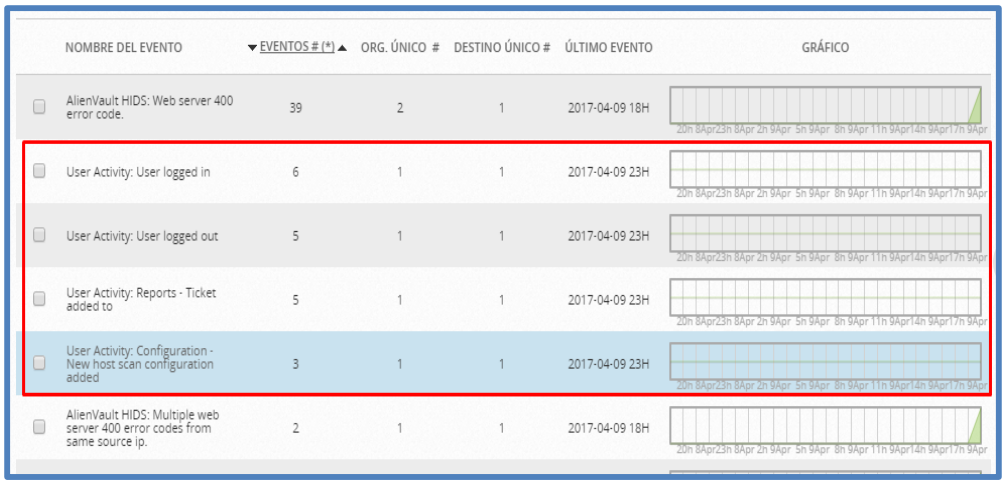
El detectar el evento de "USB agregado/removido" le ayudara al administrador a identificar en que PC y que unidad de almacenamiento ha sido conectado sin autorización.

AlienVault HIDS: USB device added/removed	6	1	1	2017-04-08 22H

Figura N° 63. UBS conectados / desconectados a los host
Fuente: Resultados obtenidos por OSSIM

En este caso hemos detectado 5 eventos de "USB agregado / removido".

También podemos detectar que usuario del dominio ha modificado la información recopilada por OSSIM, como por ejemplo cambios en alguna configuración. El administrador recibirá dicha información y detectara que usuarios han accedido a la información sin autorización.



NOMBRE DEL EVENTO	EVENTOS # (*)	ORG. ÚNICO #	DESTINO ÚNICO #	ÚLTIMO EVENTO	GRÁFICO
AlienVault HIDS: Web server 400 error code.	39	2	1	2017-04-09 18H	
User Activity: User logged in	6	1	1	2017-04-09 23H	
User Activity: User logged out	5	1	1	2017-04-09 23H	
User Activity: Reports - Ticket added to	5	1	1	2017-04-09 23H	
User Activity: Configuration - New host scan configuration added	3	1	1	2017-04-09 23H	
AlienVault HIDS: Multiple web server 400 error codes from same source ip.	2	1	1	2017-04-09 18H	

Figura N° 64. Cambios de configuración del sistema realizado por los usuarios
Fuente: Resultados obtenidos por OSSIM

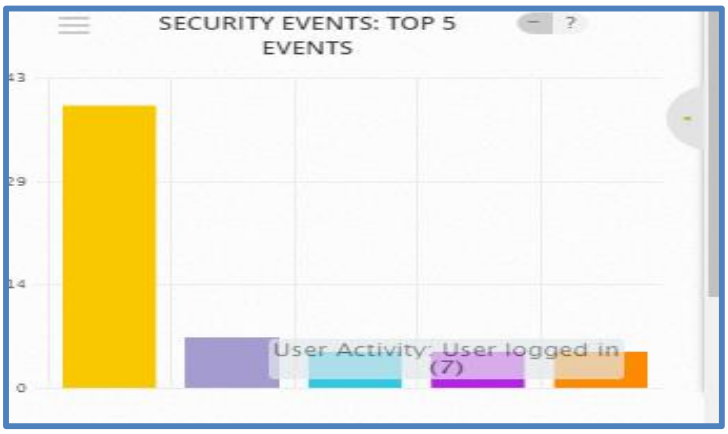


Figura N° 65. Dashboard de actividad de usuario
Fuente: Resultados obtenidos por OSSIM

<u>Proceso habilitador</u>: GESTIÓN DE OPERACIONES.

18. Número de incidentes causados por problemas operativos

Consideremos, por ejemplo, una mala configuración en un switch CISCO, específicamente, en la seguridad de puertos al agregar erróneamente una dirección MAC. Ante tal evento, el puerto se apagará.

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address


**Phase 1: Completed pre-decoding.
       full event: '%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address'
       hostname: 'alienvault'
       program_name: '(null)'
       log: '%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address'

**Phase 2: Completed decoding.
       decoder: 'cisco-ios'
       id: '%PORT_SECURITY-2-PSECURE_VIOLATION'

**Phase 3: Completed filtering (rules).
       Rule id: '4712'
       Level: '5'
       Description: 'Cisco IOS critical message.'
**Alert to be generated.
```

Figura N° 66. Regla de Puerto de switch DOWN
Fuente: Resultados obtenidos por OSSIM

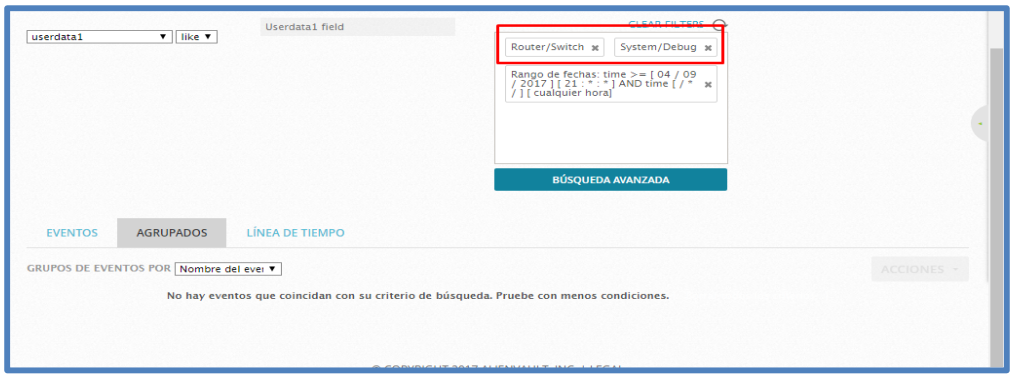


Figura N° 67. Número de eventos donde el puerto del switch es DOWN
Fuente: Resultados obtenidos por OSSIM

Como apreciamos en la imagen anterior, no ha ocurrido ninguna violación de política del switch, si en caso ocurriera se realizaría una acción. En este caso, OSSIM muestra ese evento en la interfaz web con el ID de evento 4712.

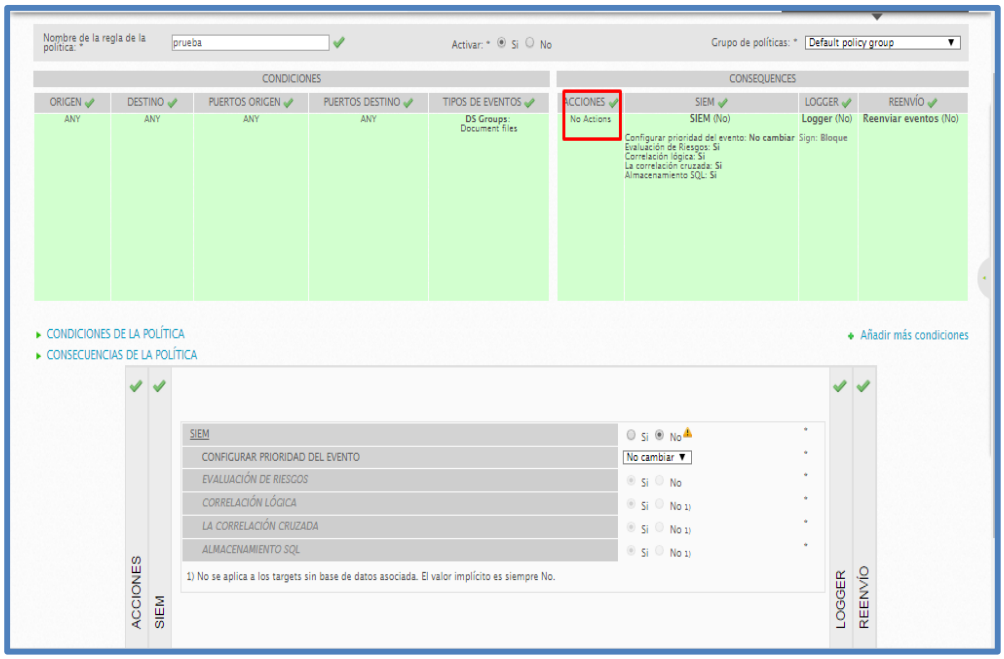
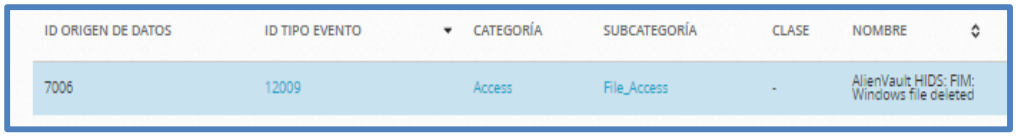


Figura N° 68. Políticas de Ossim
Fuente: Resultados obtenidos por OSSIM

Por otro lado, OSSIM puede mostrar información sobre archivos críticos eliminados.



ID ORIGEN DE DATOS	ID TIPO EVENTO	CATEGORÍA	SUBCATEGORÍA	CLASE	NOMBRE
7006	12009	Access	File_Access	-	AlienVault HIDS: FIM: Windows file deleted

Figura N° 69. ID de evento de archivos de Windows eliminados
Fuente: Resultados obtenidos por OSSIM

19. Tasa de eventos comparada con el número de incidentes

La ISO 27000 define a un incidente de seguridad de la información como un evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

OSSIM permite crear directivas de correlación las cuales permiten relacionar eventos. También puede realizar una correlación cruzada mediante el uso de direcciones IP de destinos. Así, cuando el sistema descubre una vulnerabilidad, relaciona esta información con los eventos (ataques directos) generados por los IDS e identifica si está a ocurrido en algún destino conocido mediante la dirección IP.

Un ejemplo de directiva sería los intentos de *logueo fallido*. Si bien es cierto el usuario puede ingresar su contraseña de acceso de forma incorrecta, el sistema puede detectar los intentos de autenticación por fuerza bruta (tras muchos intentos fallidos el equipo logra conectarse) generando una alarma.

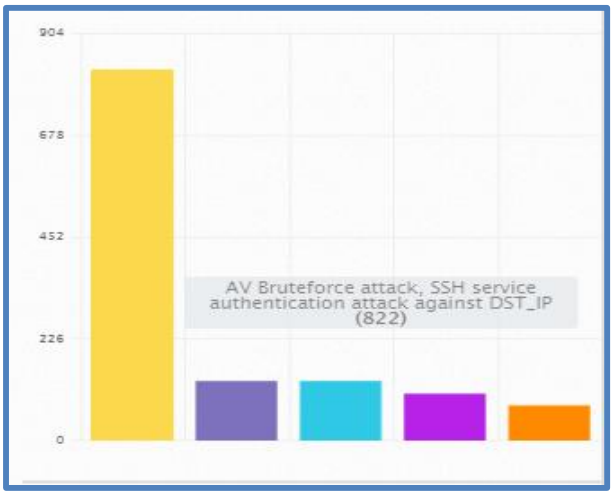


Figura N° 70. Ataques de fuerza bruta
Fuente: Resultados obtenidos por OSSIM

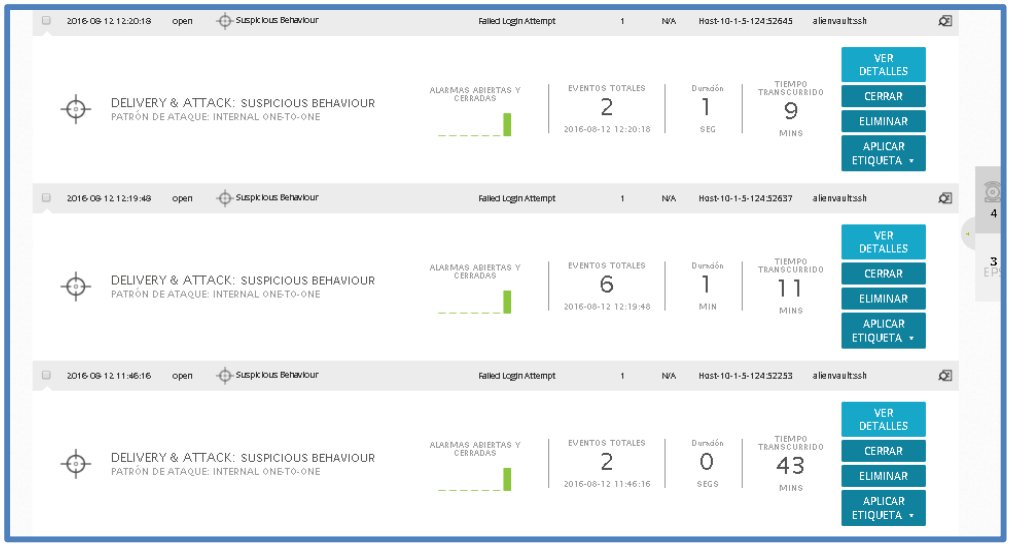


Figura N° 71. Alarmas de fuerza bruta
Fuente: Resultados obtenidos por OSSIM

En las imágenes anteriores podemos visualizar la autenticación de fuerza bruta, logrando generar 822 alarmas.

20. Porcentaje de tipos de eventos críticos cubiertos por sistema de detección automática

OSSIM es una plataforma que integra varias herramientas por lo que puede recopilar información importante sobre aplicaciones, disponibilidad y autenticación del sistema.

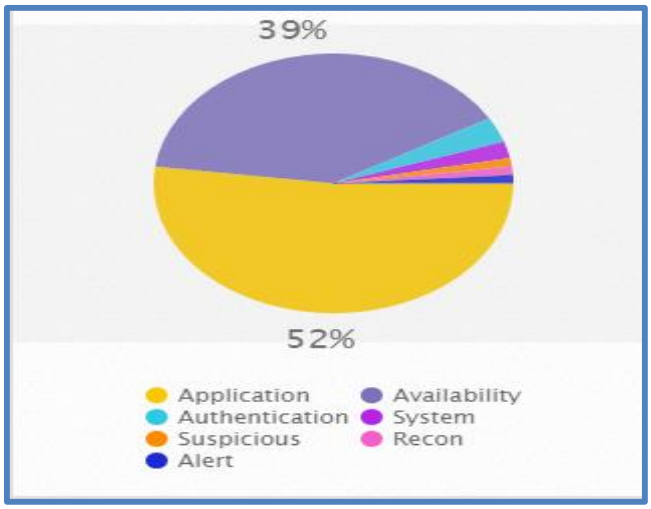


Figura N° 72. Eventos críticos en la red
Fuente: Resultados obtenidos por OSSIM

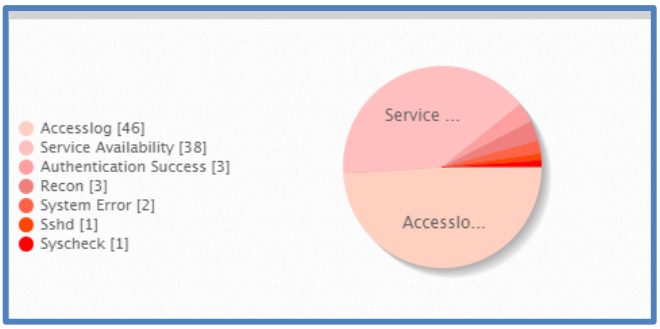


Figura N° 73. HIDS monitoreo
Fuente: Resultados obtenidos por OSSIM

4.4.2 Evaluación del nivel de madurez según COBIT PAM

Después de la implementación y recolección de datos, es posible medir el nivel de madurez alcanzado en los procesos habilitadores del caso de estudio. Esta evaluación permitirá determinar si el modelo de gestión de la seguridad de la información cumple con los objetivos propuestos en esta investigación, logrando así contrastar la hipótesis establecida.

La mecánica para identificar el nivel de madurez consiste en evaluar el cumplimiento de las actividades de gestión para cada uno de los procesos principales junto con sus habilitadores.
Esta evaluación está definida en el apéndice C de la presente investigación. El estado de cumplimiento es determinado por el administrador de red, basándose en las actividades diarias, controles establecidos y el entorno de red antes de implementar la plataforma de gestión.

La siguiente tabla muestra criterios de evaluación de la norma ISO/IEC 15504 y los criterios para identificar la escala de cumplimiento para cada nivel de madurez.

Tabla N° 29: Leyenda para especificar el nivel de madurez de un proceso habilitador

Leyenda	Descripción
N: "Not achieved"	No existe evidencia de la entrega o gestión del proceso habilitador. El cumplimiento de las actividades está entre cero (0) y quince (15) por ciento.
P: "Partially achieved"	Existe evidencia de la entrega de las actividades definidas para el proceso. Algunos aspectos deben ser predecibles. El cumplimiento de las sub-actividades de gestión está entre quince (15) y cincuenta (50) por ciento.
L: "Largely achieved"	Existe evidencia sistemática y significativa sobre la entrega y cumplimiento de actividades dentro del proceso. El cumplimiento está entre cincuenta (50) y ochenta y cinco (85) por ciento
F: "Fully achieved"	Existe evidencia total y sistemática sobre el cumplimiento de las actividades de gestión definidas en el proceso. El cumplimiento está entre ochenta y cinco (85) y cien (100) por ciento.

Fuente: Autores - Process Assessment Model (PAM): Using COBIT 5

4.4.3 Evaluación del nivel de madurez de los procesos habilitadores

De acuerdo al estado actual de los procesos y su cumplimiento en el caso de estudio, se procede a completar la tabla con el estado de cumplimiento para cada actividad y sus sub-actividades.

a) Proceso habilitador: **Gestión de la Disponibilidad y Capacidad**

Tabla N° 30: Evaluación de cumplimiento para proceso habilitador BAI04: Gestión de la Disponibilidad y Capacidad

BAI04	Sub-actividades	Estado de cumplimiento
Evaluar la disponibilidad, rendimiento y capacidad actual	Considerar en la evaluación de disponibilidad y capacidad de servicios y recursos lo siguiente: Requisitos del cliente, objetivos de negocio, impacto en el presupuesto, utilización de recursos, capacidades de TI y tendencias de la industria.	NO CUMPLE
	Supervisar el rendimiento y la utilización de la capacidad reales frente a los umbrales definidos.	CUMPLE
	Identificar y dar seguimiento a todos los incidentes causados por un rendimiento o una capacidad inadecuados.	CUMPLE
	Evaluar periódicamente los niveles reales de rendimiento a todos los niveles de procesamiento mediante la comparación de las tendencias y los acuerdos de nivel de servicios,	CUMPLE

	teniendo en cuenta los cambios en el entorno.	
Evaluar el impacto en el negocio	Identificar los servicios críticos para los procesos de gestión de la disponibilidad y la capacidad	CUMPLE
	Realizar un mapa de soluciones o servicios seleccionados con las aplicaciones e infraestructura de los que dependen para permitir un enfoque en los recursos críticos para la planificación de la disponibilidad.	NO CUMPLE
	Recolectar datos de patrones de disponibilidad de los registros de fallos pasados y de la monitorización del rendimiento.	CUMPLE
	Crear escenarios basados en datos recolectados, describiendo situaciones de disponibilidad futura.	CUMPLE
	Determinar la probabilidad de que el objetivo del rendimiento de la disponibilidad no será alcanzado basado en los escenarios.	CUMPLE
	Determinar el impacto de los escenarios en las medidas de rendimiento del negocio. Involucrar a la línea de negocio, líderes funcionales y regionales para comprender su evaluación del impacto.	NO CUMPLE
	Asegurar que los propietarios de procesos de negocio comprenden completamente y están de acuerdo con los resultados del análisis.	CUMPLE
Planificar requisitos de servicios nuevos o modificados	Revisar las implicaciones en la disponibilidad y la capacidad del análisis de tendencias del servicio.	CUMPLE
	Identificar las implicaciones en la disponibilidad y la capacidad de cambios en las necesidades del negocio y las oportunidades de mejora.	NO CUMPLE
	Priorizar las necesidades de mejora y crear planes de disponibilidad y capacidad justificadas en costos.	NO CUMPLE
	Ajustar los planes de rendimiento y capacidad y los acuerdos de nivel de servicio sobre la base de los procesos de negocio y servicios que los soportan realistas, nuevos, propuestos o proyectados, sobre cambios a las aplicaciones y la infraestructura.	NO CUMPLE
	Asegurar que la dirección lleva a cabo comparaciones de la demanda actual de recursos con la demanda y suministro previstos para evaluar las técnicas de previsión actuales y realizar mejoras donde sea posible.	NO CUMPLE
Supervisar y revisar la disponibilidad y la	Establecer un proceso de recolección de datos para proporcionar a la dirección información de seguimiento e informes de la carga de trabajo de disponibilidad, rendimiento	CUMPLE

	y capacidad de todos los recursos relacionados con la información.	
	Proporcionar información periódica de los resultados en una forma apropiada para su revisión por las TI y la gestión del negocio y comunicar a la dirección empresarial.	CUMPLE
	Integrar las actividades de supervisión e información en las actividades iterativas de gestión de la capacidad.	CUMPLE
	Proveer informes de capacidad para los procesos de presupuesto.	CUMPLE
Investigar y abordar cuestiones de disponibilidad	Obtener la orientación de manuales de productos de proveedores para garantizar a un nivel adecuado de rendimiento de disponibilidad para picos de procesamiento y cargas de trabajo	NO CUMPLE
	Identificar brechas de rendimiento y capacidad sobre la base de la monitorización del rendimiento actual y previsto	CUMPLE
	Definir acciones correctivas requeridas dentro de los procesos apropiados de planificación y gestión de cambios.	CUMPLE
	Definir un procedimiento de escalado para la resolución rápida en emergencias en caso de problemas de capacidad y rendimiento.	CUMPLE

Fuente: Autores

- Nivel de Madurez alcanzado: **Ejecutado (1) - L**

  Según la norma ISO/IEC 15504, para el proceso habilitador: Gestión de la capacidad y disponibilidad (BAI04), se determina que, en gran parte, las sub-actividades se cumplen cabalmente, lo que hace de este proceso un proceso ejecutado de nivel 1. Por otro lado, la letra "L" especifica que las actividades de dicho proceso están entre 50 a 80% cumplidas lo que nos da la garantía necesaria de concluir acertadamente, de que el proceso está siendo cubierto íntegramente por el modelo de gestión propuesto.

b) Proceso **habilitador**: **Gestión de activos**

Tabla N° 31: Evaluación de cumplimiento para proceso habilitador BAI09: Gestión de activos

BAI09	Sub-actividades	Estado de cumplimiento
Identificar y registrar los activos actuales	Identificar todos los activos en propiedad en un registro que incluya el estado actual.	CUMPLE
	Identificar los requisitos legales, reglamentarios o contractuales que deben ser abordados en la gestión de los activos.	NO CUMPLE
	Verificar la existencia de todos los activos en propiedad mediante la realización periódica de controles de inventario lógicos.	CUMPLE
	Comprobar que los activos se adecuen a sus objetivos	CUMPLE
	Determinar de forma regular si cada activo continúa proporcionando valor y, si es así, estimar la vida útil prevista de dicha validez.	CUMPLE
	Asegurar la contabilización de todos los activos	CUMPLE
Gestionar activos críticos	Identificar los activos que son críticos en la provisión de la capacidad del servicio refiriéndose a los requisitos en las definiciones de servicio.	CUMPLE
	Supervisar el rendimiento de los activos críticos examinando las tendencias de incidentes.	CUMPLE
	De forma regular, considerar el riesgo de fallo o necesidad del reemplazo de cada activo físico.	CUMPLE
	Mantener la resiliencia de los activos críticos mediante la aplicación de un mantenimiento preventivo regular, de supervisión de rendimiento.	CUMPLE
	Establecer un plan de mantenimiento preventivo para todo el hardware, considerando un análisis costo beneficio.	NO CUMPLE
	Establecer contratos de mantenimiento que impliquen el acceso de terceros a las instalaciones de TI de la organización para actividades in situ y fuera del sitio.	NO CUMPLE
	Comunicar a los usuarios afectados el impacto esperado de las actividades de mantenimiento.	NO CUMPLE
	Asegurar que los servicios de acceso remoto y perfiles de usuarios están activos solo cuando sea necesario.	CUMPLE
	Incorporar el tiempo de inactividad previsto en general en el calendario de producción, y programar las actividades de mantenimiento para minimizar el impacto adverso en los procesos de negocio.	CUMPLE

Gestionar el ciclo de vida de los activos	Adquirir todos los activos basándose en solicitudes aprobadas y de acuerdo con las políticas y las prácticas de adquisición de la empresa.	NO CUMPLE
	Identificar el origen, recibir, verificar, probar y registrar todos los activos de una manera controlada, incluyendo el etiquetado físico, si fuera necesario.	NO CUMPLE
	Aprobar los pagos y completar el proceso de proveedores según las condiciones acordadas por contrato.	NO CUMPLE
	Desplegar los activos siguiendo el ciclo de vida de implementación estándar, incluyendo la gestión de cambios y pruebas de aceptación.	NO CUMPLE
	Asignar activos a usuarios, con aceptación y firma de responsabilidades, según corresponda.	NO CUMPLE
	Reasignar los activos siempre que sea posible cuando ya no sea necesario debido a un cambio de función de rol de usuario.	NO CUMPLE
	Eliminar los activos cuando no sirvan a un propósito útil debido a la finalización de todos los servicios relacionados, tecnología obsoleta o falta de usuarios.	NO CUMPLE
	Eliminar los activos de forma segura, teniendo en cuenta, por ejemplo, la eliminación permanente de los datos registrados en dispositivos y posibles daños al medio ambiente.	NO CUMPLE
	Planificar, autorizar y realizar las actividades relacionadas con la finalización de uso, manteniendo los registros apropiados para satisfacer las necesidades regulatorias cambiantes del negocio.	NO CUMPLE
Optimizar el costo de los activos	Revisar la base general de activos de forma regular, teniendo en cuenta si está alineada con los requerimientos del negocio.	NO CUMPLE
	Evaluar los costos de mantenimiento, considerar si son razonables e identificar opciones de menor costo, incluyendo, cuando sea necesaria, el remplazo con nuevas alternativa.	NO CUMPLE
	Revisar las garantías y considerar la relación calidad-precio y estrategias de reemplazo para determinar opciones de menor costo.	NO CUMPLE
	Revisar la base general para identificar oportunidades de normalización, abastecimiento único y de estrategias que pueden disminuir los costos de adquisición, soporte y mantenimiento.	NO CUMPLE
	Usar estadísticas de capacidad y utilización para identificar activos infrautilizados o redundantes que pudieran ser considerados para su eliminación o sustitución por otro con	NO CUMPLE

	menores costos.	
	Revisar el estado general para identificar las oportunidades para aprovechar tecnologías emergentes o estrategias de aprovisionamiento alternativas para reducir los costos o incrementar el valor del dinero.	NO CUMPLE
Administrar licencias	Mantener un registro de todas las licencias de software adquiridas y sus acuerdos de licencia asociados.	CUMPLE
	De forma regular, llevar a cabo una auditoria para identificar a todas las copias de software con licencia	CUMPLE
	Comparar el número de copias de software instalado con el número de licencias en propiedad.	CUMPLE
	Cuando las copias sean inferiores al número en propiedad, decidir si existe una necesidad de mantener o cancelar licencias, considerando el potencial de ahorrar en manteamiento innecesario, formación y otros gastos.	NO CUMPLE
	Cuando las copias sean superiores al número en propiedad, considerar primero la posibilidad de desinstalar copias que no sean ya necesarias o no estén justificadas.	NO CUMPLE
	De forma regular, considerar si se puede obtener un mejor valor mediante la actualización de productos y licencias asociadas.	CUMPLE

Fuente: Autores

- Nivel de Madurez alcanzado: **Ejecutado (1) - P**

  Según la norma ISO/IEC 15504, para el proceso habilitador: Gestión de activos (BAI09), se determina que las sub-actividades se cumplen parcialmente, haciéndolo de igual manera, un proceso ejecutado de nivel 1. Por otro lado, la letra "P" especifica que las actividades de dicho proceso están entre 15 a 50% cumplidas lo que nos da la garantía necesaria de concluir acertadamente, de que el proceso está siendo cubierto por el modelo de gestión propuesto.

c) Proceso habilitador: **Gestión de la configuración**

Tabla N° 32: Evaluación de cumplimiento para proceso habilitador BAI10: Gestión de la configuración

BAI10	Sub-actividades	Estado de cumplimiento
stablecer un modelo de configuración	Definir y acordar el alcance y nivel de detalle para la gestión de la configuración.	CUMPLE
	Establecer y mantener un modelo lógico para la gestión de la configuración, incluyendo información sobre los tipos de elementos de configuración.	CUMPLE

Controlar los elementos de configuración	Identificar y clasificar los elementos de configuración y rellenar el repositorio.	CUMPLE
	Crear, revisar y formalizar un acuerdo sobre las bases de referencia de configuración de un servicio, aplicación o infraestructura.	CUMPLE
Mantener y controlar los elementos de configuración	Identificar regularmente todos los cambios en los elementos de configuración.	CUMPLE
	Revisar los cambios propuestos a los elementos de configuración respecto a la base de referencia para garantizar su integridad y precisión.	CUMPLE
	Actualizar los detalles de configuración con los cambios aprobados a los elementos de configuración.	CUMPLE
	Crear, revisar y formalizar acuerdos sobre los cambios en las líneas de referencia de configuración cuando sea necesario.	NO CUMPLE
Generar informes de estado y configuración	Identificar cambios en el estado de los elementos de configuración y contrastarlo con la base de referencia.	CUMPLE
	Enlazar todos los cambios de configuración con las peticiones de cambio aprobadas para identificar cualquier cambio no autorizado	CUMPLE
	Identificar requisitos de información de todas las partes interesadas, incluyendo contenido, frecuencia y medios. Generar informes según las necesidades.	NO CUMPLE
Verificar la integridad del repositorio	Verificar periódicamente los elementos de configuración en activo contra el repositorio de configuración comparando configuraciones físicas y lógicas usando las herramientas apropiadas de descubrimiento, según sea necesario.	CUMPLE
	Informar y revisar todas las desviaciones de las correcciones o acciones aprobadas para eliminar los activos no autorizados.	CUMPLE
	Establecer y revisar periódicamente el objetivo de completitud del repositorio de configuración basado en las necesidades del negocio.	CUMPLE
	Periódicamente comparar el grado de completitud y precisión respecto a los objetivos y tomar medidas correctivas.	CUMPLE

Fuente: Autores

- Nivel de Madurez alcanzado: **Ejecutado (1) - F**

  Según la norma ISO/IEC 15504, para el proceso habilitador: Gestión de la configuración (BAI10), se determina que, en su gran totalidad, las sub-actividades se cumplen cabalmente, lo que hace de este proceso un proceso ejecutado de nivel 1. Por otro lado, la letra "F" especifica que las actividades de dicho proceso están entre 85 a 100% cumplidas lo que nos da la garantía necesaria de concluir acertadamente, de que el proceso está siendo cubierto íntegramente por el modelo de gestión propuesto.

d) Proceso habilitador: **Gestión de operaciones**

Tabla N° 33: Evaluación de cumplimiento para proceso habilitador DSS01: Gestión de operaciones

DSS01	Sub-actividades	Estado de cumplimiento
Ejecutar procedimientos operativos	Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados.	NO CUMPLE
	Mantener una programación de actividades operativas, ejecutar las actividades y gestionar el desempeño y rendimiento de las actividades programadas.	NO CUMPLE
	Asegurar que se cumple con los estándares de seguridad aplicables para la recepción, procesamiento, almacenamiento y salida de datos de forma tal que se satisfagan los objetivos empresariales, la política de seguridad de la empresa y los requerimientos regulatorios.	CUMPLE
	Verificar que todos los datos esperados para su procesamiento sean recibidos y procesados por completo y de una forma precisa y oportuna.	CUMPLE
	Programar, realizar y registrar las copias de respaldo de acuerdo con las políticas y procedimientos establecidos.	CUMPLE
Gestionar Servicios externalizados	Asegurar que los procesos de información se adhieren a los requerimientos de seguridad de la empresa y conformes con los contratos.	CUMPLE
	Asegurar que los requerimientos operativos del negocio y de procesamiento de TI se adhieren y son conformes	CUMPLE
	Integrar los procesos críticos de gestión interna de TI con los de los proveedores de servicios externalizados.	NO CUMPLE
	Planificar la realización de auditorías y aseguramientos independiente de los entornos operativos de los proveedores de externalización para confirmar que los requerimientos acordados están recibiendo el tratamiento adecuado	NO CUMPLE

Supervisar la infraestructura de TI	Registrar eventos, identificando el nivel de información a ser grabada sobre la base de una consideración y el rendimiento.	CUMPLE
	Identificar y mantener una lista de activos de infraestructura que necesiten ser monitorizados en base a la criticidad del servicio y la relación entre los elementos de configuración y los servicios que de ellos dependen.	CUMPLE
	Definir e implantar reglas que identifiquen y registren violaciones de umbral y condiciones de eventos	CUMPLE
	Producir registros de eventos y retenerlos por un periodo apropiado para asistir en investigación futuras.	CUMPLE
	Establecer procedimientos para supervisar los registros de eventos y llevar a cabo revisiones periódicas.	CUMPLE
	Asegurar que se crean oportunamente los tiques de incidente cuando la monitorización identifica desviaciones de los umbrales definidos.	CUMPLE
Gestionar el entorno	Identificar desastres naturales y causados por el ser humano que puedan ocurrir en el área donde se encuentran las instalaciones de TI.	CUMPLE
	Identificar de qué manera el equipamiento de TI, incluyendo el equipamiento móvil y el ubicado fuera de las instalaciones, está protegido contra las amenazas del entorno.	CUMPLE
	Ubicar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad ante las amenazas del entorno.	NO CUMPLE
	Supervisar y mantener de forma periódica a los dispositivos que detectan proactivamente las amenazas del entorno.	CUMPLE
	Responder a las alarmas y otras notificaciones del entorno.	CUMPLE
	Comparar medidas y planes de contingencia respecto a los requerimientos de las pólizas de seguros e informar de los resultados.	NO CUMPLE
	Asegurar que los sitios de TI están construidos y diseñados para minimizar el impacto del riesgo del entorno.	NO CUMPLE
Gestionar las instalaciones	Examinar los requerimientos de las instalaciones de TI respecto de la protección frente a la fluctuación y cortes de la energía eléctrica.	NO CUMPLE
	Probar periódicamente los mecanismos del sistema de alimentación ininterrumpida.	CUMPLE
	Asegurar que las instalaciones que alojan los sistemas de TI tienen más de un proveedor para los servicios públicos indispensables.	NO CUMPLE
	Confirmar que el cableado externo al sitio de TI está bajo tierra	NO CUMPLE

	o que tiene una protección alternativa adecuada.	
	Asegurar que el cableado y el patching físico están estructurados y organizados.	NO CUMPLE
	Analizar las instalaciones que alojan los sistemas de alta disponibilidad para verificar el cumplimiento de los requerimientos de cableado en cuanto a redundancia y tolerancia a fallos.	NO CUMPLE
	Asegurar que los sitios e instalaciones de TI cumplen de manera sistemática con la legislación, regulaciones, directrices y especificaciones de salud y seguridad en el trabajo.	NO CUMPLE
	Proporcionar periódicamente formación al personal en la legislación, regulaciones y directrices relevantes de salud y seguridad en el trabajo.	NO CUMPLE
	Registrar, supervisar, gestionar y resolver incidentes en las instalaciones siguiendo los procesos de gestión de incidentes de TI.	NO CUMPLE
	Asegurar que los sitios y el equipamiento de TI son mantenidos de acuerdo con los intervalos de servicio y las especificaciones recomendadas del proveedor.	NO CUMPLE
	Analizar las alteraciones físicas a los sitios o localizaciones de TI para reevaluar el riesgo del entorno.	NO CUMPLE

Fuente: Autores

- Nivel de Madurez alcanzado: **Ejecutado (1) - P**

  Según la norma ISO/IEC 15504, para el proceso habilitador: Gestión de operaciones (DSS01), se determina que, en su mayoría, las sub-actividades se cumplen, lo que hace de este proceso un proceso ejecutado de nivel 1. Por otro lado, la letra “P” especifica que las actividades de dicho proceso están entre 15 a 50% cumplidas lo que nos da la garantía necesaria de concluir acertadamente, de que el proceso está siendo cubierto íntegramente por el modelo de gestión propuesto.

e) Proceso habilitador: **Gestión de incidencias de servicio**

Tabla N° 34: Evaluación de cumplimiento para proceso habilitador DSS02: Gestión de incidencias de servicio

DSS02	Sub-actividades	Estado de cumplimiento
Definir esquemas de clasificación de incidentes	Definir esquemas de clasificación y priorización de incidentes para el registro de problemas.	CUMPLE
	Definir modelos de incidentes para errores conocidos con el fin de facilitar su resolución eficiente y efectiva.	CUMPLE
	Definir los modelos de peticiones de servicio según el tipo de petición de servicio correspondiente para facilitar la auto-ayuda y el servicio eficiente para las peticiones estándar.	CUMPLE
	Definir reglas y procedimientos de escalado de incidencias, especialmente para incidentes importantes e incidentes de seguridad.	CUMPLE
	Definir fuentes de conocimientos de incidentes y peticiones y su uso.	CUMPLE
Registrar, clasificar y priorizar incidencias	Registrar todos los incidentes, registrando toda la información relevante de forma que pueda ser manejada de manera efectiva y se mantenga un registro histórico.	CUMPLE
	Para posibilitar análisis de tendencias, clasificar incidentes y peticiones de servicio identificando tipo y categoría.	CUMPLE
	Priorizar peticiones de servicio según definición de impacto en el negocio.	CUMPLE
Verificar, aprobar y resolver peticiones de servicios	Verificar los derechos para realizar peticiones de servicio usuario, cuando sea posible, un flujo de proceso predefinido y cambios estándar.	NO CUMPLE
	Obtener aprobación financiera y funcional o firmada, si se requiere, o aprobaciones predefinidas para cambios estándar acordados.	NO CUMPLE
	Completar las peticiones siguiendo el procedimiento de petición seleccionado, utilizando, cuando sea posible, menús automáticos de autoayuda y modelos de petición predefinidos para los elementos solicitados frecuentemente.	NO CUMPLE
Investigar, diagnosticar y localizar indecentes	Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes.	NO CUMPLE
	Registrar un nuevo problema si un problema relacionado o error conocido no existe aún y si el incidente satisface los criterios acordados para registro de problemas.	CUMPLE
	Asignar incidentes a funciones especialistas si se necesita de un conocimiento más profundo, e implicar al nivel de gestión	CUMPLE

	apropiado, cuando sea necesario.	
Resolver y recuperarse ante incidentes	Seleccionar y aplicar las resoluciones de incidentes más apropiadas	CUMPLE
	Registrar si se usaron soluciones temporales para resolver los incidentes	NO CUMPLE
	Ejecutar acciones de recuperación, si se requieren.	CUMPLE
	Documentar la resolución de incidentes y evaluar si se puede usar como fuente de conocimiento futuro.	CUMPLE
Cerrar incidentes	Verificar con los usuarios afectados que la petición de servicio ha sido completada o el incidente ha sido resuelto de manera satisfactoria.	CUMPLE
	Cerrar peticiones de servicio e incidentes.	CUMPLE
Seguir el estado y emitir informes	Supervisar y hacer seguimiento del escalado de incidentes y de resoluciones y de los procedimientos de gestión de resoluciones para progresar hacia la resolución o cumplimiento.	CUMPLE
	Identificar la información para las partes interesadas y sus necesidades de datos o informes. Identificar la frecuencia y el medio para informarles.	CUMPLE
	Analizar incidentes y peticiones de servicio por categoría y tipo para establecer tendencias e identificar patrones de asuntos recurrentes.	CUMPLE
	Producir y distribuir informes en tiempo o proporcionar acceso controlado a datos online	NO CUMPLE

Fuente: Autores

- Nivel de Madurez alcanzado: Ejecutado (1) – L

  Según la norma ISO/IEC 15504, para el proceso habilitador: Gestión de incidencias de servicio (DSS02), se determina que las sub-actividades se cumplen en su gran mayoría, haciéndolo un proceso ejecutado de nivel 1. Por otro lado, la letra “L” especifica que las actividades de dicho proceso están entre 50 a 85% cumplidas lo que nos da la garantía necesaria de concluir que el proceso está siendo cubierto por el modelo de gestión propuesto.

f) Proceso habilitador: **Gestión de servicios de seguridad**

Tabla N° 35: Evaluación de cumplimiento para proceso habilitador DSS05: Gestión de servicios de seguridad

DSS05	Sub-actividades	Estado de cumplimiento
Proteger contra software malicioso	Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.	NO CUMPLE
	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera	CUMPLE
	Distribuir todo el software de protección de forma centralizada usando una configuración centralizada y la gestión de cambios.	CUMPLE
	Revisar y evaluar regularmente la información de sobre nuevas posibles amenazas.	CUMPLE
	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada.	CUMPLE
	Realizar formación sobre software malicioso en el uso del correo electrónico e internet.	NO CUMPLE
Gestionar la seguridad de la red y las conexiones	Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer una política de seguridad para las conexiones.	CUMPLE
	Permitir solo dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzarla solicitud de contraseña.	CUMPLE
	Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.	CUMPLE
	Cifrar la información en tránsito de acuerdo con su clasificación.	NO CUMPLE
	Aplicar los protocolos de seguridad aprobados a las conexiones de red.	CUMPLE
	Configurar los equipamientos de red de forma segura.	CUMPLE
	Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.	CUMPLE
	Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.	CUMPLE
	Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.	CUMPLE
dad de los puesto	Configurar los sistemas operativos de forma segura.	CUMPLE
	Implementar mecanismo de bloqueo de los dispositivos.	CUMPLE

	Cifrar la información almacenada de acuerdo a su clasificación.	NO CUMPLE
	Gestionar el acceso y control remoto.	CUMPLE
	Gestionar la configuración de la red de forma segura.	CUMPLE
	Implementar el filtrado de tráfico de la red en dispositivos de usuario final.	CUMPLE
	Proteger la integridad del sistema.	CUMPLE
	Proveer de protección física a los dispositivos de usuario final.	NO CUMPLE
	Deshacerse de los dispositivos de usuario final de forma segura.	NO CUMPLE
Gestionar la identidad del usuario y el acceso lógico	Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio.	NO CUMPLE
	Identificar unívocamente todas las actividades de proceso de la información por roles funcionales.	CUMPLE
	Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad.	CUMPLE
	Administrar todos los cambios de derechos de acceso.	CUMPLE
	Segregar y gestionar cuentas de usuario privilegiadas.	CUMPLE
	Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.	CUMPLE
	Asegurar que todos los usuarios y su actividad en sistemas de TI son identificados unívocamente	CUMPLE
	Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.	CUMPLE
Gestionar el acceso físico a los activos de TI	Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardando el registro de petición.	NO CUMPLE
	Asegurar que los perfiles de acceso estén actualizados.	NO CUMPLE
	Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI.	NO CUMPLE
	Instruir a todo el personal para mantener visible la identificación en todo momento.	NO CUMPLE
	Escoltar a los visitantes en todo momento mientras estén en la ubicación.	NO CUMPLE
	Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores.	NO CUMPLE
	Realizar regularmente formación de concienciación de seguridad física.	NO CUMPLE

Gestionar los documentos sensibles y dispositivos de salida	Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro y fuera de la empresa.	NO CUMPLE
	Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo requerimientos del negocio.	NO CUMPLE
	Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.	NO CUMPLE
	Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.	NO CUMPLE
	Destruir la información sensible y proteger dispositivos de salida.	NO CUMPLE
Supervisar la infraestructura para detectar eventos relacionados con la seguridad	Registrar los eventos relacionados con la seguridad, reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo.	CUMPLE
	Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocidas y sus impactos comprendidos para permitir una respuesta conmensurada.	CUMPLE
	Revisar regularmente los registros de eventos para detectar incidentes potenciales.	CUMPLE
	Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.	CUMPLE
	Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.	CUMPLE

Fuente: Autores

- Nivel de Madurez alcanzado: Ejecutado (1) – P

  Según la norma ISO/IEC 15504, para el proceso habilitador: Gestión de servicios de seguridad (DSS05), se determina que las sub-actividades se cumplen parcialmente, haciéndolo de igual manera, un proceso ejecutado de nivel 1. Por otro lado, la letra “P” especifica que las actividades de dicho proceso están entre 15 a 50% cumplidas lo que nos da la garantía necesaria de que el proceso está siendo cubierto por el modelo de gestión propuesto.

4.4.4 Discusión de resultados

Tal como vemos en la tabla siguiente, los 6 procesos habilitadores seleccionados se cumplen mediante el modelo de gestión propuesto. Esto quiere decir, que la relación entre la plataforma de gestión de seguridad OSSIM y el marco referencial COBIT 5 cumplen con el objetivo principal de brindar información necesaria y oportuna para la toma de decisiones.

Tabla N° 36: Resumen de evaluación de procesos

PROCESO	NIVEL DE MADUREZ ALCANZADO
BAI04	EJECUTADO (1) → L
BAI09	EJECUTADO (1) → P
BAI10	EJECUTADO (1) → F
DSS01	EJECUTADO (1) → P
DSS02	EJECUTADO (1) → L
DSS05	EJECUTADO (1) → P

Fuente: Autores

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- La definición del diseño de red basado en el dimensionamiento del caso de estudio permite determinar la criticidad de ciertos activos y analizar la mejor ubicación de los módulos de recolección de información que puedan gestionar adecuadamente la seguridad.

- OSSIM es una plataforma de gestión de gran utilidad pues contiene plugins compatibles con dispositivos de diferentes marcas, permitiéndole al administrador recopilar información útil y oportuna en una única consola centralizada.

- OSSIM gestiona la autenticación del usuario y el acceso lógico a la información siguiendo los lineamientos del proceso: Gestión de Servicios de Seguridad de COBIT 5 mediante la integración con Active Directory (LDAP) haciendo que el sistema sea más seguro contra ataques de denegación de usuarios.

- OSSIM proporciona información útil, relevante y oportuna ya que tiene un motor de correlación (lógica y cruzada) que genera eventos de mayor prioridad y fiabilidad reduciendo los falsos positivos y los falsos negativos de tal manera que el administrador tome las decisiones correctas respecto a los eventos detectados en la red.

- OSSIM es una herramienta SIEM open Source muy valiosa que no solo tiene implementados algunos controles de la ISO 27001, PCI DSS sino que también permite la integración con el marco de referencia COBIT 5 proporcionando un sistema de gestión de seguridad de la información alineado a los objetivos de seguridad propuestos por el caso de estudio.

- Una de las funciones esenciales de seguridad cubierta por OSSIM es el descubrimiento de activos mediante el cual proporciona información detallada de los activos en red, sus sistemas operativos, estados de los equipos, equipos agregados en red; es decir que cumple parcialmente las actividades del proceso de Gestión de activos (BAI09).

- OSSIM verifica la integridad del repositorio proporcionando información de las desviaciones entre repositorio de configuración y la configuración real; es decir cumple con las sub-actividades del proceso de Gestión de configuración.

- Nagios es una de las herramientas integradas en OSSIM la cual proporciona información de incidentes de disponibilidad identificando servicios críticos de tal manera que cubre parcialmente las actividades del proceso de Gestión de la disponibilidad y Capacidad.

- El análisis de los objetivos del caso de estudio permite identificar y contrastar estos con los procesos habilitadores que COBIT presenta en su guía logrando una adecuada integración que favorezca la gestión de la seguridad teniendo como base un marco de referencia aceptado internacionalmente.

- La relación entre la plataforma OSSIM y el marco de referencia COBIT 5 cubre parcialmente y/o totalmente los procesos que favorecen al logro del objetivo principal que es la toma de decisiones basado en información útil y oportuna.

- De acuerdo a la norma ISO/IEC 15504 los niveles de madurez para cada proceso evaluado mediante la integración de OSSIM – COBIT están ejecutados a nivel 1 como mínimo, lo que permite validar acertadamente el modelo propuesto.

- Finalmente, el uso de una plataforma de Gestión de Seguridad Open Source bajo un entorno de objetivos de control según el enfoque de COBIT tiene un impacto positivo y eficaz en la toma de decisiones de TI en la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

- OSSIM cuenta con un módulo de reportería el cual proporciona información útil y oportuna para la toma de decisiones. Pero para proporcionar dicha información, se requiere de varias horas de configuración de acuerdo al entorno de la organización.

RECOMENDACIONES

- Ya que OSSIM es una herramienta SIEM open Source muy poderosa capaz de abarcar 5 funciones de seguridad como: descubrimiento de activos, evaluación de vulnerabilidades, detección de intrusiones, monitoreo de comportamiento y SIEM, es recomendable implementar la plataforma a nivel de todo el diseño de red del campus, siendo este un proceso continuo que apunte siempre al cumplimiento de los objetivos de gestión de seguridad en la universidad

- A fin de obtener un rendimiento óptimo de la plataforma, se recomienda cumplir con los requerimientos mínimos a nivel de hardware, es decir que el servidor tenga 16 GB de RAM como mínimo y un disco duro de 1 TERABYTE para almacenar la información de eventos detectados por sus diversas herramientas en la red.

- La plataforma de gestión tiene una base de datos de eventos clasificados por producto y categorías, por lo que inicialmente recibiremos abundantes de eventos del mismo servidor; por eso se recomienda que se priorice los eventos que se deben almacenar para evitar saturaciones en el disco duro y memoria RAM.

- OSSIM tiene configuradas políticas de seguridad por defecto, pero es de suma importancia que el administrador cree y configure sus propias políticas en base a su diseño de red, por eso se recomienda que toda política o regla sea implementada por el personal que tenga conocimiento en gestión de la seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

A3Sec. (4 de Febrero de 2014). Alienvault USM Sistemas de detección de ataques en tiempo real.

Alamanni, M. (2014). OSSIM a Careful, Free and Always Available Guardian for Your Network. *Linux Journal*.

AlienVault. (2011). Take your open source security strategy to the next level (The power of Open Source from a single, unified console).

AlienVault. (2013). HOW ALIENVAULT COMPONENTS COMMUNICATE TCP/IP Connections Between OSSIM/USM Components.

AlienVault. (s.f.). Documento técnico AlienVault: Gestión de Seguridad Unificado vs SIEM.

Alramahi, N. M., Barakat, A. I., & Haddad, H. (2014). Information Technology Governance Control Level in Jordanian Banks Using: Control Objectives for Information and Related Technology (COBIT 5). *European Journal of Business and Management*.

Asociacion Colombiana de Facultades de ingeniería. (2008). Implementación y mejora de la consola de seguridad informática OSSIM: Una experiencia de colaboración Universidad- Empresa. *Educación en Ingeniería*, 9.

Balarezo, A., & Poveda, D. (2015). *Propuesta de mejoramiento de la herramienta OSSIM SIEM (Open Source), para obtener los niveles óptimos de gestión en la administración de la seguridad, en una red implementada en Cloud Computing.* Quito: Universidad Politécnica Saleciana.

Baluja García, W., Caro Reina, C. C., & Cancio Bello, F. A. (2012). OSSIM, una alternativa para la integración de la gestión de seguridad en la red. *Revista Telemática Vol N° 11 enero - abril*, pp. 11-19.

Bjarte Fjellskål, E., & Wysocki, K. (s.f.). *http://manpages.ubuntu.com*. Obtenido de http://manpages.ubuntu.com/manpages/wily/man1/prads.1.html

Bravo Bravo, Á. H., & Villafuerte Quiroz, Á. L. (2015). Implantación De Una Herramienta Ossim Para El Monitoreo Y Gestión De La Seguridad De La Red Y Plataformas Windows Y Linux Aplicado A Empresas Medianas.

Burgos, Jose & Campos, Pedro. (2013). *Modelo para seguridad de la información en TIC.* Chile: Departamento de tecnologias y sistemas de información.

Carrillo Verdún, J., & Rubio Casallas, A. P. (2012). Modelo de Procesos Integrado de Gobernanza y Gestión de TI. *AEMES TI Revista de Procesos y Métricas*.

Cerullo, G., Formicola, V., Iamiglio, P., & Sgaglione, L. (2014). Critical Infrastructure Protection: having SIEM technology cope with network heterogeneity.

Chanaluisa Viera, D. A., Meza Castillo, A. L., & Tasipanta Chicaiza, J. V. (2012). Implementación del sistema de gestión y administración de seguridad para la dirección de tecnologías de la Universidad Central del Ecuador (DTIC). Quito, Ecuador.

Chanaluisa, Darwin & Meza, Andres & Tasipanta, Jessica. (2012). *Implementación del sistema de gestion y administracion de seguridad para la direccion de tecnologías de la universidad central del Ecuador.* Ecuador: Universidad Central del Ecuador.

Chikonga, M. (2014). Exploring the Applicability of SIEM Technology in IT Security.

DragonJAR. (s.f.). *https://www.dragonjar.org/*. Obtenido de https://www.dragonjar.org/p0f-identificacion-pasiva-del-sistema-operativo.xhtml

Eset Latinoamérica. (2015). *ESET Security Report Latinoamérica 2015*.

Espinoza, H. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC/27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.* Perú: Pontificia Universidad Católica del Perú.

Ferrer, J., & Fernández, J. (2012). Seguridad Informática y Software Libre. *Hispanolinux*.

Giménez García, M. I. (2008). Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral.

Gualsaqui, J. (2013). Desarrollo del marco de referencia COBIT 5 para la gestión del área de ti de la empresa Blue Card. Quito, Ecuador - Pontificia Universidad Católica del Ecuador.

INFOSEC INSTITUTE. (2012). *http://resources.infosecinstitute.com/*. Obtenido de http://resources.infosecinstitute.com/alienvault-ossim-review-open-source-siem/

ISACA. (2010). Security Information and Event Management:Business Benefits and Security,Governance and Assurance Perspectives.

ISACA. (2012). *COBIT 5 - Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. ISACA - Information Systems Audit and Control Association. ISACA.

ISACA. (2012). *COBIT 5: Procesos Catalizadores.* EEUU: isaca.org.

Izquierdo, J. A., & Almazán, J. M. (2006). OSSIM/SOC: el «binomio» de la seguridad corporativa. *Revista Dintel*.

Kadam, A. (2012). The Evolution of COBIT. *CSI Communications*, 21 -22.

Karg, D. (2006). OSSIM-Agents Inside a Distributed Enterprise.

Karg, D., Muñoz, J., Gil, D., González, S., & Casal, J. (2003). OSSIM Open Source Security Information Management Descripción General del Sistema.

Kavanagh, K. M., & Rochford, O. (2015). *Magic Quadrant for Security Information and.*

Kershaw, M. (2016). *https://www.kismetwireless.net*. Obtenido de https://www.kismetwireless.net/documentation.shtml

Klaessig, K. (14 de Diciembre de 2014). La Evolución de SIEM.

Kotenko, I., & Chechulin, A. (2012). Attack Modeling and Security Evaluation in SIEM Systems. *International Transactions on Systems Science and Applications*, pp. 129-147.

Kotenko, I., Polubelova, O., Chechulin, A., & Saenko, I. (2013). Design and Implementation of a Hybrid Ontological-Relational Data Repository for SIEM Systems. *Future Internet Volume 5, Issue 3*, pp. 355-375.

Lepage Hoces, D. E. (2014). Diseño de un modelo de gobierno de ti con enfoques de seguridad de información para empresas prestadoras de servicios de salud bajo la óptica de COBIT 5. Lima, Perú.

Lorenzo, J. M. (2010). Herramientas Integradas OCSA (OSSIM Certified Security Analyst).

Madrid Molina, J. M., Múnera Salazar, L. E., Montoya González, C. A., Osorio Betancur, J. D., Cárdenas, L. E., Bedoya, R., & Latorre, C. (Diciembre de 2008). Implementación y mejora de la consola de seguridad informática OSSIM: una experiencia de colaboración Universidad-Empresa. *Eduación en la Ingeniería N° 6*, 29-37.

Martínez Estébanes, E., & García Cano, J. C. (2011). Gobierno de TI a través de COBIT 4.1 y cambios esperados en COBIT 5.0. *ECORFAN*, pp.109-131.

Mataracioglu, T., & Ozkan, S. (2011). Governing information security in conjunction with COBIT and ISO 27001. Ankara, Turquía: Middle East Technical University, Informatics Institute.

Mera Balseca, A. S. (2014). Diseño del modelo de gestión de seguridad de la información dek sistema ERP de EP PETROECUADOR de acuerdo a norma ISO/IEC 27002 y COBIT 5. Ecuador.

Montesino Perurena, R., Baluja García, W., & Porvén Rubier, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. *RIELAC, Vol.XXXIV*, pp. 40-58.

Montesino, R., Baluja, W., & Porvén, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. *RIELAC*, 40-58.

Nazareno Torrecillas, J. (2013). ¿Es la seguridad de la información un freno o un facilitador de la expansión del negocio? *Publicación N° 18 de la Revista Seguridad Cultura de Prevención para TI*, pp. 4-8.

Nuñez Martínez, A. (2008). Propuesta de una plataforma de Gestión de Seguridad en la intranet de la UCVL "Marta Abreu". *Telemática*.

Osorio Betancur, J. D., Cárdenas, L. E., Bedoya, R., Latorre, C., & Madrid Molina, J. M. (2008). Integración de un panel de alarma de incendio y un sistema de cámaras de vigilancia IP con la consola de seguridad informática OSSIM. *Sistemas & Telemática*, 61-74.

Parra Truyol, A. (2013). Laboratorio de malware: Automatización de la gestión de recursos virtuales para el estudio de malware. Madrid, España.

Puchades Olmos, A. (Diciembre de 2008). Análisis de la plataforma Ossim Sistema de gestión de la información Open Source. Valencia.

Robles, R., & Rodríguez de Roa, Á. (2006). La gestión de la seguridad de la información en la empresa: ISO 27001. *publicacion del mes de junio de Revista Calidad*, pp. 12-18.

Sanchez, Luis & Piattini, Mario. (2015). *Hacia un metodo para la construccion de cuadros de mando de la seguridad en TI para PYMES.* España: Departamento de tecnologias y sistemas de información.

Shelton, M. (2005). *http://manpages.ubuntu.com/*. Obtenido de http://manpages.ubuntu.com/manpages/wily/man8/pads.8.html

Shivhare, P., & Savaridassan, P. (2015). Addressing Security Issues of Small and Medium Enterprises through Enhanced SIEM Technology. *International Journal of Scientific Research (IJSR) Volume 4 Issue 4*, 1241-1243.

Tandazo Jimenez, K., & Rueda Salgado, M. Á. (2013). *Prevención, detección y reducción de riesgos de ataques por escaneo de puertos usando tecnologías de virtualización* . Sangolquí.

Tapia Jardinez, R., & Sánchez Ruiz, D. S. (Noviembre de 2009). Propuesta de un sistema de monitoreo para La red de Esime Zacatenco utilizando el protocolo SNMP y software libre. México.

Torres, M., & Villegas, D. (2010). *Integracion OSSIM UTANGLE.* Colombia: Universidad ICESI.

Vianello, V., Gulisano, V., Jimenez Peris, R., Patino Martinez, M., Torres, R., Diaz, R., & Prieto, E. (2013). A Scalable SIEM Correlation Engine and its Application to the Olympic Games IT Infrastructure. *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, 625 - 629.

Villena, M. (2006). *Sistema de gestión de seguridad de información para una institución financiera*. Perú: Pontifica Universidad Catolica del Perú.

Yagual Del Valle, C., & Chilán Rodríguez, L. (Diciembre de 2014). Análisis para la integración de un Sistema de Gestión de Seguridad de Información (SGSI) ISO-27001 Utilizando OSSIM para empresa Industrial. Guayaquil, Ecuador.

APÉNDICE A. DATA CENTER – UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

A.1. Gabinete de Servidores

N°	DESCRIPCIÓN		CAPACIDAD			SOFTWARE	
	Marca	Modelo	Microprocesador	RAM	Disco Duro	Sistema Operativo	Aplicaciones en producción
01	HP	Proliant DL380G6	Intel Xeon X5560 2.8 GHz (2)	12 GB	146GB, SAS, Dual Port, 15k (4); 72GB, Serial SCSI, 1 port, 15k (4)	Windows Server 2008 EE	Virtualización Hyper-V (Aplicaciones Web, **Servidor VPN**), Backup de Admisión, Web. EPG UNPRG
02	HP	Proliant DL585	AMD Opteron 64 Dual-Core 885 2.6 GHz (2)	4 GB	72,8GB, Ultra 320 SCSI, 10k (4)	Windows Server 2008 EE	**ISA Server 2006 - Acceso Internet**, Admin remota (Web, SSH)
03	HP	Proliant DL360 G3	Intel Xeon 2.80 GHz (2)	1 GB	72,8GB, Ultra 320 SCSI, 10k; 36,4GB, Ultra 320 SCSI, 15k	Windows 2000 Server	ISA Server 2000 - Acceso Internet
04	HP	Proliant DL360 G3	Intel Xeon 2.80 GHz (1)	2 GB	36,4GB, Ultra 320 SCSI, 15k (2)	Windows 2000 Advanced Server	Controlador de Dominio 1, DNS
05	HP	Proliant DL380	Intel Xeon 2.80 GHz (2)	1 GB	36,4GB, Ultra 320 SCSI, 15k (2)	Windows 2000 Server	Controlador de Dominio 2, DNS, DHCP
06	HP	Proliant DL380	Intel Xeon 2.80 GHz (2)	1.5 GB	36,4GB, Ultra 320 SCSI, 15k (4)	Windows 2000 Advanced Server	Base de Datos Sistema Académico Gestac
07	HP	Proliant DL580	Intel Xeon 2.50 GHz (1)	2 GB	72,8GB, Ultra 320 SCSI, 15k (4)	GNU/Linux Centos 5.3	Elearning Aula Virtual
08	HP	Proliant DL380G6	Intel Xeon Quad Core X5560 2.8 GHz (2)	12 GB	146GB, SAS, Dual Port, 15k (4)	GNU/Linux Centos 5.6	Virtualización KVM (Aplicaciones Web , Elearning EPG, postgres sql , apache ,mysql)
09	HP	Proliant DL380G5	Intel Xeon Quad Core 2.0 GHz	6 GB	72GB, Serial SCSI, 1 port, 15k (4)	GNU/Linux Centos 5.4	Servidor de Telefonía IP - System Callmanager
10	HP	Proliant DL380G5	Intel Xeon Quad Core 2.0 GHz	4 GB	72GB, Serial SCSI, 1 port, 15k (4)	Oracle Enterprise Linux 5.6	Servidor de Base de Datos Oracle (Sistemas informáticos Produccion)
11	HP	Proliant DL380G5	Intel Xeon Quad Core 2.0 GHz	4 GB	72GB, Serial SCSI, 1 port, 15k (4)	GNU/Linux Centos 5.5	Servidor de Gestión, comunicaciones y monitoreo de la red TCP/IP
12	HP	Proliant DL380G5	Intel Xeon Quad Core 2.0 GHz	4 GB	72GB, Serial SCSI, 1 port, 15k (4)	GNU/Linux Debian	Sistema de Biblioteca UNPRG, Base de Datos MySQL, PHP, Apache
13	HP	Proliant DL380G5	Intel Xeon Quad Core 2.0 GHz	4 GB	72GB, Serial SCSI, 1 port, 15k (4)	GNU/Linux Centos 5.6	Servidor de Base de Datos ORACLE y Aplicaciones (Pruebas)
14	HP	Proliant DL380G5	Intel Xeon Quad Core 2.0 GHz	8 GB	72GB, Serial SCSI, 1 port, 15k (4)	Oracle Enterprise Linux 5.6	Virtualización KVM (server Aplicaciones web 2, Acceso Remoto, server FTP)
15	HP	Proliant DL380G5	Intel Xeon Quad Core 2.0 GHz	4 GB	72GB, Serial SCSI, 1 port, 15k (4)	Windows Server 2003 EE	Servidor de Base de Datos Sistema SIGA, Sistema Control, Actualizaciones
16	HP	BladeSystem C3000	Intel Xeon Quad Core 2 GHz(1 Blade BL)	6GB	72GB, Serial SCSI, 1 port, 15k (2)	Windows Server 2008 EE	Servicios Active Directory Domain Services windows 2008 R2, aplicaciones de escritorio SIGA, Radius
17	HP	StorageWorks MSA20	-	1.5T	250GB, Serial SCSI, 1 port, 15k (6)	Administrable por Software	Sistema de Almacenamiento de Bases de Datos y archivos
18	HP	StorageWorks MSA20	-	1.5T	250GB, Serial SCSI, 1 port, 15k (6)	Administrable por Software	Sistema de Almacenamiento de Bases de Datos y archivos
19	HP	DC7600	Intel Dual Core 3.0 GHz	2GB	130GB, SATA, 10k	FreeBSD	Firewall de Seguridad Perimetral VYATTA linea 2
20	compatible	pemtium IV	Intel pemtium IV	500MB	80 GB	FreeBSD	Firewall de Seguridad Perimetral VYATTA linea speedy
21	HP	DC7600	Intel Pentium 4 3.0 GHz	512 MB	80 GB	Endian	Firewall Proxy Endian linea 2
22	HP	DC7600	Intel Pentium 4 3.0 GHz	512 MB	80 GB	Endian	Firewall Proxy Endian linea speedy
22	HP	DC7600	Intel Pentium 4 3.0 GHz	512 MB	80 GB	Endian	Firewall Proxy Endian SIAF-Mef(transmisión)
23	HP	DC7600	Intel Pentium 4 3.0 GHz	512 MB	80 GB	Endian	Firewall Proxy Endian Linea 2,3 en pruebas
24	HP	DC7600	Intel Pentium 4 3.0 GHz	512 MB	80GB	Windows Server 2003 R2	ADM Active Directory , Reporte Firewall
25	HP	DC7600	Intel Pentium 4 3.0 GHz	512 MB	80GB	Linux Centos 5.6	Sistema de Gestión SNMP, NTP
26	HP	DC5750	Intel 2 DUO Core 3.0 GHz	1GB	80GB	Windows Server 2003	Server Antivirus Consola de Actualización
27	HP	Laptop	Centrino Dual Core	1GB	80GB	Windows server 2008 /Centos 6.0	Documentancion y Labores de Oficina , PRUEBAS DE Software

A.2. Gabinete de comunicaciones

N°	Ubicación	Dispositivo	Fabricante	Modelo	Caracteristicas	Descripción
1	Data Center	Media Converter	Huawei	OptiX 155/622H (Metro1000)	Dispositivo de integracion o conversion de medios de transmision, 2 RU	Dispositivo de conversion de señal optica a señal electrica y otros medios
2	Data Center	UPM (uninterrupted power module)	Huawei	GIE4805S	Rectificador de 220VAC a -48VDC	Equipo de reserva de energía
3	Data Center	Router	Cisco	2821	2 puertos ethernet 10/100/1000, soporta tarjetas AIMs, NMs, WICs, VWICs, and VICs, switching de capa 2 con Power over Ethernet (PoE), On-board encryption, soporta llamadas de voz analogica y digital, Dedicated Extension Voice Module slot, voice mail support, soporta Cisco CallManager Express (Cisco CME) for local call processing in stand alone business for up to 48 IP Phones. QoS, 802.1p, 802.1q, CDP, Survivable Remote Site Telephony support, voice and advanced services to multiple T1/E1WAN rates.	Enrutamiento Front End Primario - Acceso a internet 10 MB
4	Data Center	Router	Cisco	2821	2 puertos ethernet 10/100/1000, soporta tarjetas AIMs, NMs, WICs, VWICs, and VICs, switching de capa 2 con Power over Ethernet (PoE), On-board encryption, soporta llamadas de voz analogica y digital, Dedicated Extension Voice Module slot, voice mail support, soporta Cisco CallManager Express (Cisco CME) for local call processing in stand alone business for up to 48 IP Phones. QoS, 802.1p, 802.1q, CDP, Survivable Remote Site Telephony support, voice and advanced services to multiple T1/E1WAN rates.	Enrutamiento Front End Primario - Acceso a internet 2MB
5	Data Center	Router	Cisco	1905	DIspositivo de enrutamiento Gigabit Ethernet, 1RU	Enrutamiento Front End Primario - Acceso a internet 2MB
6	Data Center	Modem Sobremesa	Teldat S.A.	Ebano NG V.35	modulación para tecnología xDSL simétrica	Modulador de Señal - Acceso a internet
7	Data Center	Router	Cisco	2801	2 puertos ethernet 10/100Mbps, soporta tarjetas AIMs, NMs, WICs, VWICs, and VICs, switching de capa 2 con Power over Ethernet (PoE), On-board encryption, soporta llamadas de voz analogica y digital, Dedicated Extension Voice Module slot, voice mail support, soporta Cisco CallManager Express (Cisco CME). QoS, 802.1p, 802.1q, CDP, Survivable Remote Site Telephony support, voice and advanced services to multiple T1/E1WAN rates, survivable Remote Site Telephony support for up to 24 IP phones.	Enrutamiento Front End Secundario - Acceso a internet 2MB
8	Data Center	Firewall	Cisco	PIX 515E	Security Appliance, supports up to six 10/100 Fast Ethernet interfaces, Market-Leading Voice-Over-IP and Multimedia Security, combina VPN y calidad de servicio (QoS) con los servicios de inspección de protocolos estándares de redes convergente, soporta 802.1q, policy-based QoS services, with support for LLQ and traffic policing for prioritizing latency-sensitive network traffic and limiting bandwidth.	Dispositivo de Seguridad
9	Data Center	Intrusion Detection Sensor	Cisco	IDS 4215	2 puertos 10Mbps Ethernet, 100Mbps Fast Ethernet, 80 Mbps performance, QoS, trafico 802.1q, adecuado para entornos E1/T1y T3, IPSec, ACL, Politicas de Firewall, ACL's	Dispositivo de Seguridad
10	Data Center	Switch	Cisco	Catalyst 4507R (WS-C4507R)	L2/3/4, QoS, 802.1q, VLANs de voz, PoE, HSRP, ACLs, portsecurity, 802.1p	Switch Core
11	Data Center	Switch	Cisco	Catalyst 2950 (WS-C2950G-24-EI)	L2, QoS, 802.1q, VLANs de voz, ACLs, portsecurity, 802.1p	Dispositivo de Acceso
12	Data Center	Switch	Cisco	Catalyst 2950 (WS-C2950G-24-EI)	L2, QoS, 802.1q, VLANs de voz, ACLs, portsecurity, 802.1p	Dispositivo de Acceso y enlaces en cascada
13	Data Center	Switch	Cisco	Catalyst 2950 (WS-C2950G-24-EI)	L2, QoS, 802.1q, VLANs de voz, ACLs, portsecurity, 802.1p	Dispositivo de Acceso
14	Data Center	Switch	Cisco	Catalyst 2960 (WS-C2960-S-24PS-L)	L2, QoS, 802.1q, VLANs de voz, ACLs, portsecurity, 802.1p	Dispositivo de Acceso
15	Data Center	Gateway GSM	Xibelis	x3	Gateway para comunicación Servidor de comunicaciones de voz - Red Celular GSM	Gateway GSM
16	Data Center	Gateway GSM	ITS Telecom	CGW-T GSM	Gateway para comunicación Servidor de comunicaciones de voz - Red Celular GSM	Gateway GSM
17	Data Center	Gateway GSM	ITS Telecom	CGW-T GSM	Gateway para comunicación Servidor de comunicaciones de voz - Red Celular GSM	Gateway GSM
18	Data Center	Gateway GSM	ITS Telecom	CGW-T GSM	Gateway para comunicación Servidor de comunicaciones de voz - Red Celular GSM	Gateway GSM
19	Data Center	Gateway GSM	ITS Telecom	CGW-T GSM	Gateway para comunicación Servidor de comunicaciones de voz - Red Celular GSM	Gateway GSM
20	Data Center	Access Point	Cisco	Aironet 1100	802.11a/b/g, QoS, 802.1q, VLANs de voz, ACLs, 802.1p	Acceso Inalambrico Indoor
21	Data Center	Pannel Radio-Antena	NetKrom	CPE500G	1puerto 10/100Base-TX (RJ-45), 5, 10 ó 20MHz de ancho de banda seleccionable, 54Mbps de tasa de transferencia de datos, Access Control List, WEP 64/128, WPA1/WPA2 con TKIP & AES ciphers, Vlan (802.1Q) Support, Estadísticas sobre la Radio y el tráfico Ethernet, Power over Ethernet – PoE 802.3af.	Acceso Inalambrico Outdoor a Biotecnología
22	Data Center	Pannel Radio-Antena Externa	Motorola	PTP58600 Lite Conectorizado	Banda de RF 5.725 GHz–5.850 GHz, Modulación Dinámica; se adapta entre BPSK simple y 256 QAM dual; Rendimiento de datos del usuario: Dinámicamente variable hasta 150 Mbps con Ethernet (en total)	Acceso Inalambrico Outdoor a Centro Preuniversitario
23	Data Center	Pannel Radio-Antena integrada	Radwin	2000c	Equipo radio para enlace PTP Motorola 5.8 GHz; Radio única para bandas múltiples (2,4 y 4,9-5,9 GHz); MIMO (entrada múltiple, salida múltiple) avanzado, OFDM (múltiplex por división de frecuencia ortogonal) y tecnologías de diversidad ; MIMO (entrada múltiple, salida múltiple) avanzado, OFDM (múltiplex por división de frecuencia ortogonal) y tecnologías de diversidad	Acceso Inalambrico Outdoor a Centro Preuniversitario - Backup
24	Data Center	Pannel Radio-Antena integrada	Motorola	PTP58600 Lite Integrado	Banda de RF 5.725 GHz–5.850 GHz, Modulación Dinámica; se adapta entre BPSK simple y 256 QAM dual; Rendimiento de datos del usuario: Dinámicamente variable hasta 150 Mbps con Ethernet (en total)	Acceso Inalambrico Outdoor a Contabilidad - Tesorería Gnral
25	Data Center	Pannel Radio-Antena integrada	Motorola	PTP58600 Lite Integrado	Banda de RF 5.725 GHz–5.850 GHz, Modulación Dinámica; se adapta entre BPSK simple y 256 QAM dual; Rendimiento de datos del usuario: Dinámicamente variable hasta 150 Mbps con Ethernet (en total)	Acceso Inalambrico Outdoor a Local Central (Administración)
26	Data Center	Injector PoE	NetKrom	PoE-48i	100/240V - 48V / 0.35A	Dispositivo Power Injector, para Equipo de radio enlace PTP Netkrom CPE500G
27	Data Center	Injector PoE	Motorola	WB2521(P/N); ACPSSW200-03A (Product Code)	PIDU Plus PTP 300/500/600 Series; Input: 100/240VAC, 47-63Hz, 1.8 A ó - 48V DC, 1.4A; Output ODU - 48-SSV, 1A / DC Out - 48-SSV, 1.4 A	Dispositivo Power Injector, para Equipo de radio enlace PTP Motorola PTP58600 Lite
28	Data Center	Injector PoE	Motorola	WB2521(P/N); ACPSSW200-03A (Product Code)	PIDU Plus PTP 300/500/600 Series; Input: 100/240VAC, 47-63Hz, 1.8 A ó - 48V DC, 1.4A; Output ODU - 48-SSV, 1A / DC Out - 48-SSV, 1.4 A	Dispositivo Power Injector, para Equipo de radio enlace PTP Motorola PTP58600 Lite
29	Data Center	Injector PoE	Motorola	WB2521(P/N); ACPSSW200-03A (Product Code)	PIDU Plus PTP 300/500/600 Series; Input: 100/240VAC, 47-63Hz, 1.8 A ó - 48V DC, 1.4A; Output ODU - 48-SSV, 1A / DC Out - 48-SSV, 1.4 A	Dispositivo Power Injector, para Equipo de radio enlace PTP Motorola PTP58600 Lite
30	Data Center	Injector PoE; AC Power Adaptor	N/I (No Identificado)	ET0061040 - 00334B5555 Black	High Power 10/100 Base-T; 100-240 / 50-60 Hz 1.5A	Dispositivo Power Injector, para Equipo de radio enlace PTP Radwin 2000c
31	Data Center	Protector contra sobretensiones PoE	L-comm Hyperlink Technologies	HGLN-CAT5-HP	Indoor High Power 10/100 Base-T Shielded CAT5 Lightning Surge Protector; Protects 10/100 Base-T Ethernet networks; Power-over-Ethernet (PoE) compatible; Supports reverse polarity PoE pinouts; Compatible with Cisco Aironet® 1100/1200 AP and DC Injectors	Dispositivo Surge Protector, para Equipo de radio enlace PTP Radwin 2000c
32	Data Center	UPS	SALICRU	SLC CUBE3 20 KVA	20 KVA, Baterias KOLFF	Sistema de Alimentación Ininterrumpida
33	Data Center	UPS	Ablerex	HS6000	6 KVA	Sistema de Alimentación Ininterrumpida
34	Data Center	UPS	Power Com PCM	VGD-10k	10 KVA, Banco de baterías Elise	Sistema de Alimentación Ininterrumpida

APÉNDICE B. MANUAL DE INSTALACION Y CONFIGURACION DE OSSIM 5.3

B.1. Instalación

Descargamos el ISO de la página de Alienvault.

En el menú de instalación nos aparecen dos opciones, en nuestro caso seleccionaremos el servidor Ossim.

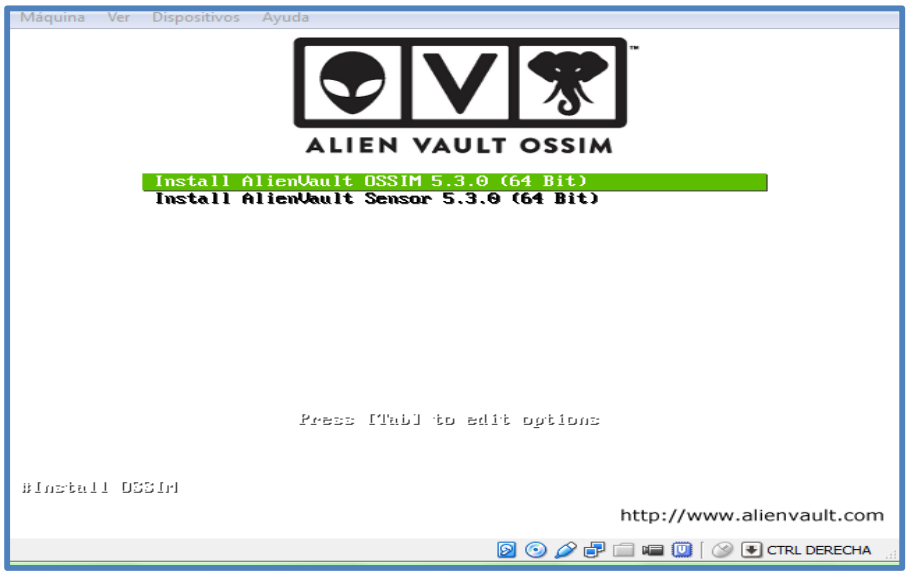


Figura B. 1 Instalación del server Ossim

Seleccionamos el lenguaje, país y el tipo de teclado

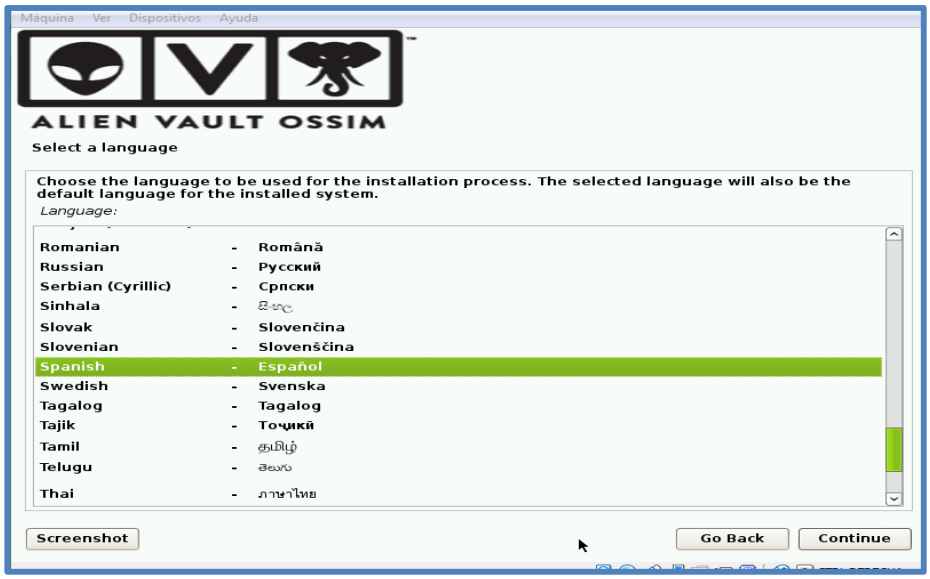


Figura B. 2 Selección del idioma para el proceso de instalación

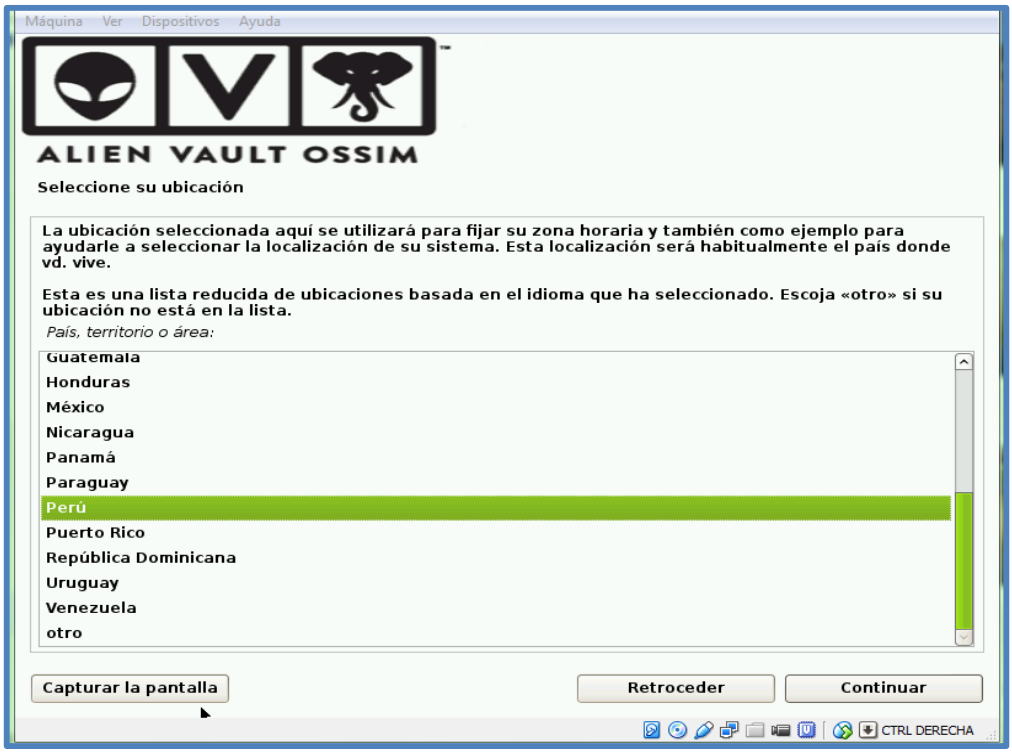


Figura B. 3 Selección de ubicación

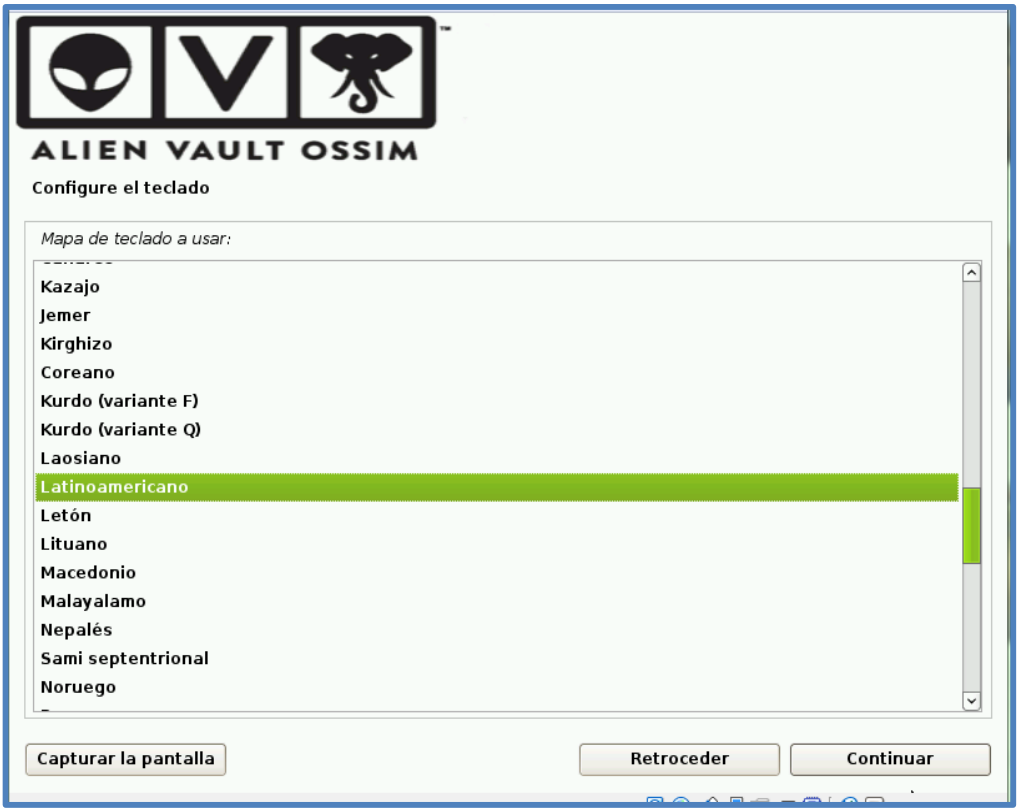


Figura B. 4 Idioma del teclado

Luego comenzara a cargar los componentes de instalación

Figura B. 5 Instalación de componentes

Durante la instalación pueden ocurrir algunos inconvenientes como es que no reconoce el firmware de la tarjeta de red, esto surge debido que son firmware no libres. Para solucionar esto descargamos el paquete non-free de la versión del sistema operativo (en cual está ejecutando el Ossim).

Figura B. 6 Configuración de red

Así como configuramos la IP del servidor también configuraremos su máscara de red, puerta de enlace y DNS.

Luego nos pedirá configurar la contraseña para el usuario "root"

Figura B. 7 Configuración de contraseña de superusuario

Luego continuará con la instalación

Figura B. 8 Finalización de instalación

B.2. Wizard

Luego de haber finalizado la instalación de Ossim, accedemos a la interfaz web con la IP asignada anteriormente al servidor (https://**X.Y.Z.W**) y creamos la cuenta de administrador.

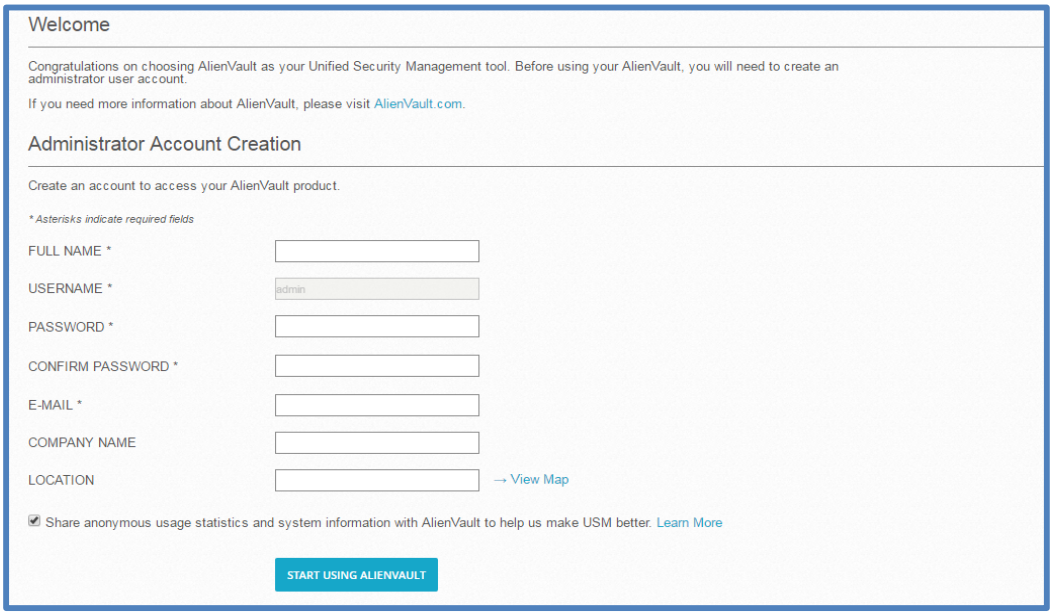


Figura B. 9 Creación de cuenta administrador

Una vez configurados los parámetros iniciales, tendremos acceso al inicio de sesión donde ingresaremos con el ID: admin y el Password: *******

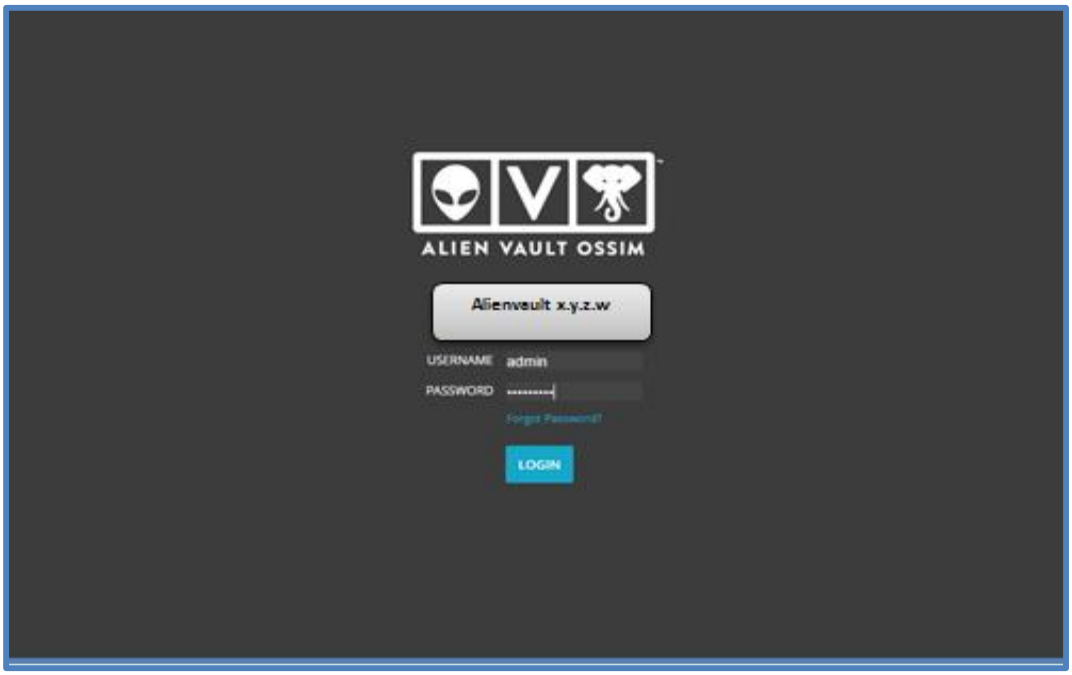


Figura B. 10 Acceso al framework

Alienvault proporciona un Asistente de introducción para ayudar a usuarios nuevos a configurar las capacidades de seguridad incorporadas por lo que iniciamos el wizard antes de ir al framework Alienvault Ossim.

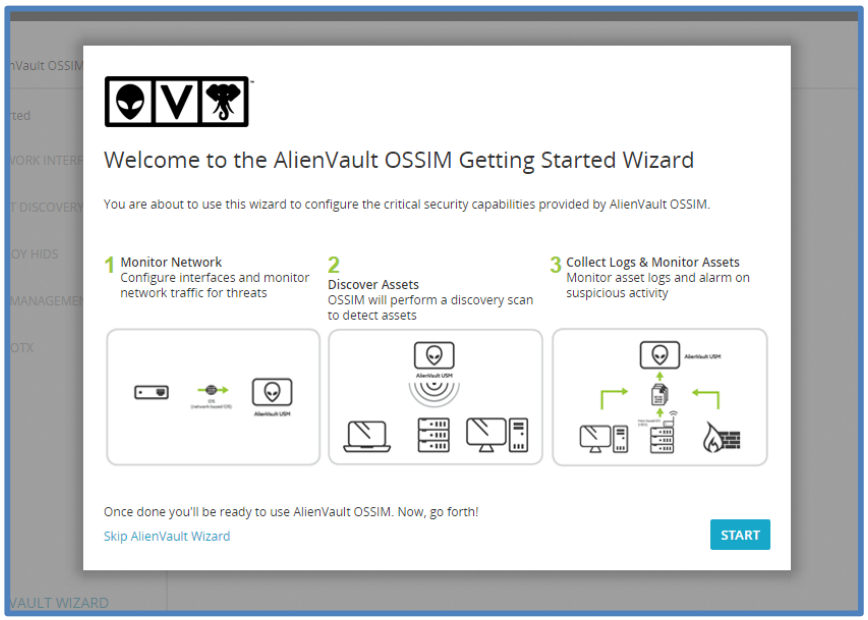


Figura B. 11 Iniciando el Wizard

Configuraremos 5 pasos antes de ir a la interfaz de Ossim

- Interfaces de red

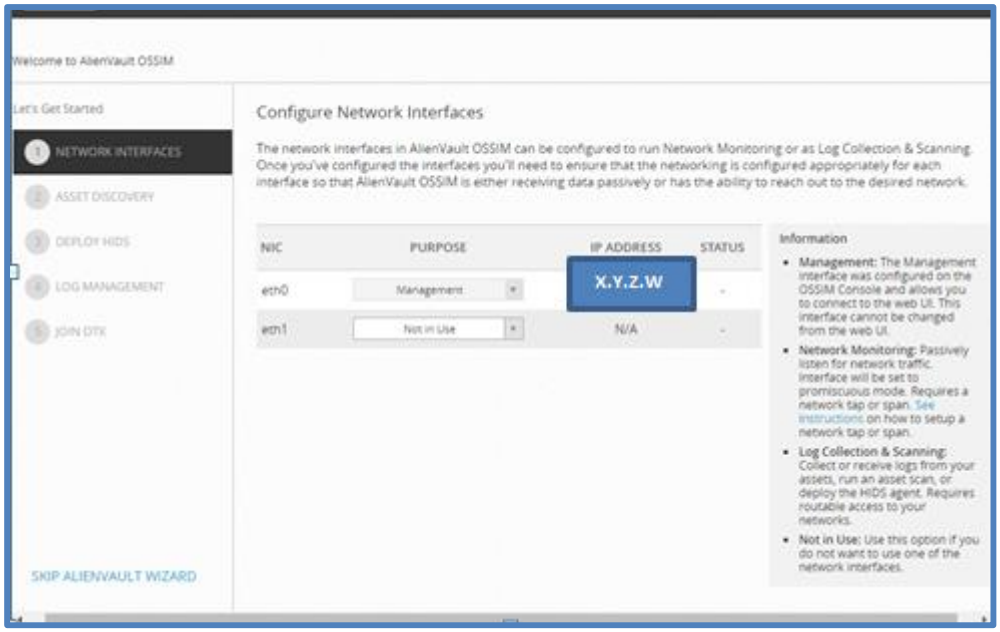


Figura B. 12 Configuración de interfaces de red

- Descubrimiento de activos

La comprensión de lo que está en su entorno es un paso crítico hacia la identificación de amenazas y vulnerabilidades. Por ello primero realizamos un escaneo de la red para identificar los equipos conectados y seleccionar posteriormente quienes actuarán como agentes que enviarán información de auditoria al servidor.

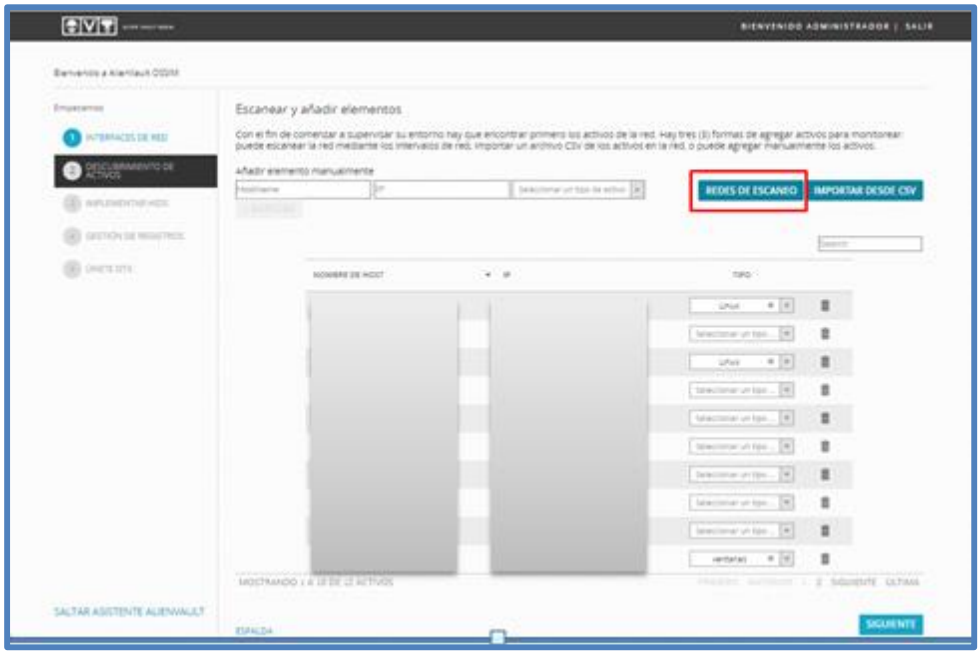


Figura B. 13 Descubrimiento de activos

- Desplegar HIDS

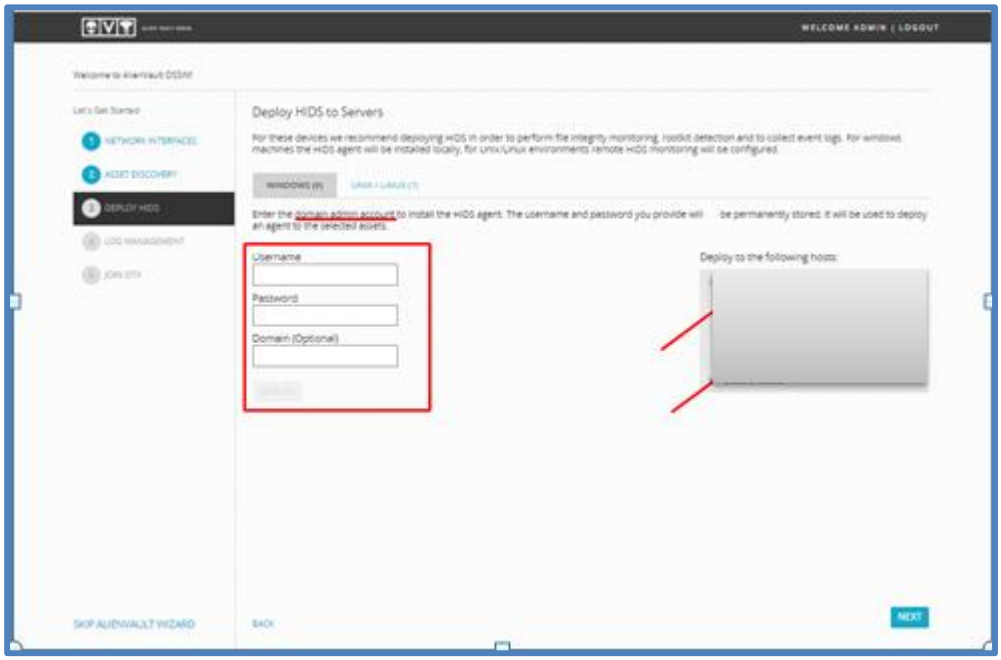


Figura B. 14 Desplegar HIDS para servidores

- Gestión de logs

Otra de las capacidades clave proporcionadas por Ossim es la capacidad de recoger datos de sus servidores, dispositivos de red y dispositivos de seguridad. Los datos recogidos permiten a Ossim correlacionar eventos para ver los patrones de actividad y emisión de alarmas

A continuación podemos agregar plugins para dispositivos de red según proveedor, modelo y versión para que envíen los logs de eventos hacia el servidor principal.

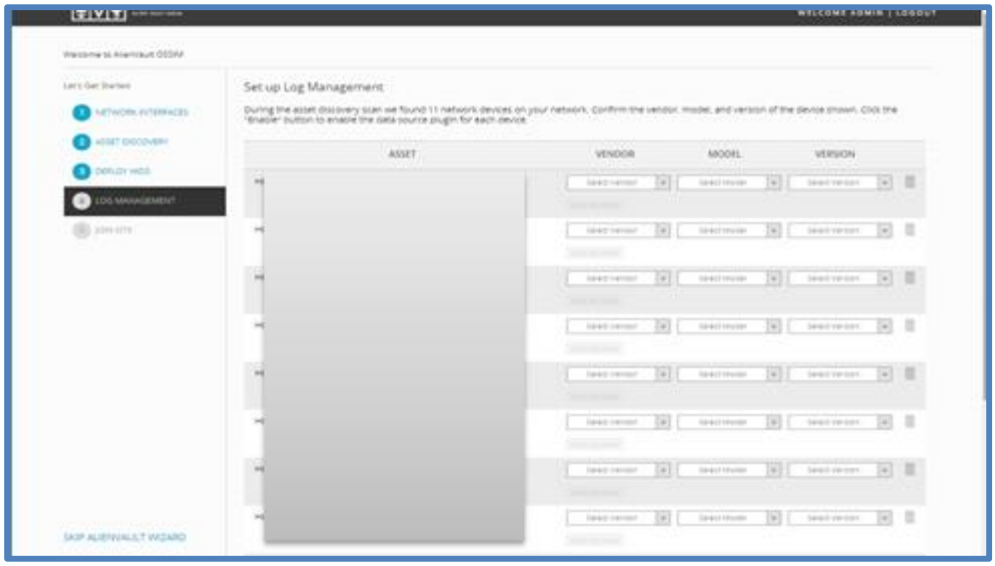


Figura B. 15 Plugins disponibles para dispositivos de red

- OTX

La herramienta OTX permite el intercambio de amenazas entre toda la comunidad Alienvault y sirve para mantenerse informado sobre todas las amenazas actuales y sus posibles orígenes y soluciones. Para nuestro caso, se obviara este paso, y se configurará más adelante.

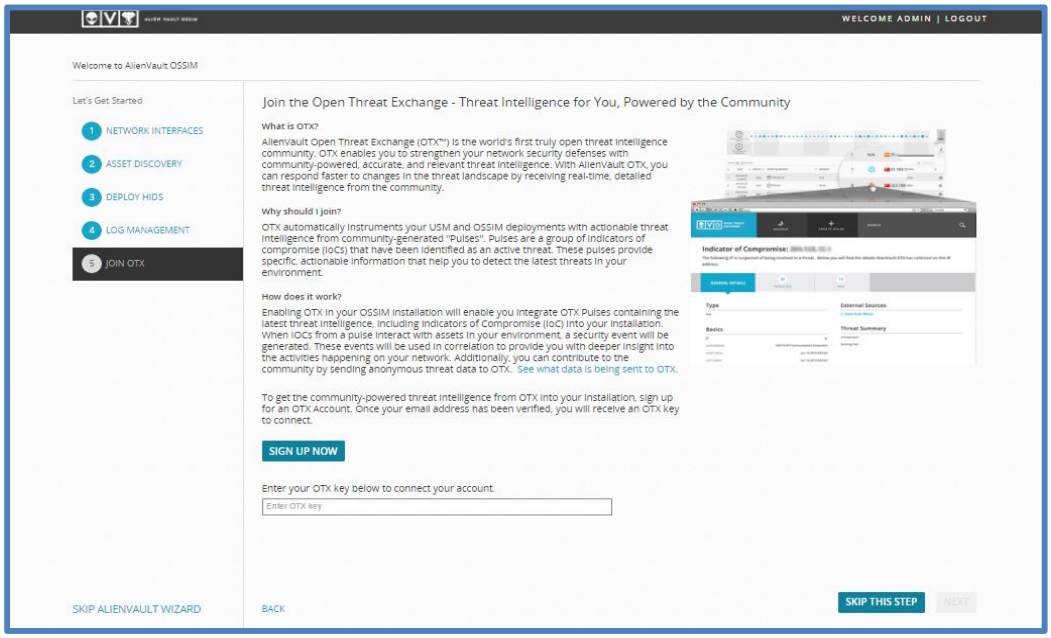


Figura B. 16 Intercambio de amenazas

Una vez terminada la configuración del wizard, podemos acceder al framework Ossim.

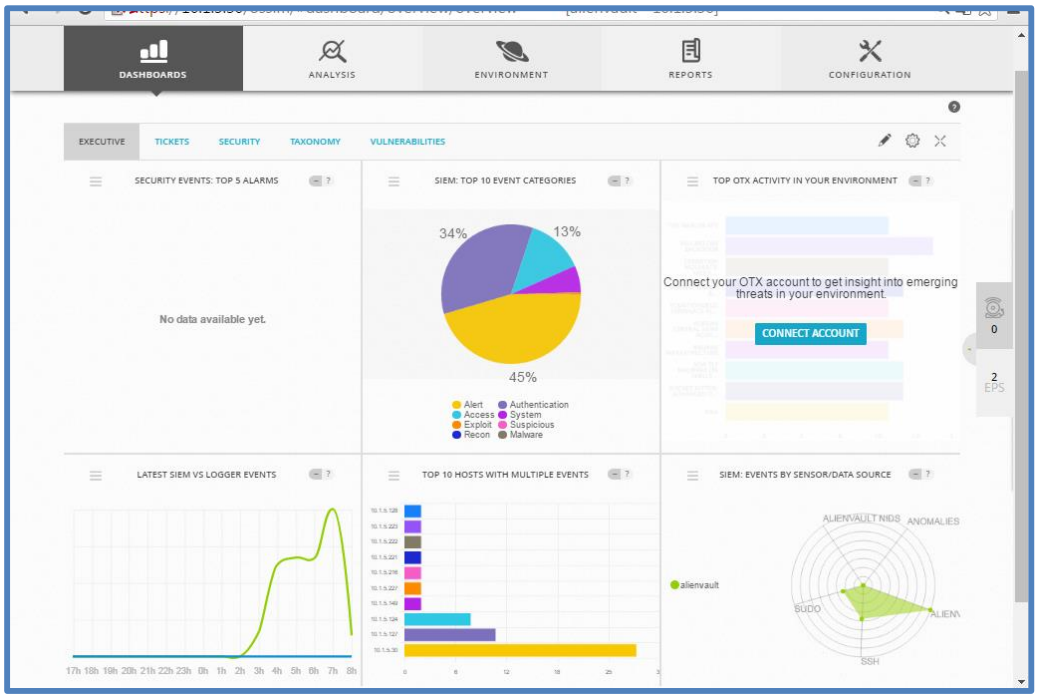


Figura B. 17 Framework OSSIM

B.3. Envío de correo electrónico

Para poder configurar el envío de correo electrónico configuramos los siguientes parámetros: email_notify, mailserver_relay, mailserver_relay_passwd, mailserver_relay_port, mailserver_relay_user.

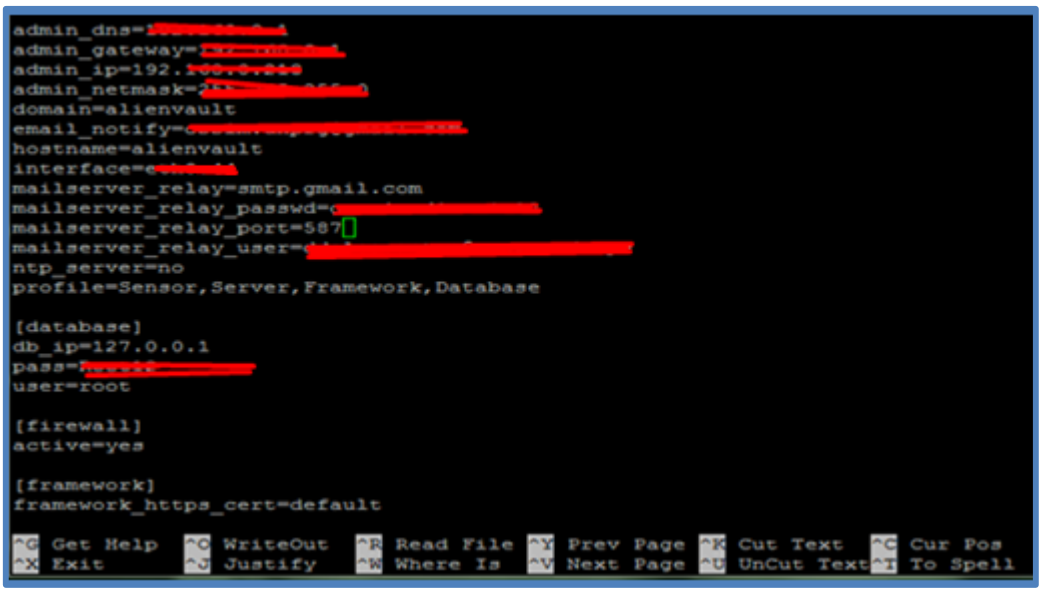


Figura B. 18 Configuración de parámetros para envío de correo electrónico

Para probar que el mail Relay se ha configurado correctamente ejecutamos el siguiente comando para enviar un correo de prueba:

echo “mensaje” | mail –s “asunto” correo_electronico_destinatario

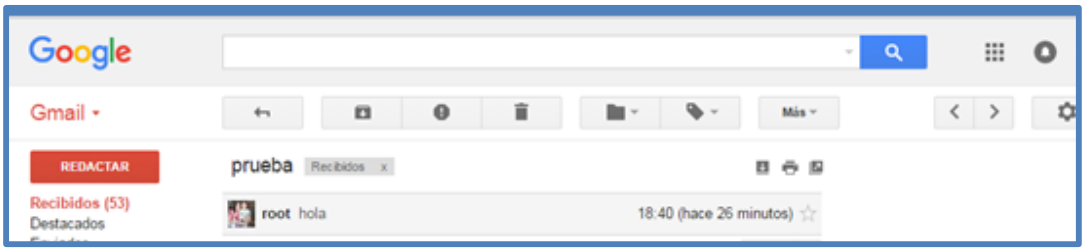


Figura B. 19 Verificación en la bandeja de entrada

B.4. Descubrimiento de activos

Ossim puede realizar un escaneo de los activos en nuestra red, de tal manera que nos proporciona información como IP, sistema operativo, etc.

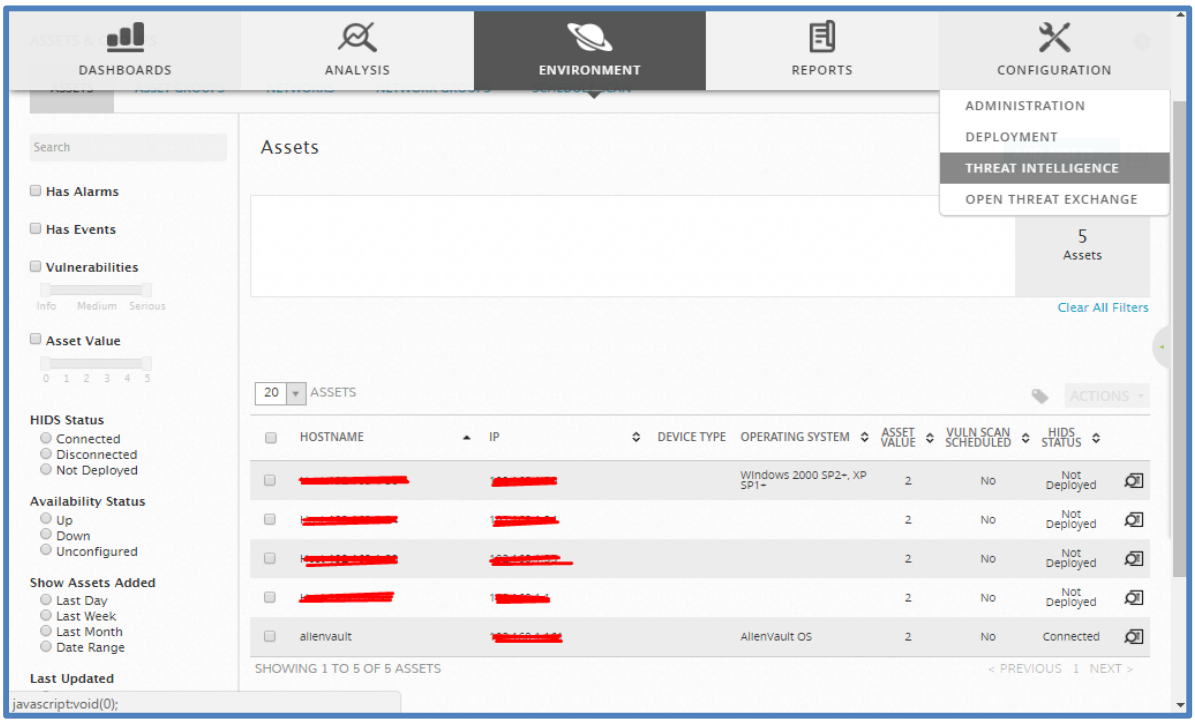


Figura B. 20 Escaneo de activos en red

Además nos permite habilitar el monitoreo de disponibilidad, detectar nuevo equipos agregados a la red, equipos que han presentado cambios de IP, MAC.

Podemos ver la información de los activos más detallada

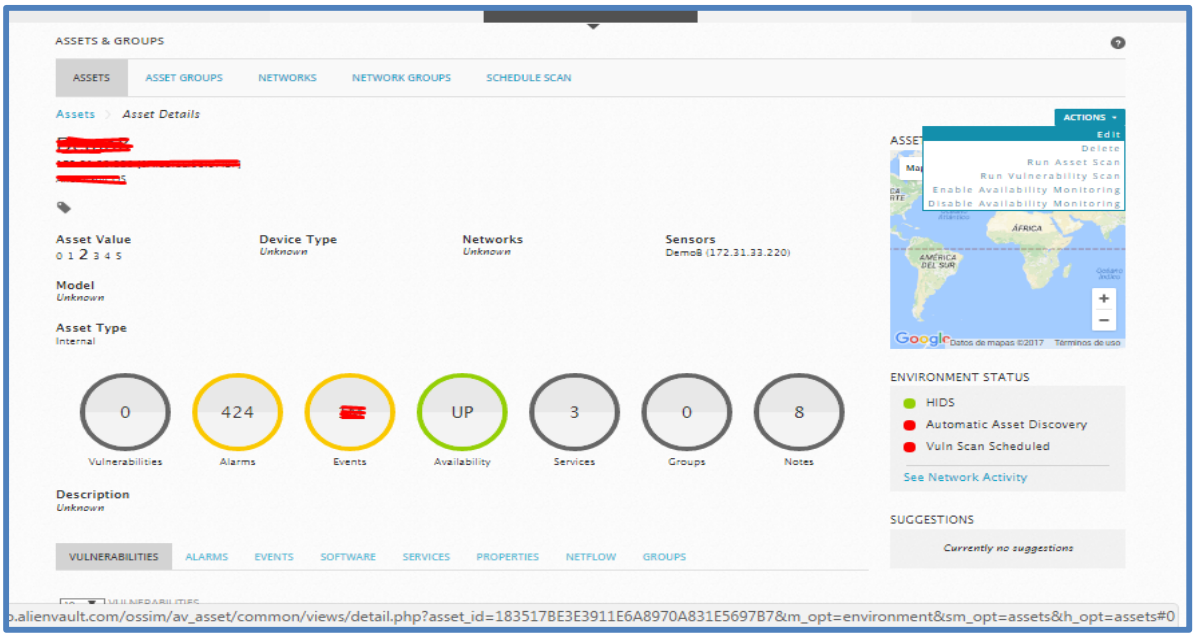


Figura B. 21 Detalle de los activos

B.5. Nagios

Nagios es una de las herramientas integradas en OSSIM, por lo que podemos configurar para recibir información de disponibilidad de los equipos.

<u>Instalación agentes en Windows:</u>

Primero será necesario instalar la herramienta NSClient++ en el equipo cliente en modo genérico (capacidad de trabajar con cualquier sistema de monitoreo).

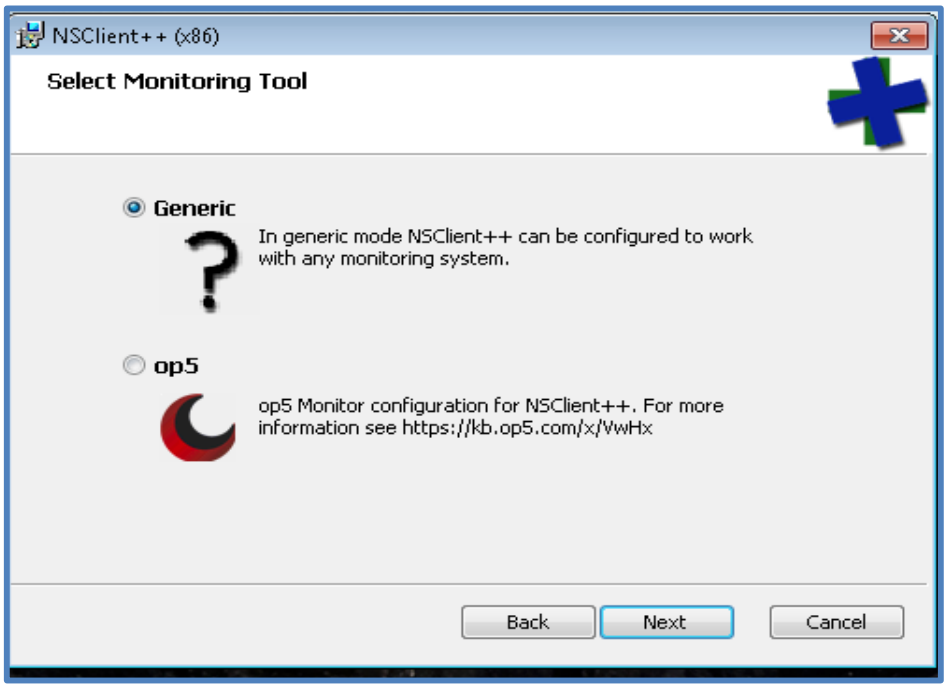


Figura B. 22 Instalación de NSClient ++

Ingresamos la IP del servidor que servirá de monitor y una contraseña que por defecto será la que a continuación vemos:

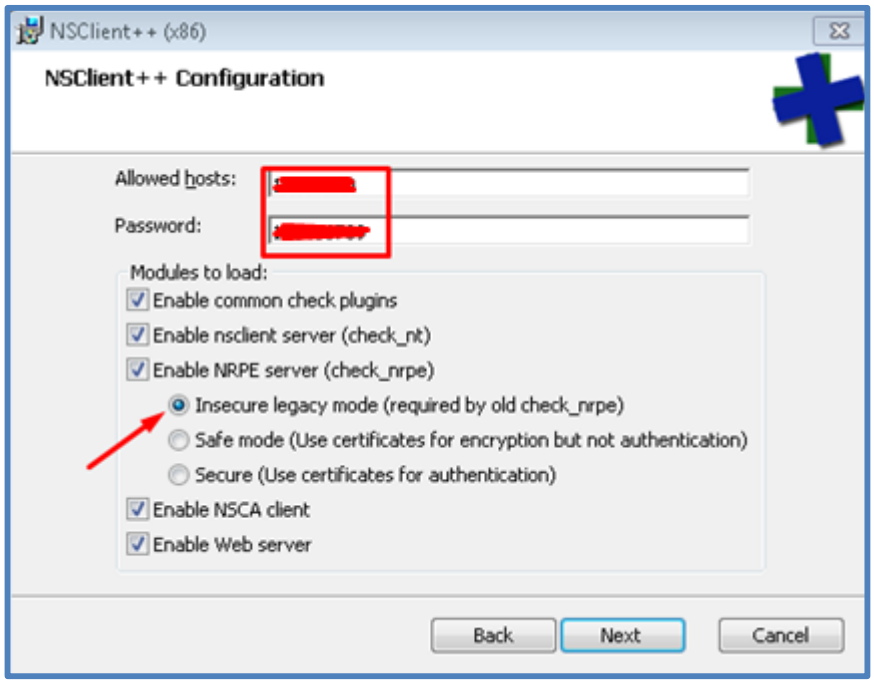


Figura B. 23 Configuración de parámetros de NSClient ++

Terminada la instalación, en una consola de Windows ejecutamos: services.msc para ver todos los servicios disponibles. Seleccionamos NSClient++(x86)

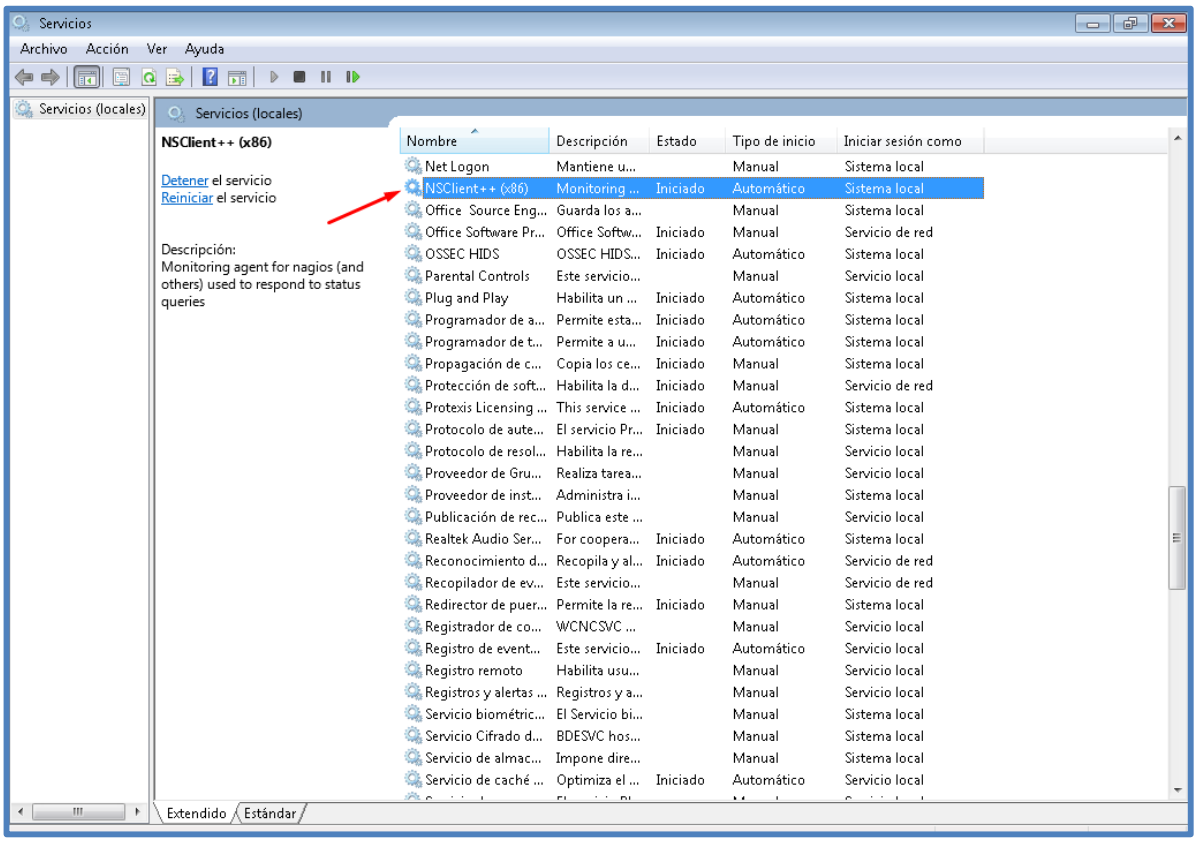


Figura B. 24 Servicios locales en el equipo

En propiedades/iniciar sesión permitimos que el servicio interactúe con el escritorio

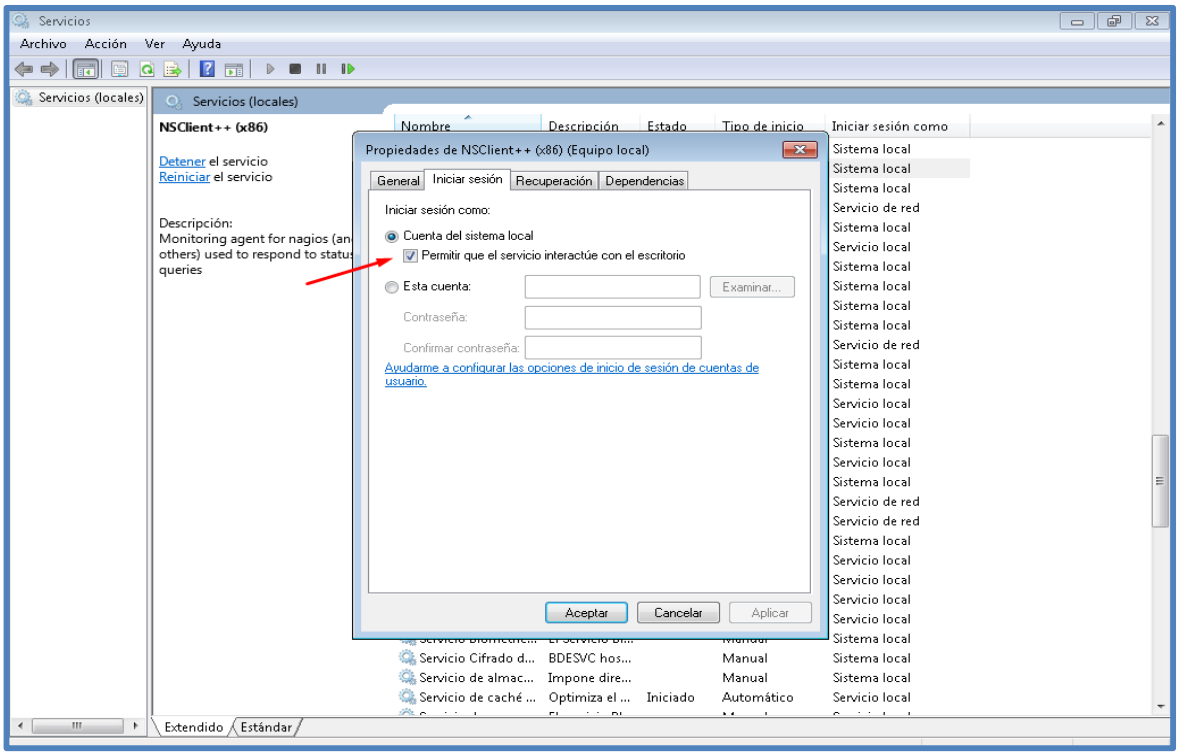


Figura B. 25 Configuración del servicio NSClient ++

Ejecutamos el símbolo del sistema como administrador

Y seguimos los siguientes pasos en línea de comando: (detenemos e iniciamos el servicio NSCP)

Creación de reglas en el firewall de Windows de nuestro cliente para permitir que responda el programa.

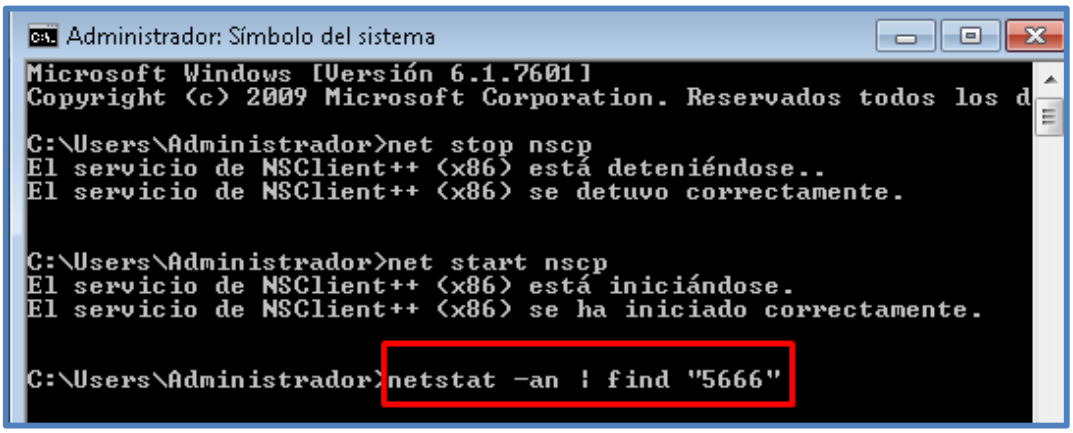


Figura B. 26 Creación de reglas en el firewall a través de símbolo del sistema

<u>Configuración en el servidor OSSIM</u>

Creación del archivo con extensión .cfg para nuestro cliente.

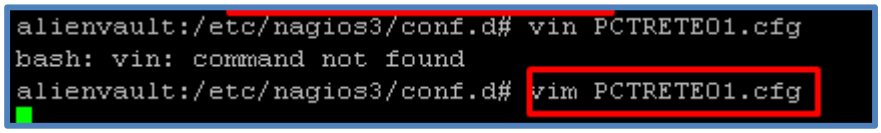


Figura B. 27 Configuración para monitoreo del equipo cliente

En el archivo con extensión .cfg creado definiremos el host y los servicios a monitorizar

```
#####DEFINE HOST
define host {
        use generic-host
        host_name PCTRETE01
        alias Windows
        address [redacted]

}

#####DEFINE SERVICE
define service{
        use generic-service
        host_name PCTRETE01
        service_description NSClient Version
        check_command check_nt!CLIENTVERSION
}

define service{
        use generic-service
        host_name PCTRETE01
        service_description Uptime
        check_command check_nt!UPTIME
}

define service{
        use generic-service
        host_name PCTRETE01
        service_description CPU Load
        check_command check_nt!CPULOAD!-w 80 -c 90 -l 5,80,90
}
```

Figura B. 28 Definición del equipo y servicios a monitorear

Editaremos el archivo nt.cfg y verificamos que no haya ningún error

```
# If you are confused about this command definition, cause you was
# reading other suggestions, please have a look into
# /usr/share/doc/monitoring-plugins/README.Debian

# 'check_nt' command definition
define command {
        command_name    check_nt
        command_line    /usr/lib/nagios/plugins/check_nt -H $HOSTADDRESS$ -p 12489 -s [redacted] -v $ARG1$ $ARG2$ -t 180
}

# 'check_nscp' command definition
define command {
        command_name    check_nscp
        command_line    /usr/lib/nagios/plugins/check_nt -H '$HOSTADDRESS$' -p 12489 -v '$ARG1$'
}
```

password del ns_client

Figura B. 29 Configuración de nt.cfg

En la interfaz web del sistema verificamos que se recopile la información de nuestro equipo monitoreado.

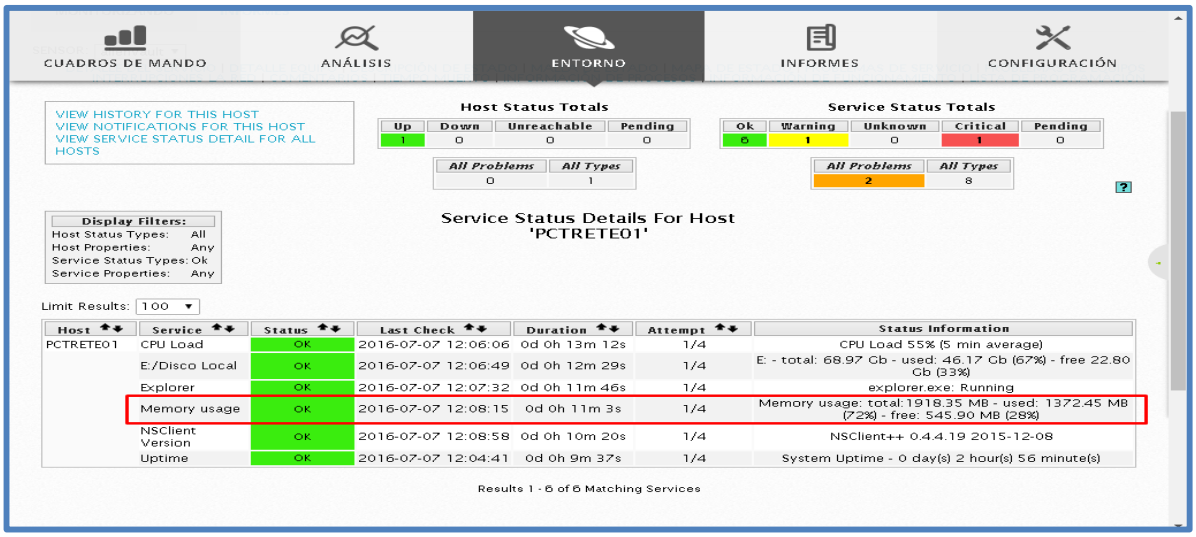


Figura B. 30 Monitoreo de hosts y servicios a través de Nagios

B.6. Ossec

OSSEC es un sistema de código abierto para detección de intrusiones basado en host. Se realiza el análisis, la comprobación de la integridad, la supervisión del registro de Windows, detección de rootkits, alertas en tiempo real y la respuesta activa de registro. Se ejecuta en la mayoría de sistemas operativos, incluyendo Linux, OpenBSD, FreeBSD, Mac OS X, Solaris y Windows.

Agente en Windows

Antes de instalar el agente verificaremos que el visor de eventos este recopilando los eventos del equipo.

Luego en la interfaz web: Entorno > Detección > Agentes

Agregamos el equipo Windows del cual recibiremos sus eventos.

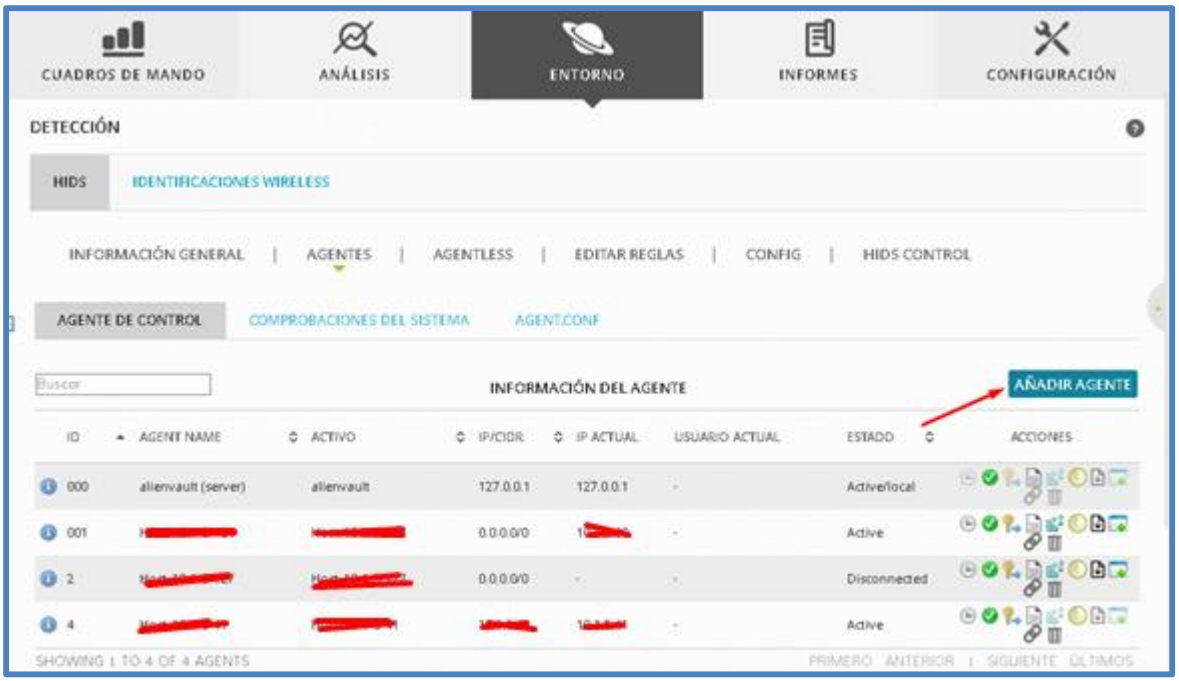


Figura B. 31 Listado de agentes monitoreados por Ossec

Luego descargamos el ejecutable y lo instalamos en el agente o hacemos un despliegue automático.

Reiniciamos el agente y el servidor Ossec.

Si la instalación ha sido correcta podemos visualizar en SIEM que recibimos eventos de dicho agente.

Figura B. 32 Eventos detectados por Ossec

Agente en Linux

La instalación del agente Ossec lo haremos en un equipo Centos, primeramente instalaremos los prerrequisitos:

```
sudo yum groupinstall "Development Tools" -y &&
sudo yum install kernel-devel -y
```

Figura B. 33 Instalación de prerrequisitos de Ossec en equipos Linux

Luego descargamos el agente:

wget https://bintray.com/artifact/download/ossec/ossec-hids/ossec-hids-2.8.3.tar.gz

Desempaquetamos y compilamos:

```
[root@localhost src]# cd ./ossec-hids-2.8.3
[root@localhost ossec-hids-2.8.3]# /bin/bash ./install.sh
which: no host in (/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:
/root/bin)

  ** Para instalação em português, escolha [br].
  ** ■ ■ ■ ■ ■ ■ ■ ■ ■ , ■ ■ ■  [cn].
  ** Fur eine deutsche Installation wohlen Sie [de].
  ** ■■■ ■■■■■■■■■■■ ■■■ ■■■■■■■■, ■π■■■■■■■ [el].
  ** For installation in English, choose [en].
  ** Para instalar en Español , eliga [es].
  ** Pour une installation en français, choisissez [fr]
  ** A Magyar nyelvű telepítéshez válassza [hu].
  ** Per l'installazione in Italiano, scegli [it].
  ** ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ [jp].
  ** Voor installatie in het Nederlands, kies [nl].
  ** Aby instalować w języku Polskim, wybierz [pl].
  ** Для инструкций по установке на русском ,введите [ru].
  ** Za instalaciju na srpskom, izaberi [sr].
  ** Türkçe kurulum için seçin [tr].
  (en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: es_
```

Figura B. 34 Instalación de Ossec Agente 2.8.3

Seleccionamos el tipo de instalación en este caso agente

```
1- Que tipo de instalación Usted desea (servidor, agente, local ó ayuda)? agente

  - Usted eligió instalación de Agente(cliente).

2- Configurando las variables de entorno de la instalación.

 - Eliga donde instalar OSSEC HIDS [/var/ossec]:

    - La instalación se realizará en  /var/ossec .

3- Configurando el sistema OSSEC HIDS.

  3.1- Cuál es la direccion ó nombre de vuestro del servidor OSSEC HIDS?: [redacted]
```

Figura B. 35 Tipo de instalación de Ossec a seleccionar

Configuramos unos parámetros más y finalizaremos la instalación.

```
 - La configuración puede ser leída ó mofificada en /var/ossec/etc/ossec.conf


    Gracias por usar OSSEC HIDS.
    Si tuviera Usted alguna duda, sugerencia ó haya encontrado
    algun desperfecto, contactese con nosotros a contact@ossec.net
    ó usando nuestrs lista pública de correo en ossec-list@ossec.net

    Más información puede ser encontrada en http://www.ossec.net

            ---  Presione ENTER para finalizar. ---
       (Tal vez encuentre más información a continuación).


 - Usted debe de añadir este agente en el servidor así podran
   comunicarse el úno con el ótro. Una vez culminada la tarea
   podra ejecutar la herramienta 'manage_agents' para importar
   la autentificación de llaves extraidas del servidor.

   /var/ossec/bin/manage_agents

   Más información en:
   http://www.ossec.net/en/manual.html#ma

[root@localhost ossec-hids-2.8.3]#
```

Figura B. 36 Instalación de Ossec terminada

Reiniciamos Ossec tanto en el agente como el servidor para recibir los eventos del agente en el sistema Ossim.

B.7. Usuarios

Ossim tiene diferentes niveles de usuario para la administración y gestión:

- Usuario Root: creado durante la instalación. Este usuario puede acceder y realizar todas las operaciones en la consola Ossim, además es el único que puede restablecer la contraseña del administrador por defecto.
- Default Admin: Creada la primera vez que un usuario accede a la interfaz web.

  Tiene todo el acceso y la visibilidad en la interfaz web OSSIM.

Puede crear los administradores con acceso completo a la interfaz web y usuarios con diferentes grados de acceso a determinados componentes de Ossim.

En el framework Ossim se pueden crear usuarios locales y por LDAP (integración con Active Directory)

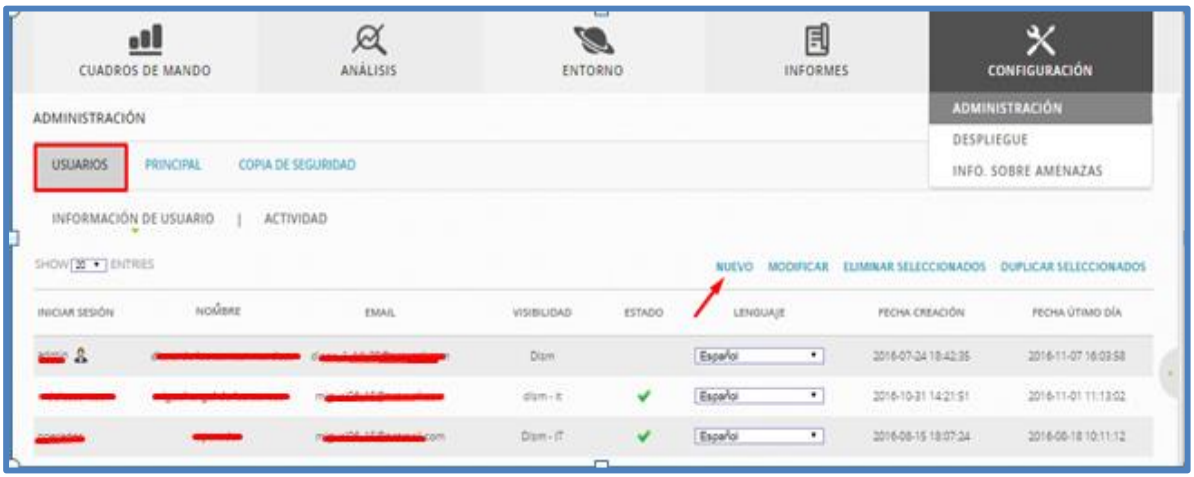


Figura B. 37 Usuarios del sistema

B.8. Tickets

El sistema de tickets AlienVault le permite hacer lo siguiente:

- Delegar tareas a otros usuarios administradores
- Seguir el progreso en la investigación de alarmas y eventos específicos

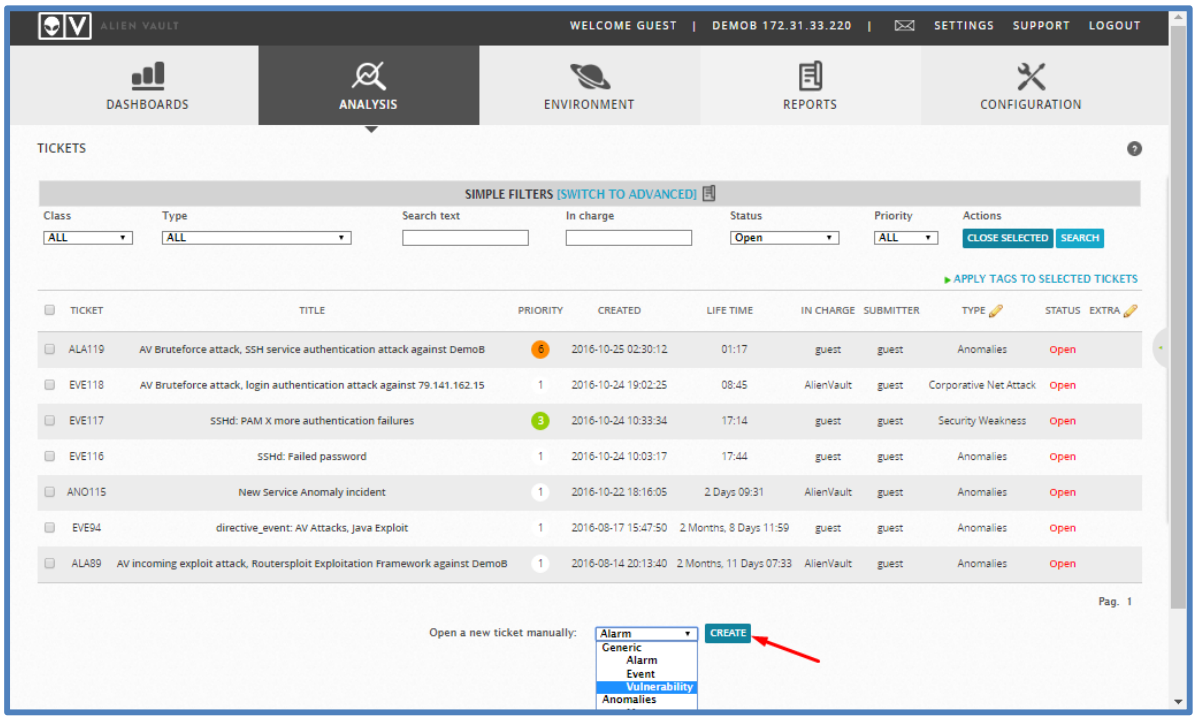


Figura B. 38 Sistema de tickets según el tipo de incidencias

La prioridad que se le asigna a un ticket es de 1 a 10 (bajo, medio, alto).

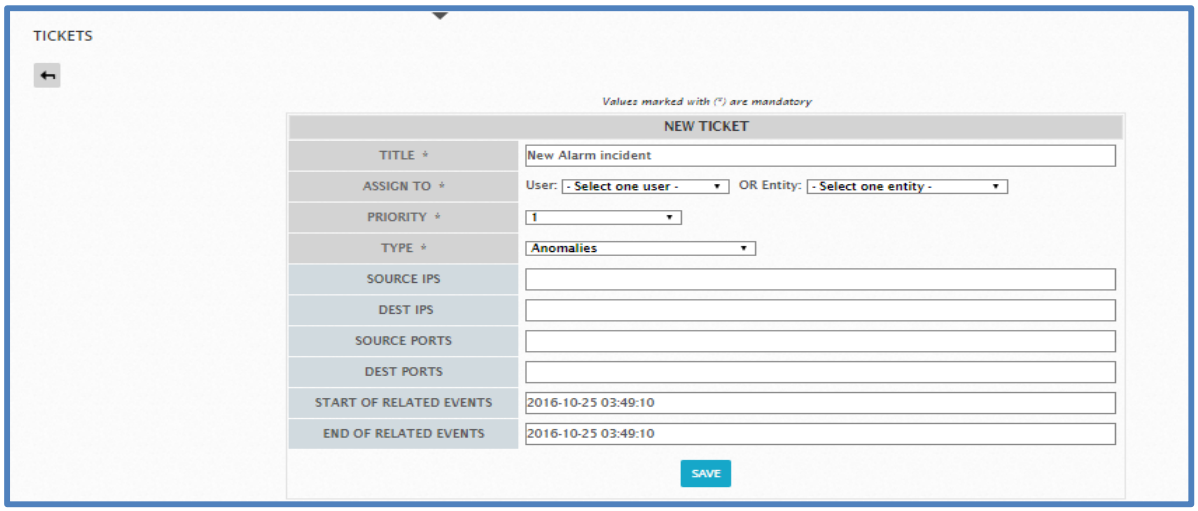


Figura B. 39 Parámetros a ingresar para crear un ticket

B.9. Políticas

Las políticas juegan un papel crítico en la respuesta efectiva a incidentes e influyen en muchos aspectos de la USM, por ejemplo:

- El procesamiento de eventos
- Filtrado de eventos que no necesitan ser procesados, tales como los hechos que provocan alarmas falsas positivas o ruidosos.

Las políticas incluyen condiciones y consecuencias. Las condiciones determinan que eventos son procesados por la política. Las consecuencias definen que sucederá cuando los eventos coinciden con las condiciones especificadas.

AlienVault le permite crear políticas para eventos externos y del sistema

Grupos de políticas

- Por defecto grupo de política

Contienen las políticas que se crean para manejar los eventos externos. Los eventos externos incluyen todos los eventos recogidos de sistemas externos a la red a través de los sensores.

- Políticas AV predeterminadas

Esta sección filtra los eventos del usuario AVAPI, un servicio interno al Server que realiza numerosas tareas del sistema. Los clientes que se encuentren viendo todos estos registros molestos pueden filtrar acontecimientos de la política, para que no aparezcan en eventos de seguridad (SIEM) o en los registros RAW LOG (solo USM). Estas políticas se encuentran deshabilitadas a partir de la versión 5.3.2 viene habilitada por defecto.

- Políticas para eventos generados en el servidor

Contienen las políticas que se crean para manejar los eventos del sistema.

Los eventos del sistema, también llamada directiva eventos, incluir los eventos generados por el Server dentro de su red.

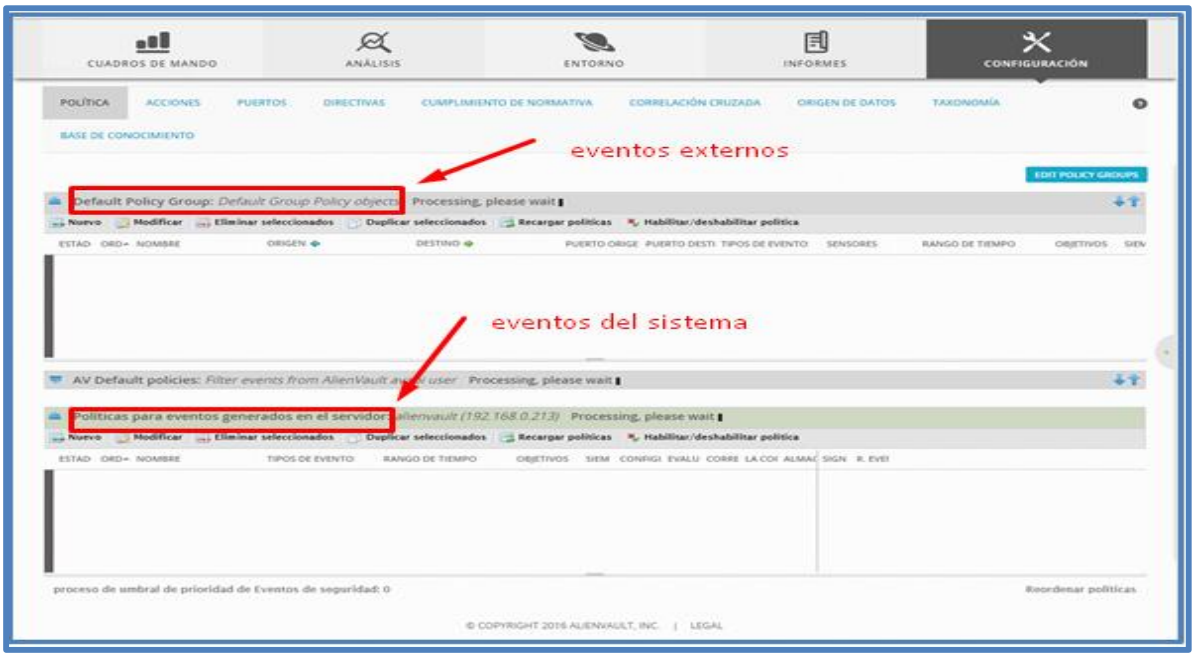


Figura B. 40 Tipos de políticas a configurar en el sistema

Creación de políticas

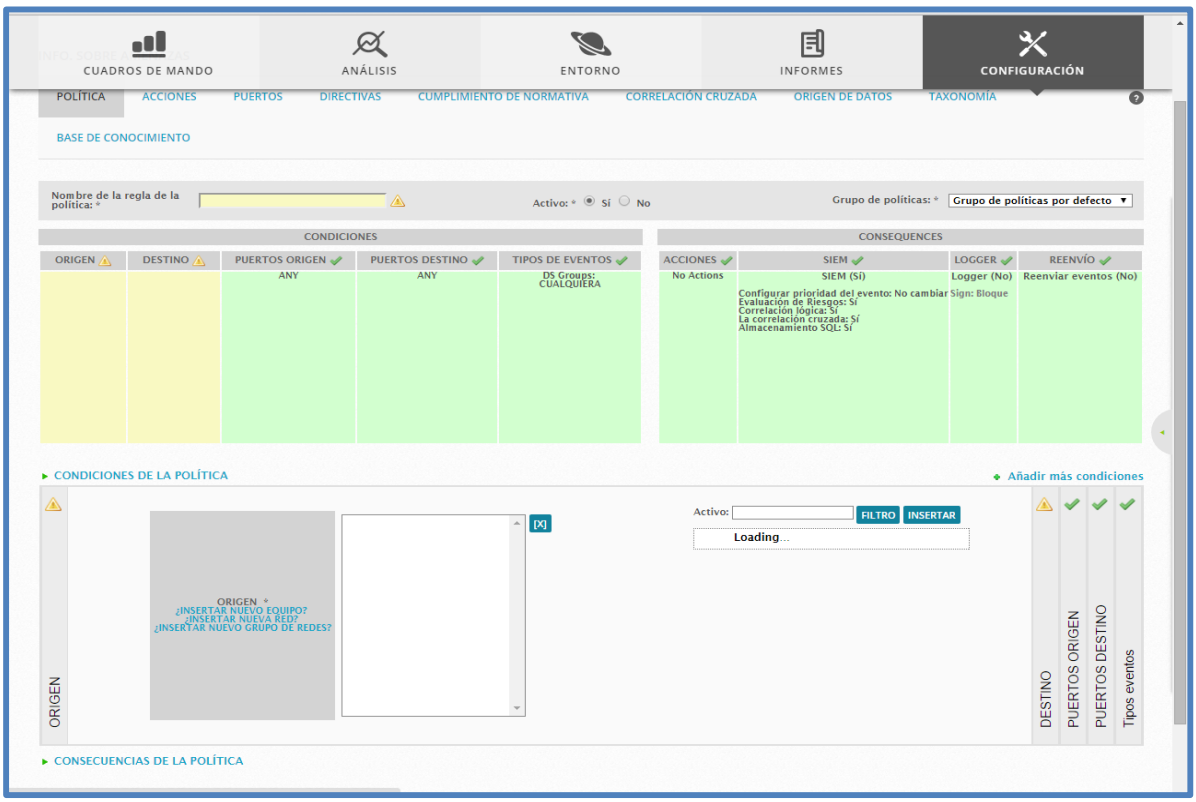


Figura B. 41 Condiciones a configurar en una política

Las condiciones de política determinan qué eventos son procesados por la política.

✓ **Origen**

Define activos, grupos de activos, redes o grupos de la red como la dirección IP de origen del evento. Eligiendo una fuente, usted determina que sólo los eventos que provienen de esa fuente serán procesados por esta política

✓ **Destino**

Define activos, grupos de activos, redes o grupos de la red como la dirección IP de destino de un evento. Al elegir un destino, están determinando que sólo los eventos que tienen ese destino específico serán procesados por esta política.

✓ **Puerto de origen**

Define el puerto TCP/UDP de origen de un evento. También puede elegir a CUALQUIERA como una condición del puerto de la fuente de aceptar todos los puertos.

✓ **Puerto de destino**

Define el puerto de destino de un evento.

✓ **Tipo de evento**

Define los tipos de eventos que serán procesados por esta política.

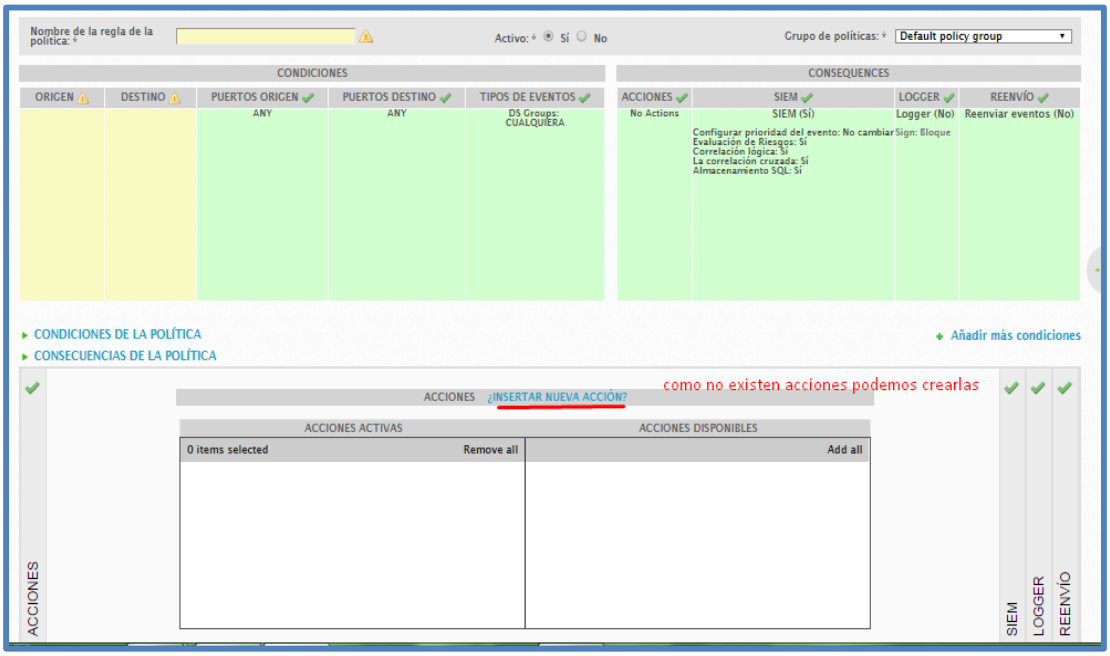


Figura B. 42 Consecuencias a configurar en una política

Las consecuencias definen que sucederá cuando los eventos coinciden con las condiciones especificadas.

✓ **Acciones**

La sección de acciones define acciones tomadas como consecuencia de condiciones en la política.

Hay tres posibles acciones que puede configurar:

• Enviar un correo electrónico a una dirección de correo electrónico preconfigurada.

• Ejecutar un comando para invocar un script en AlienVault.

• Abra un ticket en el sistema interno de incidencias de AlienVault

B.10. Vulnerabilidades

AlienVault ofrece una evaluación de la vulnerabilidad como parte de un paquete completo de capacidades de monitorización y gestión de la seguridad para la detección de amenazas eficiente. Debido a que para mejorar la seguridad en la red, primero tiene que saber lo que es vulnerable.

Correspondencias internas entre los umbrales de las entradas de la vulnerabilidad

Gravedad	Valor interno
Grave	1
Alto	2
Medio	3
Bajo	6
información	7

Figura B. 43 Correspondencias internas entre umbrales de entradas de vulnerabilidad

AlienVault normaliza estos valores usando la siguiente formula:

$risk = 8 - $internal_value

La realización de exploraciones de vulnerabilidades

Accedemos a la interfaz web de Ossim y en Entorno seleccionamos Vulnerabilidades y también seleccionamos Nuevo Trabajo de escaneo.

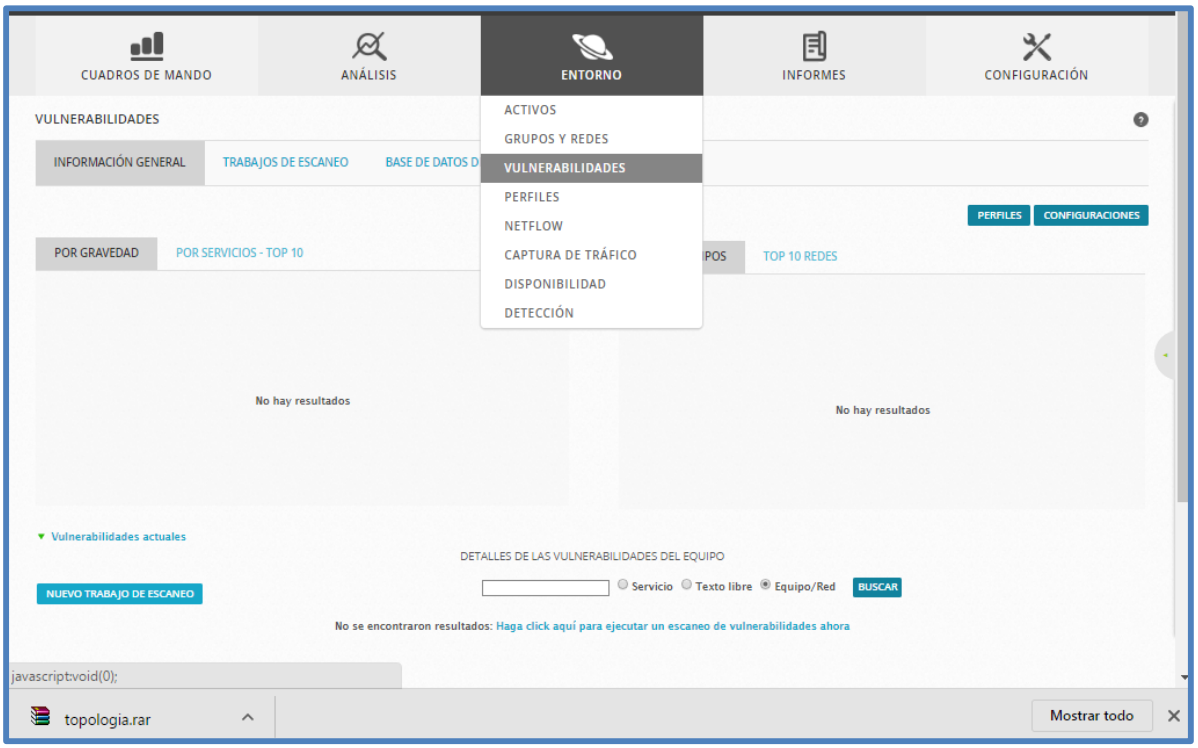


Figura B. 44 Crear un nuevo trabajo de escaneo de vulnerabilidades

Seleccionamos un perfil existe y los equipos que evaluaremos sus vulnerabilidades, luego nos mostrara resultados como se muestra en la siguiente imagen.

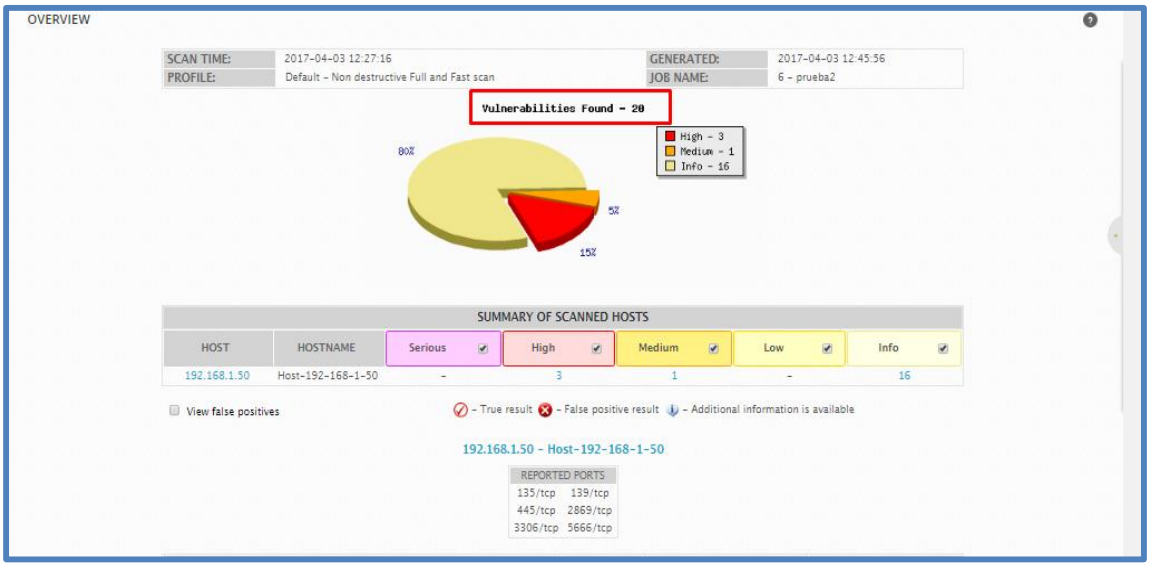


Figura B. 45 Vulnerabilidades detectadas

B.11. Netflow

NetFlow es un protocolo estándar de la industria diseñada por Cisco Systems que le permite capturar información sobre los flujos de red (comunicación entre los hosts que utilizan TCP / IP).

El sensor de AlienVault puede generar información NetFlow del tráfico recibido en los puertos reflejados o dispositivos de red pueden enviar información NetFlow directamente al Servidor.

Figura B. 46 Información proporcionada por Netflow

B.12. Captura de tráfico

AlienVault permite capturar el tráfico en la red para el análisis fuera de línea y forense.

Figura B. 47 Captura de tráfico en la red

B.13. Cumplimiento Normativo

Ossim cumple ciertos aspectos de la ISO 27001, así como también PCI DSS 2 Y PCI DSS3

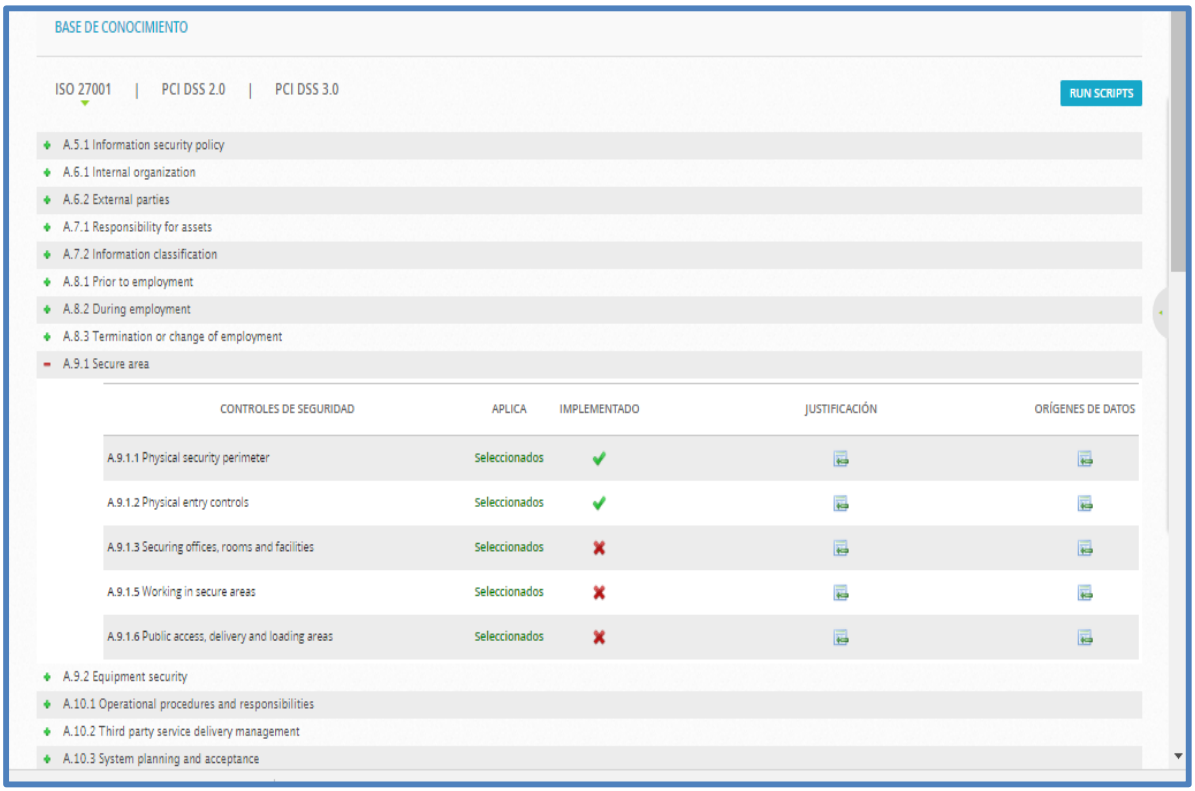


Figura B. 48 Cumplimiento Normativo ISO 27001

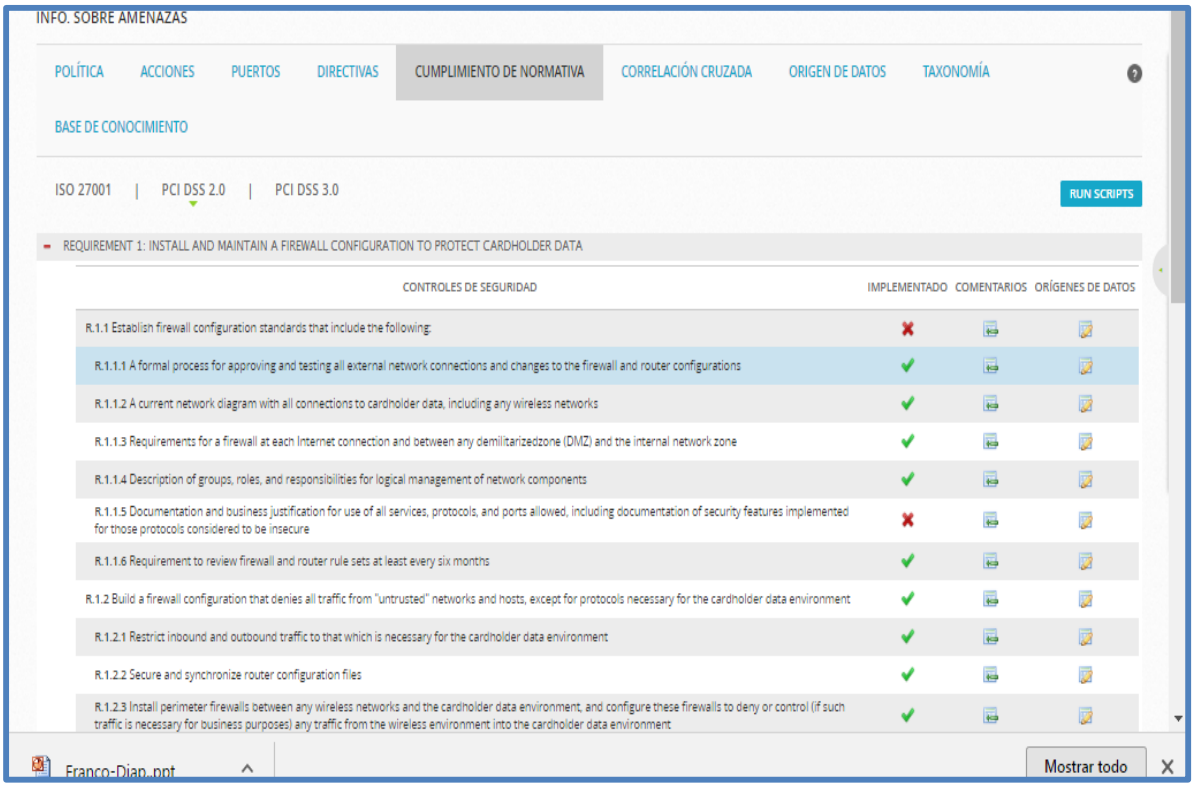


Figura B. 49 Cumplimiento Normativo PCI DSS 2.0

B.14. Dashboard y Reportes

Dashboard

Proporciona visibilidad global en la actividad de la red, y muestra diversas métricas de seguridad de red.

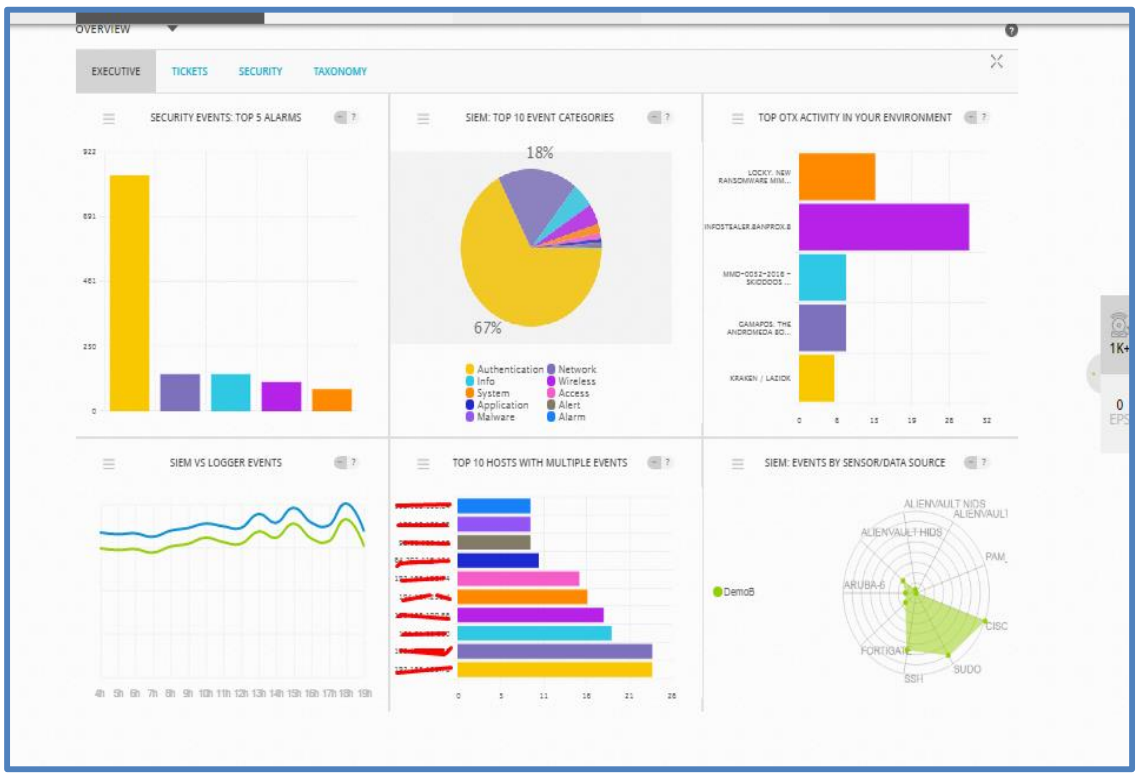


Figura B. 50 Dashboard nivel gerencial

Reportes

Ossim permite generar reportes y descargarlos en formatos pdf o enviarnos a un correo electrónico.

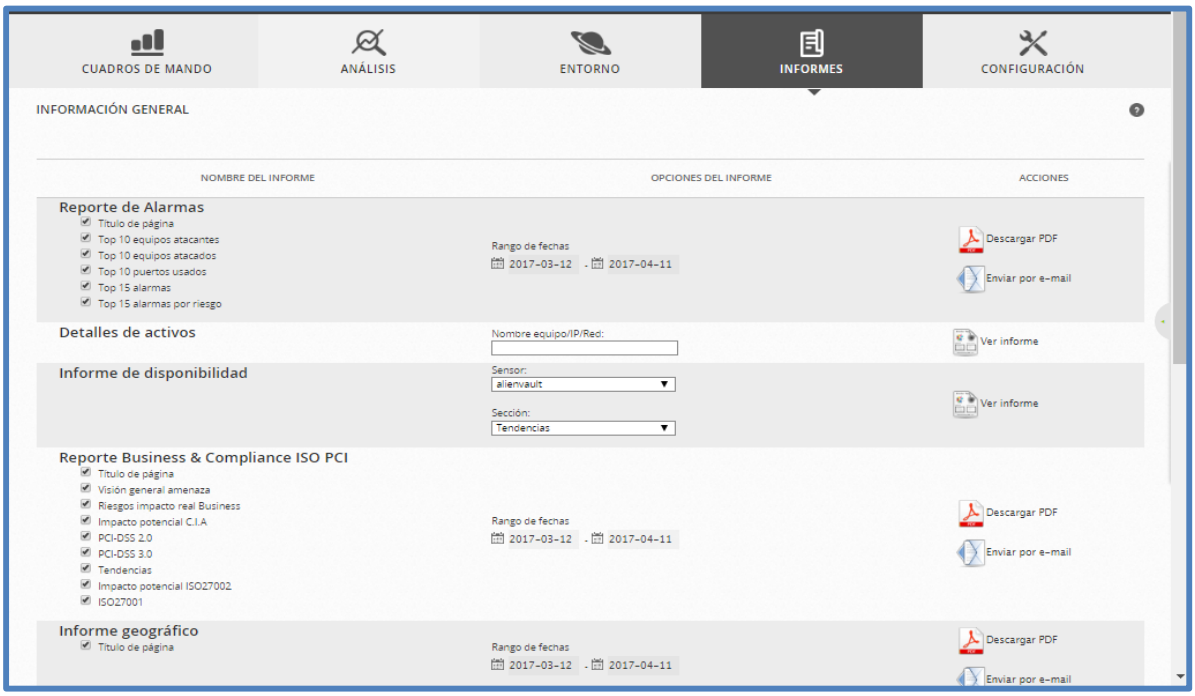


Figura B. 51 Reportes generados por Ossim

APÉNDICE C. GUÍA DE AUTOEVALUACIÓN: EL USO DE COBIT ® 5 (SELF-ASSESSMENT GUIDE: USING COBIT ® 5)

C.1. Introducción

¿Qué capacidades tienen sus procesos de TI? ¿Satisfacen las necesidades de la empresa?

C.1.1. El Programa de Evaluación de COBIT

El programa de evaluación de COBIT está diseñado para proporcionar a las empresas una metodología repetible, fiable y robusta para la evaluación de la capacidad de sus procesos de TI. Tales evaluaciones normalmente se utilizan como parte del programa de mejora de los procesos de una empresa y luego se pueden utilizar para informar a la alta dirección ejecutiva de la empresa sobre la capacidad actual de sus procesos de TI y de los objetivos de mejora que deben tenerse en cuenta, para poder atender los requerimientos del negocio.

Estas evaluaciones se pueden utilizar como parte de la iniciación de un programa de mejora de procesos o para evaluar el progreso después de un período de mejora de procesos.

El programa de evaluación de COBIT incluye:

a. Modelo de Evaluación de Procesos COBIT® (PAM): Usando COBIT 5
   - Basado en COBIT 5 e ISO/IEC 15504.
   - El proceso de evaluación permite la evaluación fiable, consistente y repetible de un proceso en el ámbito de la gobernanza y la gestión de la empresa de TI basada en la evidencia.
   - El modelo de evaluación permite a los órganos internos de evaluación de las empresas apoyar la mejora de procesos.

b. Guía Asesor COBIT® 5
   - Este producto es compatible con los que quieren llevar a cabo una evaluación de carácter formal, basada en la evidencia.

c. Guía de Autoevaluación COBIT® 5
   - Este producto ha sido desarrollado para apoyar el desempeño para las más simples y menos rigurosas autoevaluaciones.

d. Kit de herramientas del programa de evaluación COBIT® 5
   - Las herramientas soportan actividades para la evaluación de procesos e incluye plantillas base. Las herramientas dan soporte a la Guía Asesor COBIT® y a la Guía de Autoevaluación COBIT® 5. También incluye: los objetivos de negocio y los objetivos de TI.

C.1.2. Propósito de la autoevaluación COBIT

La guía de autoevaluación se ofrece como una publicación 'stand alone-'5, que puede ser utilizado por las empresas para llevar a cabo una evaluación de la capacidad de sus procesos de TI menos rigurosa. Es una evaluación previa y más rigurosa, basada en la evidencia. El enfoque se basa en la utilización del programa COBIT PAM, pero no exige requisitos de prueba en apoyo de la auto-evaluación. Sin embargo, se recomienda a los usuarios consultar el COBIT PAM, la guía evaluador y el kit de herramientas.

C.2. El Programa de Evaluación COBIT-Información general

El Modelo de Referencia de Proceso (PRM) para el programa de evaluación de COBIT es COBIT 5. Esto significa que COBIT 5 ofrece definiciones de los procesos en un ciclo de vida, junto con una arquitectura que describe las relaciones entre los procesos.

C.2.1. Arquitectura COBIT 8

El COBIT 5 PRM es un ciclo de vida para la gobernanza y la gestión de la TI empresarial, compuesta por 37 procesos, como se muestra en la figura C.1.

Figura C. 1 Modelo de referencia de proceso COBIT 5 (PRM)

[5] Stand alone: independiente

C.2.2. Marco de medición

El proceso de evaluación implica el establecimiento de una clasificación de la capacidad para cada proceso. Esto considera:

- Niveles de capacidad definidos (de ISO / IEC 15504)
- Atributos de proceso, utilizado para evaluar cada proceso (de ISO / IEC 15504)
- Los indicadores en los que se basa la evaluación de cada atributo de proceso (basado en la norma ISO / IEC 15504)
- Una escala de calificación estándar (de ISO / IEC 15504)

C.2.2.1. Niveles de capacidad de procesos

La capacidad de cada proceso evaluado se expresa como un nivel de capacidad de 0 a 5, como se muestra en la figura C.2. Cada nivel de capacidad de proceso está alineado con una situación proceso.

Nivel de capacidad del proceso	Capacidad
0 (Incompleto)	El proceso no se ejecuta o no lograr su propósito. En este nivel, hay poca o ninguna evidencia de los logros de la finalidad proceso.
1 (Realizado)	El proceso implementado logra su propósito.
2 (Administrado)	El proceso realizado ahora se implementa de una manera administrada (planeada, monitoreada y ajustada) y sus productos o resultados se establecen adecuadamente, se controlan y mantienen.
3 (Establecido)	El proceso gestionado ahora se implementa mediante un proceso definido que es capaz de lograr los resultados definidos del proceso.
4 (Predecible)	El proceso establecido ahora opera dentro de los límites definidos para lograr sus resultados del proceso (se mide).
5 (Optimizado)	El proceso predecible se mejora continuamente para satisfacer los objetivos de negocio actual y proyectado.

Figura C. 2 Niveles de Capacidad de Procesos

El Proceso de nivel de capacidad 0 no tiene un atributo. El Nivel 0 refleja un proceso no aplicado o un proceso que no logra alcanzar al menos parcialmente sus resultados.

Como parte de la determinación del alcance, la empresa debe elegir el nivel de capacidad que requiere alcanzar, en función de los objetivos de negocio.

La determinación del alcance también puede restringir una evaluación para reducir la complejidad, el esfuerzo y el costo de la evaluación.

C.2.2.2. Atributos de proceso

Dentro del COBIT PAM, la medida de la capacidad se basa en los nueve atributos de proceso (prefijo PA) definidos en la norma ISO / IEC 15504-2, como se muestra en la figura C.3. Cada

atributo se aplica a una capacidad de proceso específico. Los Atributos de proceso se utilizan para determinar si un proceso ha alcanzado una capacidad determinada.

C.2.2.3. Indicadores de evaluación

Indicadores de evaluación del PAM COBIT proporcionan la base para determinar si los atributos de proceso se han logrado:

- Capacidad del nivel 1: los indicadores son específicos para cada proceso y se evalúa si el siguiente atributo se ha logrado. Lograr el "proceso implementado" es el propósito proceso.

  Para cada uno de los 37 procesos del COBIT PRM hay un contenido detallado.

- Capacidad de los niveles del 2 al 5: la evaluación de la capacidad se basa en indicadores de proceso de rendimiento genérico. Es genérico porque se aplican en todos los procesos, pero son diferentes las capacidades entre un nivel y otro.

  Para los niveles 2 a 5 se discuten los 'atributos genéricos considerados para todos uno de los procesos.

  Se entiende que cuanto mayor es el nivel de capacidad que un proceso alcanza, menor es el riesgo de que el proceso no cumpla su propósito previsto. También se entiende que cuanto mayor sea la capacidad, más costoso es la operación del proceso.

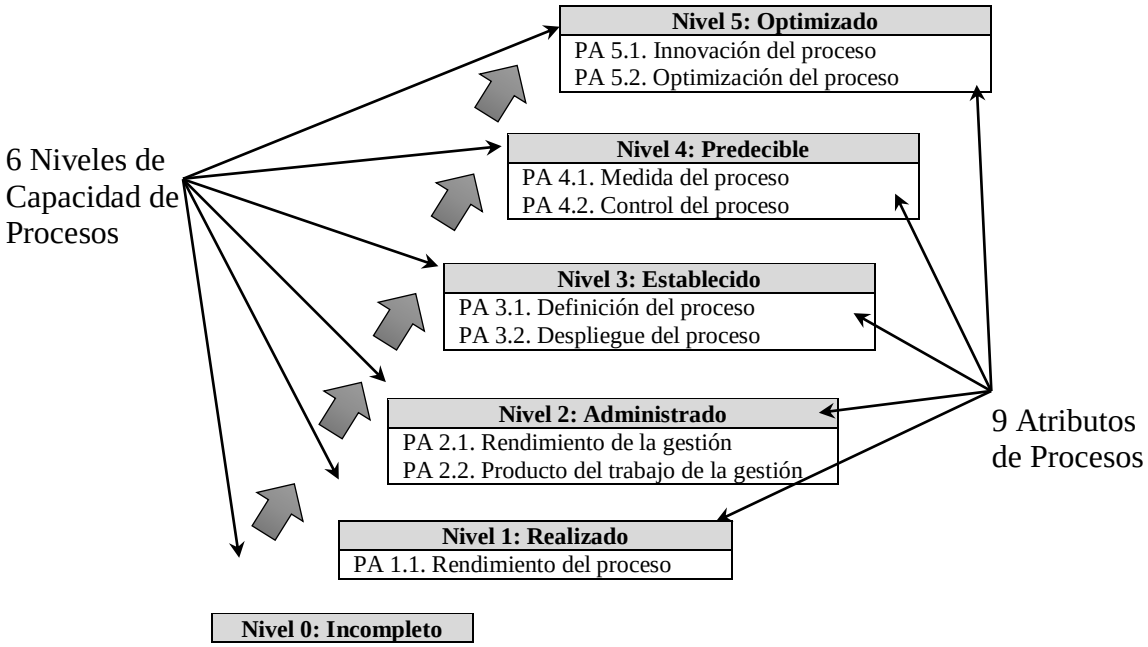


Figura C. 3 Atributos de proceso

C.2.2.4. Escala de evaluación

Cada atributo tiene el uso de una escala de calificación estándar definido en la norma ISO / IEC 15504. Esta clasificación se compone de:

- **N: No conseguido**. Hay poca o ninguna evidencia de logro del atributo definido en el proceso evaluado.
- **P: Logrado parcialmente**. Existe alguna evidencia de algún acercamiento al logro del atributo definido en el proceso evaluado. Algunos aspectos para el logro de los atributos pueden ser impredecibles.
- **L: Logrado en gran parte:** Hay evidencia de la aplicación de un enfoque sistemático para el logro significativo del atributo definido del proceso evaluado. Pueden existir algunas debilidades relacionadas con el atributo en el proceso de evaluación.
- **F: Logrado totalmente**. Hay evidencia de un enfoque completo y sistemático y, de la plena consecución del atributo definido del proceso evaluado. No existen debilidades significativas relacionadas con este atributo en el proceso evaluado.

Debe existir un grado constante de interpretación (para asignar la calificación) para garantizar una calificación correcta de los procesos. Por ejemplo, la tabla de la figura C.4 describe la calificación la escala de calificación definida anteriormente, en términos de una escala de porcentajes, que muestra el grado de logro.

Los evaluadores deben definir estas escalas antes de la evaluación para guiar su juicio en la calificación del logro de una capacidad determinada.

Escala de evaluación		Escala porcentual
N	No conseguido	0 a 15% de logro
P	Logrado parcialmente	>15% a 50% logrado
L	logrado en gran parte	>50% a 85% logrado
F	Logrado totalmente	>85% a 100% logrado

Figura C. 4 Escala de Niveles

C.2.2.5. Determinación del nivel de capacidad

El nivel de capacidad de un proceso depende de si el proceso ha logrado parte o totalmente los atributos de proceso de un nivel determinado y si los atributos de proceso para los niveles más bajos han sido plenamente alcanzado. La tabla de la figura C.5 describe cada nivel y las calificaciones necesarias que se deben alcanzar.

Escala	Atributos de proceso	Calificación
Nivel 1	PA 1.1. Rendimiento del proceso	En Gran Parte o Totalmente
Nivel 2	PA 1.1. Rendimiento del proceso PA 2.1. Rendimiento de la gestión PA 2.2. Producto del trabajo de la gestión	Totalmente En Gran Parte o Totalmente En Gran Parte o Totalmente
Nivel 3	PA 1.1. Rendimiento del proceso PA 2.1. Rendimiento de la gestión PA 2.2. Producto del trabajo de la gestión PA 3.1. Definición del proceso PA 3.2. Despliegue del proceso	Totalmente Totalmente Totalmente En Gran Parte o Totalmente En Gran Parte o Totalmente
Nivel 4	PA 1.1. Rendimiento del proceso PA 2.1. Rendimiento de la gestión PA 2.2. Producto del trabajo de la gestión PA 3.1. Definición del proceso PA 3.2. Despliegue del proceso PA 4.1. Medida del proceso PA 4.2. Control del proceso	Totalmente Totalmente Totalmente Totalmente Totalmente En Gran Parte o Totalmente En Gran Parte o Totalmente
Nivel 5	PA 1.1. Rendimiento del proceso PA 2.1. Rendimiento de la gestión PA 2.2. Producto del trabajo de la gestión PA 3.1. Definición del proceso PA 3.2. Despliegue del proceso PA 4.1. Medida del proceso PA 4.2. Control del proceso PA 5.1. Innovación del proceso PA 5.2. Optimización del proceso	Totalmente Totalmente Totalmente Totalmente Totalmente Totalmente Totalmente En Gran Parte o Totalmente En Gran Parte o Totalmente

Figura C. 5 Niveles y puntuaciones necesarias

Nota: Un proceso puede ser clasificado en un nivel con un atributo 'en gran parte' o 'totalmente' logrado. Sin embargo, tendrá que ser alcanzado plenamente para ser evaluado en el siguiente nivel.

C.3. El proceso de autoevaluación COBIT

El proceso de autoevaluación COBIT, que se muestra en la figura C.6, es un enfoque simplificado para la realización de una evaluación que no se basa en la evidencia, no requiere de un evaluador independiente o certificado y se puede realizar como un paso previo para una evaluación más formal. Una autoevaluación puede identificar brechas de proceso que requieren mejoras para superar una evaluación formal; permite realizar inversiones pequeñas y ayuda de la empresa en el establecimiento de niveles de capacidad objetivo.

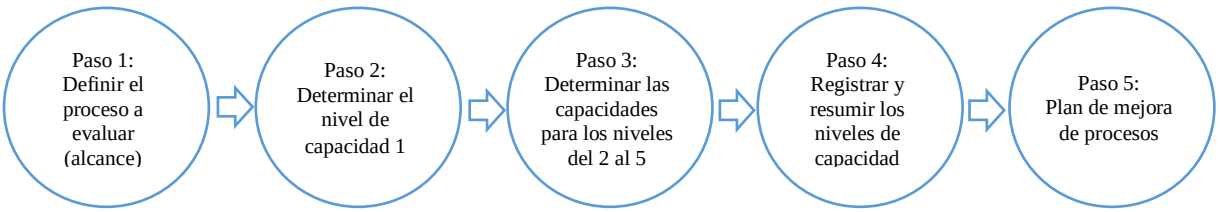


Figura C. 6 Proceso de autoevaluación

C.3.1. Paso 1. Decidir sobre el (los) procesos a evaluar (alcance)

El primer paso en la autoevaluación es decidir qué procesos deben ser evaluados. Se utiliza la plantilla de alcance en el kit de herramientas programa de evaluación de COBIT para ayudar a seleccionar los procesos para ser evaluados.

Una autoevaluación puede abordar todos los procesos de COBIT o centrarse en una serie de procesos de interés para la gestión de la empresa o en los relativos a los objetivos de negocio específicos para TI.

ID del proceso	Nombre del proceso	Evaluado?	Nivel objetivo	Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Procesos para la Gobernabilidad de TI de las empresas Evaluar, Orientar y Supervisar									
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.				F	L			
EDM02	Asegurar la entrega de beneficios								
EDM03	Asegurar la optimización del riesgo.								
EDM04	Asegurar la optimización de recursos								
EDM05	Asegurar la transparencia hacia las partes interesadas.								
Procesos para la Gestión de TI Alinear, Planificar y Organizar									
APO01	Gestionar el marco de gestión de TI.								
APO02	Gestionar la estrategia.								
APO03	Gestionar la arquitectura empresarial.								
APO04	Gestionar la innovación.								

Decidir y registrar qué procesos deben ser evaluados

Anote el nivel de capacidad de proceso de destino

Figura C. 7 Tabla resumen de la evaluación

En esta etapa, se establece el nivel de capacidad requerida del proceso. Al establecer los niveles de capacidad destino, se debe considerar cuál es el impacto en los objetivos de negocio de la empresa si no se alcanza un nivel determinado de capacidad. La primera consideración es el impacto en la empresa si el proceso no existe o no funciona con eficacia o eficiencia. La segunda consideración se refiere a las consecuencias adicionales de la operación eficaz y eficiente de los procesos en los distintos niveles de capacidad, como se muestra en la figura C.8 de la norma ISO / IEC 15.504-4.

Escala	Atributos de proceso donde ocurren brechas	Consecuencias potenciales
Nivel 1	PA 1.1. Rendimiento del proceso	– Proceso no logra resultados
Nivel 2	PA 2.1. Rendimiento de la gestión	– Costo o tiempo excesivos; uso ineficiente de los recursos; responsabilidades poco claras – Decisiones no controladas; incertidumbre sobre si se cumplirán los objetivos de tiempo y de costos
	PA 2.2. Producto del trabajo de la gestión	– La calidad e integridad del producto es impredecible; versiones no controladas; aumento de los costos de apoyo; problemas de integración; aumento de los costos por retrabajo
Nivel 3	PA 3.1. Definición del proceso	– Las mejores prácticas y lecciones aprendidas de proyectos anteriores no se definen, publican, ni están disponibles dentro de la organización – No hay base para la mejora de procesos de toda la organización
	PA 3.2. Despliegue del proceso	– El proceso de implementación no incorpora las mejores prácticas y lecciones identificadas en proyectos anteriores; – El rendimiento de los procesos en toda la organización es inconsistente – Pérdida de oportunidades para entender el proceso e identificar mejoras
Nivel 4	PA 4.1. Medida del proceso	– No se tiene la comprensión cuantitativa del rendimiento del proceso ni de los objetivos del negocio definidos que se están logrando – No hay capacidad cuantitativa para detectar problemas de rendimiento temprano
	PA 4.2. Control del proceso	– El proceso no logra la capacidad y/o estabilidad (predecible) dentro de límites definidos – Los objetivos de desempeño cuantitativos y objetivos de negocio definidos no se cumplen
Nivel 5	PA 5.1. Innovación del proceso	– Los objetivos de mejora de procesos no están claramente definidos – Las oportunidades de mejora no están claramente identificados
	PA 5.2. Optimización del proceso	– Incapacidad para cambiar el proceso con eficacia con la finalidad de alcanzar los objetivos de mejora de procesos – Incapacidad para evaluar la eficacia de los cambios de procesos

Figura C. 8 Consecuencias adicionales del funcionamiento eficaz y eficiente de los procesos

C.3.2. Paso 2. Determinar si el proceso seleccionado está en el Nivel 1 de Capacidad

El primer paso en la evaluación de cada proceso es determinar si en realidad se está realizando un proceso y está logrando sus resultados. Los indicadores del nivel de capacidad 1 son específicos para cada proceso. Para evaluar si el proceso implementado logra su propósito se evalúa si el siguiente atributo se ha logrado.

Proceso	EDM 01: Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno							
Nivel	**Evaluar si los resultados se logran.**	**Criterio**	**El criterio, se cumple? (Y/N)**	**Comentario**	**No logrado (0 – 15%)**	**Logrado parcialmente (>15-50%)**	**Logrado en gran parte (>50-85%)**	**Logrado totalmente (>85-100%)**
Nivel 0 Incompleto	El proceso no se ha implementado, o falla para lograr su propósito.							
Nivel 1 Realizado	PA 1.1 El proceso implementado logra su propósito	Se están logrando los siguientes resultados del proceso. – EDM01-O1 Se consigue un modelo de toma de decisiones estratégicas óptima para TI, alineados con los requisitos del entorno y de los grupos de interés internos y externos de la empresa. – EDM01-O2 El sistema de gobernanza de TI está integrado en la empresa. – EDM01-O2 El aseguramiento está logrando que el sistema de gobernanza de TI esté funcionando con eficacia.						
Nivel 2 Administrado	PA 2.1 Rendimiento de la gestión. Medida del grado en que se gestiona el rendimiento del proceso.	Como resultado de la plena consecución de este atributo: a. Los objetivos para el desempeño del proceso están identificados. b. Se organizó y se controló el rendimiento del proceso. c. El rendimiento del proceso están ajustados para satisfacer los planes. d. Las responsabilidades y autoridad para la realización del proceso están definidos, asignados y comunicados. e. Los recursos y la información necesarios para realizar el proceso están identificados, disponibles, asignados y utilizados. f. Las interfaces entre las partes involucradas se las arreglaron para garantizar tanto la comunicación efectiva y clara asignación de responsabilidades.						

Figura C. 9 Plantilla ejemplo de evaluación

Al llevar a cabo una evaluación de nivel de capacidad 1 para cualquier proceso, el grado en que se están logrando los resultados para el proceso tiene que ser decidido, como se muestra en la figura C.4.

En el caso de EDM01 en la figura C.11, si se están logrando los tres resultados, puede ser una clasificación F para "plenamente logrado"; si se logran sólo dos resultados, puede ser clasificado de L 'logrado en gran medida'; si se logra sólo un resultado, puede ser clasificado P para 'logrado parcialmente ", y si no se logra, puede ser clasificado N para" no logrado ". En algunos casos, algunos de los resultados se están cumpliendo, en cuyo caso se calificará L (en gran medida) o P (parcialmente) logrado; Se requiere juicio.

C.3.3. Paso 3. Determinar cuáles de los niveles de capacidad del 2 a 5 para los procesos seleccionados se están cumpliendo

Para el nivel 2, los criterios de evaluación son genéricos, es decir, los criterios son los mismos para todos y cada proceso.

Proceso							
Nivel	**Evaluar si los resultados se logran.**	**Criterio**	**Comentario**	**No logrado (0 – 15%)**	**Logrado parcialmente (>15-50%)**	**Logrado en gran parte (>50-85%)**	**Logrado totalmente (>85-100%)**
Nivel 2 Administrado	PA 2.1 Rendimiento de la gestión. Medida del grado en que se gestiona el rendimiento del proceso.	Como resultado de la plena consecución de este atributo: g. Los objetivos para el desempeño del proceso están identificados. h. Se organizó y se controló el rendimiento del proceso. i. El rendimiento del proceso están ajustados para satisfacer los planes. j. Las responsabilidades y autoridad para la realización del proceso están definidos, asignados y comunicados. k. Los recursos y la información necesarios para realizar el proceso están identificados, disponibles, asignados y utilizados. l. Las interfaces entre las partes involucradas se las arreglaron para garantizar tanto la comunicación efectiva y clara asignación de responsabilidades.					
Nivel 2 Administrado	PA 2.2 Trabajo gestionado. Se realiza medición sobre el grado en el que el resultado del trabajo del proceso se gestionan adecuadamente.	Los productos de trabajo (salidas del proceso) se definen y controlan: a) Los requisitos para los productos de trabajo del proceso se definen. b) Se definen los requisitos para la documentación y el control de los productos de trabajo. c) Los productos de trabajo están debidamente identificados, documentados y controlados. d) Los productos de trabajo se revisan de acuerdo con las disposiciones planificadas y se ajusta, si es necesario, para cumplir con los requisitos.					

Hacer un juicio sobre el número de criterios se han cumplido como base para la calificación

Figura C. 10 Evaluación detallada del Nivel 2 (administrado) – Parte 2

En cada caso, el juicio para la evaluación debe tener en cuanto si se han cumplido los criterios y, la decisión se debe traducir en una clasificación (según la figura C.4). Luego se registra en la plantilla para el proceso. Esto debe repetirse para cada capacidad.

C.3.4. Paso 4. Resumen de los resultados de la evaluación de los niveles de capacidad

El resumen de los resultados de la evaluación se debe registrar en la figura C.11. El nivel de capacidad se logra cuando ambos indicadores de capacidad del nivel son o bien "en gran medida" o "plenamente logrado". En la figura C.10, el nivel de capacidad del proceso es el nivel 2. Esto se debe registrar en la tabla de resultados de la evaluación del proceso, como se muestra en la figura C.11.

Nombre del proceso	**Nivel 0**	**Nivel 1**	**Nivel 2**		**Nivel 3**		**Nivel 4**		**Nivel 5**	
EDM01		**PA 1.1**	**PA 2.1**	**PA 2.2**	**PA 3.1**	**PA 3.2**	**PA 4.1**	**PA 4.2**	**PA 5.1**	**PA 5.2**
Clasificación por criterios		**F**	**F**	**L**	**P**	**N**				
Nivel de capacidad alcanzado				**2**						
Leyenda: **N** (No logrado, 0-15%), **P** (Parcialmente logrado,> 15% -50%), **L** (En gran parte conseguido, 50% -85%), **F** (Totalmente Conseguido,> 85 a 100%)										

Figura C. 11 Evaluación detallada – Sección 1

Nombre del proceso	**Para ser evaluado**	**Nivel objetivo**	**Nivel de capacidad del proceso**					
			0	**1**	**2**	**3**	**4**	**5**
Evaluar, Dirigir y Monitorear								
EDM01 Asegurar un marco de gobernabilidad establecimiento y mantenimiento								
EDM02 Asegurar la entrega beneficios								
EDM03 Asegurar la optimización de los riesgos								
EDM04 Asegurar la optimización de recursos								
EDM05 Asegurar la transparencia para los stakeholder								

Registro del nivel de capacidad alcanzado

Figura C. 12 Tabla resumen de la evaluación

C.3.5. Paso 5 Desarrollar un Plan de Mejora de Acción

Sobre la base de la autoevaluación, se debe considerar un plan de acción para la mejora de los procesos. Una opción sería centrarse en mejorar las áreas donde existen brechas entre los niveles de capacidad "actuales" y el "objetivo" de un proceso.

Una segunda opción sería la de llevar a cabo una evaluación independiente más formal, basado en el COBIT PAM. Esto proporcionará una evaluación más fiable y más orientada a identificar las áreas que requieren mejoras.

APÉNDICE D. CUADRO DE OPERACIONALIZACION DE VARIABLES SEGÚN LA RELACION OSSIM-COBIT

PROCESO COBIT 5	INDICADORES	FUNCIONES DE SEGURIDAD (OSSIM)	HERRAMIENTAS INTEGRADAS
Gestión de la disponibilidad y capacidad	- Número de picos de transacciones donde se excede la meta de rendimiento - Número de incidentes de disponibilidad - Número de eventos donde la capacidad ha excedido los límites planificados.	Monitoreo de comportamiento	**NAGIOS** Repositorio de plugins desarrollados para supervisar la infraestructura de TI referente a sitios web, formularios y transacciones permitiendo la verificación del logueo de usuarios, acceso y disponibilidad. Muestra el estado de disponibilidad de los dispositivos de red (up-down-unknown) Comprueba el estado de los servicios. Detecta cambios en el estado (normal-warning-unknown-critical) y permite la configuración de alertas mediante límites especificados.
Gestión de los activos	- Numero de activos no utilizados - Número de activos obsoletos	Descubrimiento de activos	**NMAP y PRADS** Permite el escaneo automático de la red, mostrando activos conectados y especificando características relevantes de los mismos. Puede trabajar en asociación con **NAGIOS** mediante el monitoreo de disponibilidad a fin de realizar filtros según el estado de los activos. Las herramientas interactúan de tal forma que es posible identificar tecnología obsoleta referente a software y hardware de los activos (SO, drivers, memoria RAM, disco duro, etc.).

Gestión de la configuración	- Numero de desviaciones entre el repositorio de configuración y la configuración real	Descubrimiento de activos Detección de intrusiones	**PRADS** Muestra los activos que han sufrido cambios en sus configuraciones, como: actualizaciones, sistema operativo, servicios, asignación de direcciones IP, etc. Esta herramienta sustituye a otras como: P0F, PADS y ARPAWATCH de versiones anteriores de OSSIM que cumplían funciones similares, pero de forma independiente. **Monitoreo de integridad de archivos (FIM)** Permite registrar los cambios en los archivos críticos de sistema (ejecutables del sistema y de las aplicaciones), archivos de configuración y archivos de contenido.
Gestión de las peticiones y los incidentes de servicio	- Número y porcentaje de incidentes que causan interrupción en los procesos críticos de negocio - Porcentaje de incidentes resueltos dentro de un periodo acordado/aceptable - Nivel de satisfacción del usuario con la resolución de las peticiones de servicio	Descubrimiento de activos Monitoreo de comportamiento Evaluación de vulnerabilidades SIEM: Respuesta Incidentes (Tickets) SIEM: Tickets	**NMAP, OPENVAS Y NAGIOS** Los activos detectados pueden agruparse en una red dedicada y mostrar información detallada referente a: número de activos, número de eventos, número de vulnerabilidades, porcentaje de disponibilidad y número de servicios propios de una red. **TICKETS** Permite la gestión de incidentes a través de la presentación de estados y muestra información detallada mediante Dashboards (cuadros de mando) sobre el tiempo de resolución de incidencias. Muestra información de tickets de incidencias generados por usuarios, así como su estado actual priorizándolos y dándoles seguimientos de acuerdo a las políticas establecidas por la organización. La solución efectiva conlleva a la satisfacción de los usuarios finales.

Gestión de servicios de seguridad	- Número de vulnerabilidades descubiertas - Número de rupturas de cortafuegos - Número de incidentes que impliquen dispositivos de usuario final - Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno	Evaluación de vulnerabilidades Detección de intrusiones SIEM: Integración con otros dispositivos Descubrimiento de activos Descubrimiento de activos	**OPENVAS** Permite la evaluación de vulnerabilidades. De acuerdo a la tarea de análisis configurada y establecida por las políticas de la organización, se obtendrá información detallada de los incidentes en la red. Estos últimos, almacenados en una base de datos que puede ser consulta en cualquier momento. La configuración de análisis permite también, la generación automática de tickets de eventos que serán enviados de forma inmediata al administrador con el fin de solucionarlos. **NIDS** Capturan las amenazas dirigidas a sistemas vulnerables, identifican ataques, infecciones de malware, así como también violaciones de políticas de seguridad. **PLUGINS DE ACCESO** OSSIM cuenta con plugins de integración para Firewalls de diferentes marcas, mostrando información de los eventos de denegación de acceso. **NMAP** Mediante el inventario de activos actualizado, es posible filtrar activos por eventos, vulnerabilidades y alarmas. **PRADS** Muestra información de los activos que se han agregado a la red en un determinado periodo de tiempo.

	- Promedio de tiempo entre los cambios y las actualizaciones de cuentas - Número de cuentas - Número de incidentes relacionados con seguridad física - Número de incidentes relacionados con accesos no autorizados a la información	**SIEM: Cumplimiento normativo ISO 27001** **SIEM: Cumplimiento normativo ISO 27001** SIEM: Integración de otros dispositivos Detección de intrusiones	**ADMINISTRADOR DE CUENTAS** Detalla el número de **cuentas locales,** así como las cuentas creadas mediante **LDAP** con Active Directory. **ZONEMINDER** OSSIM puede integrarse con cámaras de vigilancia IP a través de este software para recopilar información de los eventos ocurridos en el entorno. **OSSEC y FIM** Analizan el comportamiento del sistema y el estado de configuración para controlar el acceso de usuarios y actividad.
Gestión de Operaciones	- Número de incidentes causados por problemas operativos - Tasa de eventos comparada con el número de incidentes - Porcentaje de tipos de eventos	Monitoreo del comportamiento	**NAGIOS** Supervisa el correcto funcionamiento de los servicios y permite realizar una programación automática para revisión de servicios, así como para la configuración del tiempo de inactividad. Genera notificaciones de alerta cuando algún host o servicio no esté funcionando. Proporciona información detallada de eventos a través de histogramas e historiales de acuerdo a estados.

	críticos cubiertos por sistemas de detección automática		Mantiene actualizada la información de monitorización de agentes configurados (host y servicios) dentro de la red.