Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS PARA OBTENER EL TÍTULO PROFESIONAL
DE INGENIERA DE SISTEMAS

TITULO

Gestión de la Seguridad de la Información de la Infraestructura de Red Datos de la Minera Shahuindo Mediante Ossim y Cobit

PRESENTADO POR

Tahnee Lilibeth Luján Flores

Verónica Elizabeth Huancas Samillán

ASESOR

Dr. Ing. Ernesto Karlo Celi Arévalo

SUSTENTADO

Viernes 29 de Diciembre del 2023

Lambayeque – Perú

2023

Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS PARA OBTENER EL TÍTULO PROFESIONAL
DE INGENIERA DE SISTEMAS

TITULO

Gestión de la Seguridad de la Información de la Infraestructura de Red Datos de la Minera Shahuindo Mediante Ossim y Cobit

APROBADO POR

Msc. Ing. Robert Edgar Puican Gutierrez	**Presidente**
Msc. Ing. Gilberto Martín Ampuero Pasco	**Secretario**
Msc. Ing. Roberto Carlos Arteaga Lora	**Vocal**
Dr. Ing. Ernesto Karlo Celi Arévalo	**Asesor**

Lambayeque – Perú
2023

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL DE SISTEMAS Y DE ARQUITECTURA
DECANATO

ACTA DE SUSTENTACIÓN
N° 559-2023-FICSA-D

Siendo las 10:30 am del día 29 de diciembre del 2023, se reunieron los miembros de jurado de la Tesis titulada: **"GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA INFRAESTRUCTURA DE RED DATOS DE LA MINERA SHAHUINDO MEDIANTE OSSIM Y COBIT" con código de proyecto N° IS-218-055**, autorizado por Resolución No 285-2023-CU,y designado por Decreto Directoral N° 013-2019-UNPRG-FICSA-UI y Decreto Directoral N° 293-2018-UNPRG-FICSA-UI; con la finalidad de Evaluar y Calificar la sustentación de la tesis profesional antes mencionada, conformado por los siguientes docentes:

MSC. ING. ROBERT EDGAR PUICAN GUTIERREZ — PRESIDENTE
MSC. ING. GILBERTO MARTÍN AMPUERO PASCO — SECRETARIO
MSC. ING. ROBERTO CARLOS ARTEAGA LORA — VOCAL
Asesorado por DR. ING. ERNESTO KARLO CELI ARÉVALO

El acto de sustentación fue autorizado por **OFICIO VIRTUAL N° 200-2023-UIFICSA**, la Tesis fue presentada y sustentada por las Bachilleres: **TAHNEE LILIBETH LUJÁN FLORES Y VERÓNICA ELIZABETH HUANCAS SAMILLÁN**, tuvo una duración de 60 minutos Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado; se procedió a la calificación respectiva:

	NUMERO	LETRAS	CALIFICATIVO
TAHNEE LILIBETH LUJÁN FLORES	18	DIECIOCHO	MUY BUENO
VERÓNICA ELIZABETH HUANCAS SAMILLÁN	18	DIECIOCHO	MUY BUENO

Por lo que quedan **APTOS** para obtener el Título Profesional de **INGENIERO (A) DE SISTEMAS** de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ingeniería Civil De Sistemas y de Arquitectura de la Universidad Nacional Pedro Ruiz Gallo.

Siendo las 11.30 ; del mismo día, se dio por concluido el presente acto académico, dándose conformidad al presente acto, con la firma de los miembros del jurado.

MSC. ING. ROBERT EDGAR PUICAN GUTIERREZ
PRESIDENTE

MSC. ING. GILBERTO MARTÍN AMPUERO PASCO
SECRETARIO

MSC. ING. ROBERTO CARLOS ARTEAGA LORA
VOCAL

DR. ING. ERNESTO KARLO CELI ARÉVALO
ASESOR

DR. ING. SERGIO BRAVO IDROGO
DECANO

SBI/

INFORMACIÓN GENERAL

Titulo

Gestión de la seguridad de la información de la infraestructura de red datos de la Minera Shahuindo mediante OSSIM y COBIT

Autoras

Apellidos y Nombres:

Luján Flores Tahnee Lilibeth

tahneelu15@gmail.com

Huancas Samillán Verónica Elizabeth

vero_150_1@hotmail.com

Asesor de especialidad y metodológico

Dr. Ing. Ernesto Karlo Celi Arévalo

eceli@unprg.edu.pe

Institución donde se realizó la investigación

Minera Shahuindo, Lima, Perú

Fecha de presentación

Abril del 2021

Firma de los responsables

Tahnee Lilibeth Luján Flores

Verónica Elizabeth Huancas Samillán

Ernesto Karlo Celi Arévalo

DEDICATORIA

Esta tesis la dedico a mis padres Segundo y Ricardina quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades porque Dios está conmigo siempre.

A mis hermanos(as) por su apoyo incondicional, durante todo este proceso, porque con sus consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

Tahnee Lilibeth Luján Flores

La presente tesis se la dedico a mis padres, Pablo Huancas y Rosa Samillán, quienes a pesar de las adversidades, siempre buscaron la forma de apoyarme para salir adelante y convertirme en un profesional de éxito.

A mi hijo, Ian Mathias, quien a pesar de su corta edad, entiende, valora y admira el esfuerzo y dedicación de mamá para dar un paso más en su vida profesional.

A mi familia en general, que confían en mí y alientan a seguir creciendo personal y profesionalmente.

Verónica Elizabeth Huancas Samillán

AGRADECIMIENTO

Agradezco a Dios por protegerme durante todo mi camino y darme fuerzas para superar obstáculos y dificultades a lo largo de toda mi vida.
A mi familia quienes son mi motor y mi mayor inspiración que a través de su amor, paciencia, buenos valores, ayudan a trazar mi camino.
Agradezco a nuestros docentes de la Escuela de Ingeniería de Sistemas, por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión, de manera especial, al Dr. Ing. Ernesto Karlo Celi Arévalo asesor de nuestro proyecto de investigación quien ha guiado con su paciencia, y su rectitud como docente.
Y finalmente a la Universidad Nacional Pedro Ruíz Gallo por ser la sede de todo el conocimiento adquirido en estos años.

Tahnee Lilibeth Luján Flores

En primer lugar, quiero agradecer a nuestro padre todo poderoso, Dios, y a la Virgencita de Guadalupe, que me ayudaron a no doblegar mi esfuerzo a pesar de las adversidades.
A mi familia quienes estuvieron en todo momento apoyándome e incentivándome para cumplir una más de mis metas, obtener el título profesional.
Al Dr. Ing. Ernesto Karlo Celi Arévalo, asesor de nuestro proyecto de investigación, quien con su paciencia y dedicación, nos apoyó a culminar nuestro proyecto con éxito.
Finalmente, a nuestra casa de estudios, la Universidad Nacional Pedro Ruíz Gallo, por ser la forjadora de muchos profesionales de renombre en toda la región Lambayeque.

Verónica Huancas Samillán

RESUMEN

Uno de los problemas que hoy en día tienen las empresas que soportan sus procesos sobre tecnologías de la información y las comunicaciones es la gestión que realizan sobre ellas, para evitar eventos que ocasionen impactos negativos sobre sus actividades. La seguridad de la información y la continuidad de los procesos debe asegurarse a través de la gestión preventiva y proactiva de su infraestructura tecnológica.

Esta investigación plantea una solución para gestionar de manera más adecuada la seguridad en la red de datos de la empresa Minera Shahuindo aplicando las buenas prácticas recomendadas por los marcos de referencia OSSIM y COBIT.

Para el desarrollo de la propuesta se utilizó métodos descriptivos que identifican los componentes de la solución, su funcionalidad y el tratamiento de la información a través de las implementaciones realizadas.

Finalmente, la solución fue validada 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 clave: activo de TI, escenario de riesgo, política de seguridad, COBIT, SIEM.

ABTRACT

One of the problems that companies that support their processes on information and communication technologies have today is the management that they carry out on them, to avoid events that cause negative impacts on their activities. The security of information and the continuity of processes must be ensured through the preventive and proactive management of its technological infrastructure.

This research proposes a solution to more adequately manage the security in the data network of the company Minera Shahuindo applying the best practices recommended by the OSSIM and COBIT reference frameworks.

For the development of the proposal, descriptive methods were used that identify the components of the solution, its functionality and the treatment of the information through the implemented implementations.

Finally, the solution was validated using the ISO / IEC 15504 standard, which allows for the reliable, consistent and repeatable evaluation of a process in the field of evidence-based IT company management.

Key words: IT asset, risk scenario, security policy, COBIT, SIEM.

INDICE DE CONTENIDOS

INTRODUCCION

La presente investigación, comienza a desarrollarse a partir de la descripción de la realidad problemática Minera Shahuindo 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 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 exponen 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. 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.

I. EL PROBLEMA DE LA INVESTIGACION

1.1. Descripción de la realidad problemática

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.

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 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.

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

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 (Madrid Molina, y otros, 2008):

- 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

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

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

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.

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).

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.

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.

Influencia de COBIT 5.0 en la seguridad de la Información

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.

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.

La Minera Shahuindo es un proveedor líder de servicios integrales de minería y construcción en Latinoamérica, con quince años de experiencia ofreciendo servicios integrales de clase mundial en minería y construcción, en operaciones

mineras a tajo abierto y subterráneo. Sus servicios cubren todas las etapas de un proyecto minero, desde la planificación, desarrollo, construcción, operación, hasta el cierre de la mina. Con numerosos proyectos exitosamente desarrollados en la región.

La Minera Shahuindo cuenta con un órgano administrativo de soporte a todas las operaciones de la empresa, encargado del procesamiento y tratamiento de información, por lo tanto, su disponibilidad y continuidad es un factor crítico de éxito para la empresa. Esta es la Gerencia de TI, que dentro de su jefatura tiene a cargo la administración de la red de datos y comunicaciones, la cual se divide en:

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

Dentro sus principales servicios figuran:

- Servidor Web
- Servidor de Correo
- Servidor FTP
- Servidor de archivos
- Telefonía IP
- Acceso a Internet, etc.
- Gestión de aplicaciones y sistemas informáticos

Como se puede notar, la diversidad de servicios brindados sumado con el crecimiento continuo de la infraestructura tecnológica en la empresa 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.

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

1.2. Formulación de la pregunta de investigación

¿Cuál será el impacto del uso de una plataforma OSSIM bajo un entorno de objetivos de control según el enfoque de COBIT en la Gestión de la seguridad de la información de la infraestructura de red datos de la Minera Shahuindo?

1.3. Objetivo general

Evaluar el impacto que produce una plataforma OSSIM bajo un entorno de objetivos de control según el enfoque de COBIT sobre la Gestión de la seguridad de la información de la infraestructura de red datos de la Minera Shahuindo.

1.4. Objetivos específicos

a. Realizar un diagnóstico de la situación actual de la gestión de la seguridad de la información tomando como referencia los objetivos de control de la ISO/IEC 27002, con la finalidad de determinar el nivel de madurez de los controles.
b. Definir el tramo de red que cumpla con los requerimientos de hardware y software apropiados, según las especificaciones técnicas de OSSIM, para la correcta implementación de la primera prueba piloto.
c. Identificar las métricas que serán evaluadas con OSSIM a través del proceso de alineamiento de cascada propuesto por COBIT 5.0.
d. Implementar la plataforma OSSIM en un entorno de prueba para identificar, clasificar y evaluar los eventos de seguridad de las métricas seleccionadas.
e. Determinar el nivel de cumplimiento de las actividades en cada proceso de TI evaluado, para establecer el nivel de madurez de cada proceso en relación a la seguridad requerida.

1.5. Justificación e importancia

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

a. 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 minera, logrando centralizarla y convertirla en un conjunto de acciones que se tomarán de acuerdo a las políticas y objetivos perseguidos.

b. 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.

c. 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.

d. 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.

1.6. Alcances y limitaciones

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

a. Debido a la complejidad de la infraestructura de la red de datos de la Minera Shahuindo, 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.

b. 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 minera, razón por la cual nos basaremos en la información proporcionada por el administrador de la red.

c. 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 15504.

II. MARCO TEÓRICO

2.1. Fundamento teórico

2.1.1. La seguridad de la información

"La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada" (NTP ISO/IEC 27002:2013, 2013).

Por su parte, los autores Andreu, Ricart, & Valor (1998) explican como la información se convierte en un recurso estratégico para las empresas y se integra dentro de su proceso de planificación estratégica.

Así entonces, "la información se ha convertido en un recurso clave para las empresas a todos los niveles jerárquicos y para todos los departamentos ya que las organizaciones deben conseguir, procesar, usar y comunicar información, tanto interna como externa, en sus procesos de planificación, dirección y toma de decisiones" (Carrasco, 2010).

Por lo tanto este recurso el cual puede adoptar diferente formas ya sea impresa o escrita en papel, trasmitida por algún medio electrónico, mostrada en video o simplemente hablada en conversación sigue siendo importante para una empresa ya que para la labor de un directorio o algún otro responsable la información tiene la función clave de minimizar la incertidumbre en la toma de decisiones así que esta debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

Sabiendo que la información de toda empresa es un activo importante, y que se encuentra expuesta a un gran número de amenazas internas como externas, cuyo origen puede ser natural o consecuencia del hombre, ya sea de forma deliberada o accidental, es necesario que se establezcan medidas para evitar la pérdida o modificación de los datos, información o software inclusive, por personas no autorizadas asegurando apropiadamente su resguardo.

> *"La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios.*

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad de la organización.

La seguridad de información es importante en negocios tanto del sector público como del privado y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de información permitirá, por ejemplo, lograr el gobierno electrónico o el comercio electrónico, evitando y reduciendo los riesgos relevantes" (NTP ISO/IEC 27002:2013, 2013).

Así mismo la NTP ISO/IEC 27001:2014 (2014) define seguridad de la Información como: "La preservación de la confidencialidad, integridad y disponibilidad de la información; así como de los sistemas implicados en su tratamiento, dentro de una organización. Además, también pueden estar involucradas otras propiedades como son: la autenticidad, la responsabilidad, el no-repudio y la confiabilidad".

También es muy importante tener en claro que la seguridad de tecnologías de información y la seguridad de información son conceptos diferentes: la seguridad de TI se encarga en particular, de la protección tecnológica y es gestionada desde un nivel operativo por las áreas de sistemas de las organizaciones.

"La seguridad de información va más allá ocupándose de riesgos, beneficios, buen uso, procesos y actividades involucradas con la información y los activos relacionados a ella, impulsados por la Alta Dirección empresarial" (Tupia, 2011).

2.1.2. Activo de información

"Los activos son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Estos son necesarios para que la organización funcione y alcance los objetivos que propone su dirección" (Espinoza, 2013).

Según el contexto de la NTP ISO/IEC 27002:2013 (2013), un “activo de información es algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger”.

La NTP ISO/IEC 27002:2013 (2013) clasifica el activo en dos tipos:

a. “Los activos primarios: Son usualmente los procesos e información centrales de la actividad en cuestión. Otros activos primarios como los procesos de la organización también pueden considerarse, lo cual será más apropiado para diseñar una política de seguridad de la información o un plan de continuidad del negocio.
   - Procesos y actividades de negocio
   - Información

b. Los activos de apoyo: Estos activos tienen vulnerabilidades que son explotables por amenazas que tienen como objetivo desactivar los activos primarios del alcance (proceso e información). Son de varios tipos:
   - Hardware
   - Software
   - Red
   - Personal
   - Sitio
   - Estructura de la Organización

2.1.3. Principios de la seguridad de la Información

“Los diferentes ataques a los activos informáticos pueden provocar la pérdida de la disponibilidad, confidencialidad o integridad de la información; lo cual generalmente implica graves consecuencias para las empresas y en muchas ocasiones se provocan daños irreparables” (Montesinos, Baluja, & Porven, 2013).

Estos últimos tres términos constituyen la base de la seguridad de la información, de donde se resume la explicación que se da a continuación, de acuerdo a lo explicado por (Condori, 2014).

a. ***“Confidencialidad***

   Este principio tiene como propósito asegurar que sólo la persona o personas autorizadas tengan acceso a cierta información. La

información, dentro y fuera de una organización, no siempre puede ser conocida por cualquier individuo, si no por el contrario, está destinada para cierto grupo de personas, y en muchas ocasiones, a una sola persona. Esto significa que se debe asegurar que las personas no autorizadas, no tengan acceso a la información restringida para ellos. La confidencialidad de la información debe prevalecer y permanecer, por espacios de tiempo determinados, tanto en su lugar de almacenamiento, como durante su procesamiento y tránsito, hasta llegar a su destino final.

b. Integridad

Este principio permite garantizar que la información no sea modificada o alterada en su contenido por personas no autorizados o de forma indebida. Asimismo, la integridad se aplica a los sistemas, teniendo como propósito garantizar la exactitud y confiabilidad de los mismos.

c. Disponibilidad

Este principio tiene como propósito, asegurar que la información y los sistemas que la soportan, estén disponibles en el momento en que se necesiten, para los usuarios autorizados a utilizarlos. Adicionalmente, la disponibilidad hace referencia a la capacidad que deben tener los sistemas de recuperarse ante interrupciones del servicio, de una manera segura que garantice el continuo desarrollo de la productividad de la organización sin mayores inconvenientes."

2.1.4. Políticas de seguridad de la información

"Una política de seguridad de la información es aquella que fija los lineamientos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen" (Hernández, 2016).

"Tiene como objetivo de dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones. La gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización" (NTP ISO/IEC 27002:2013, 2013).

Peltier, Peltier y Blackley (2015), consideran a las políticas de seguridad de información como “la piedra angular de una efectiva arquitectura de seguridad de la información, ya que de ella nacen otros documentos importantes tales como directivas, estándares, procedimientos y guías y nos menciona que estas cumplen con 2 roles importantes, un rol interno y otro externo”.

a. Rol Interno: Ya que se menciona a cada uno de los miembros de la organización que se espera que realicen y como se evaluará el trabajo realizado.

b. Rol Externo: Ya que sirve para mostrarle al mundo como es que se trabaja dentro de la organización, que somos conscientes de la necesidad de proteger nuestra información y la de los clientes y que estamos trabajando para realizarlo.

Según Hernández (2016) “una buena política de seguridad corporativa debe recoger, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos, es decir que estás políticas de seguridad deben abarcar las siguientes áreas.

- Seguridad física
- Seguridad lógica
- Seguridad en redes
- Seguridad en los recursos humanos
- Seguridad en el outsourcing
- Planes de contingencia”

2.1.5. Sistema de gestión de seguridad de la información

Los diferentes y constantes usos de las tecnologías de información en los negocios hacen que cada vez sea más fácil la expansión de éstos. Sin embargo, la cercanía y facilidad de éstos ha generado ciertos problemas a las organizaciones, que día tras día son más vulnerables a las amenazas que se presentan en el medio, las cuales pueden llegar a convertirse en un verdadero riesgo para la organización afectando el correcto funcionamiento de las actividades del negocio.

“Para contrarrestar dichas amenazas, las organizaciones deben generar un plan de acción frente a éstas. Este plan de acción es conocido como Sistema de

Gestión de Seguridad de la Información (SGSI) y contiene los lineamientos que deben seguirse en la organización, los responsables y la documentación necesaria para garantizar que el SGSI sea aplicado y genere una retroalimentación. La definición de SGSI se hace de manera formal en la norma ISO 27001, donde están los estándares y mejores prácticas de seguridad de la información" (Ladino, Villa, & López, 2014).

"El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas" (ISO/IEC 27001:2014, 2014).

"La implementación de un Sistema de Gestión de Seguridad de la Información permite establecer un proceso de mejora continua a través del seguimiento de un modelo PHVA (Planear, Hacer, Verificar, Actuar), para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información, con unas responsabilidades claras y el compromiso manifiesto por parte de directivas" (Caviedes Sanabria & Prado Urrego, 2012).

2.1.6. Incidentes de seguridad de la información

La identificación de un incidente de seguridad 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 (Villena, 2016).

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.

Villena (2016) argumenta lo siguiente:

> *"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.*
>
> *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."*

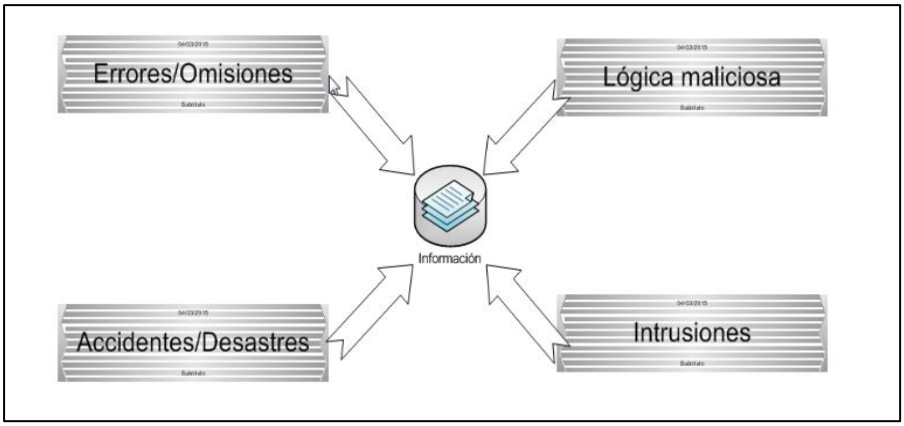


Figura N° 1. Tipos de amenazas
Fuente: (Villena, 2016).

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: (Balarezo & Poveda, 2015).

2.1.7. 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. Balarezo y Poveda (2015) mencionan a:

a. **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.

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

c. **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.

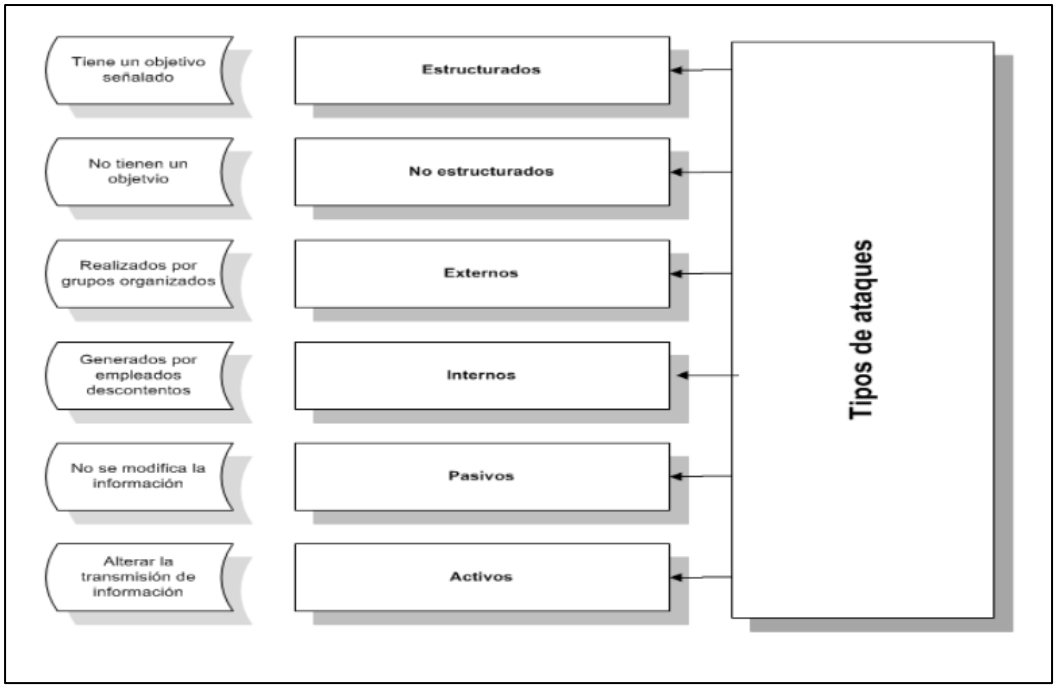


Figura N° 2. Tipos de ataques a la seguridad de la información
Fuente: (Balarezo & Poveda, 2015).

Según Villena (2016), 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.).

2.1.8. Mecanismos de protección

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.

De acuerdo a Canaluisa, Meza y Tasipanta (2012), 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".

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, 2014).

2.1.9. 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" (Sánchez & Piattini, 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).

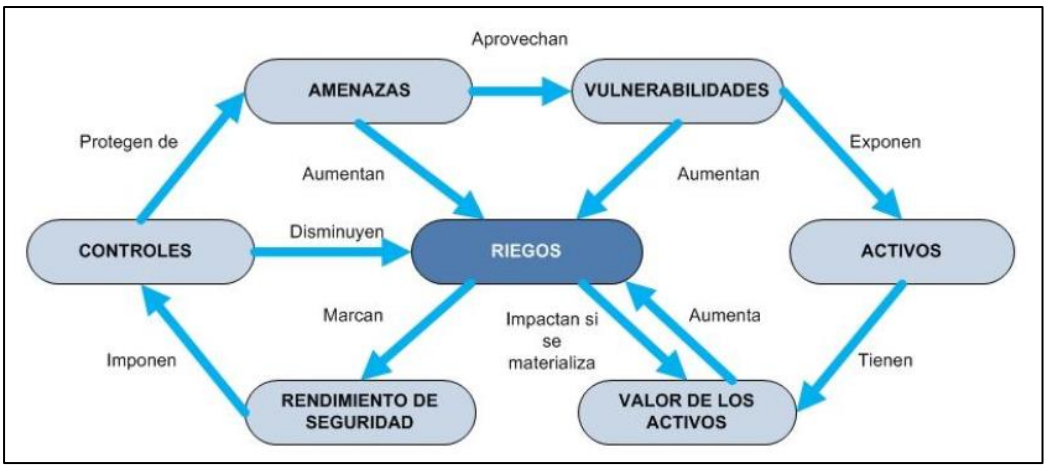


Figura N° 3. Sistema de gestión de seguridad de la información
Fuente: (Canaluisa, Meza, & Tasipanta, 2012)

"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" (Canaluisa, Meza, & Tasipanta, 2012).

2.1.10. Gestión de eventos en una infraestructura de red

"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).

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).*

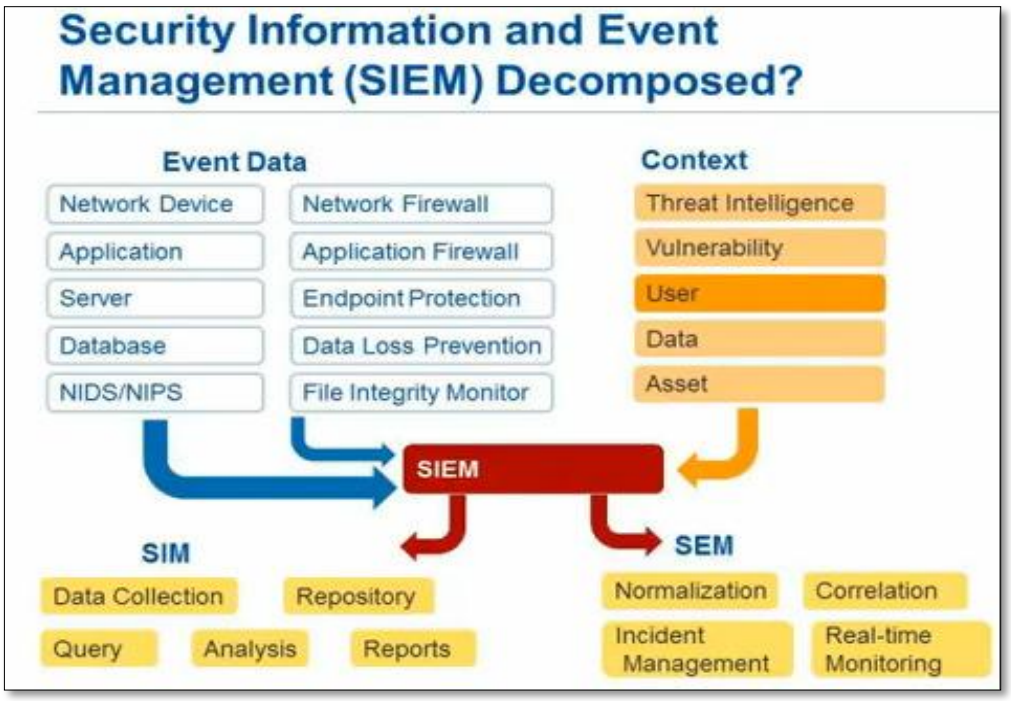


Figura N° 4. Fusión de SIM y SEM
Fuente: (Chikonga, 2014)

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

2.1.11. 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.

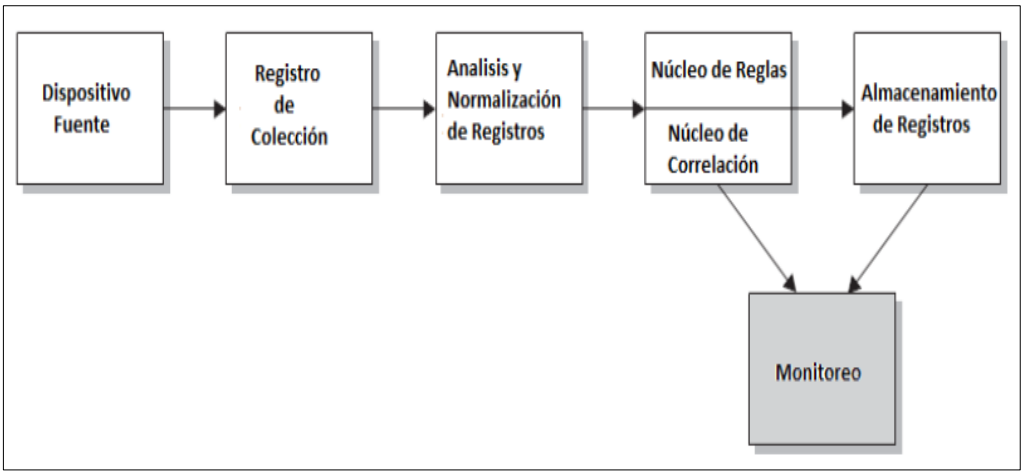


Figura N° 5. Arquitectura básica de un sistema SIEM
Fuente: (Baluja, Caro, & Cancio, 2012)

Baluja, Caro y Cancio (2012) describen las partes o módulos que aparecen en la figura anterior de la siguiente manera:

a. ***"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.*

b. ***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.

c. ***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.

d. ***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.*

e. ***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).*

f. ***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 Sánchez y Piattini (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.

2.1.12. Evaluación de SIEM

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).

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

Sin embargo, implementar una solución SIEM tiene un costo elevado que incluye: costos iniciales de licenciamiento, costos de implementación y optimización, costos constantes de gestión, costos de integración de fuentes de datos de diferentes tecnologías y formación de personal / personal nuevo (AlienVault, 2015).

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: (Canaluisa, Meza, & Tasipanta, 2012).

Como apreciamos en la tabla anterior 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.

2.1.13. 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, Caro, & Cancio, 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).

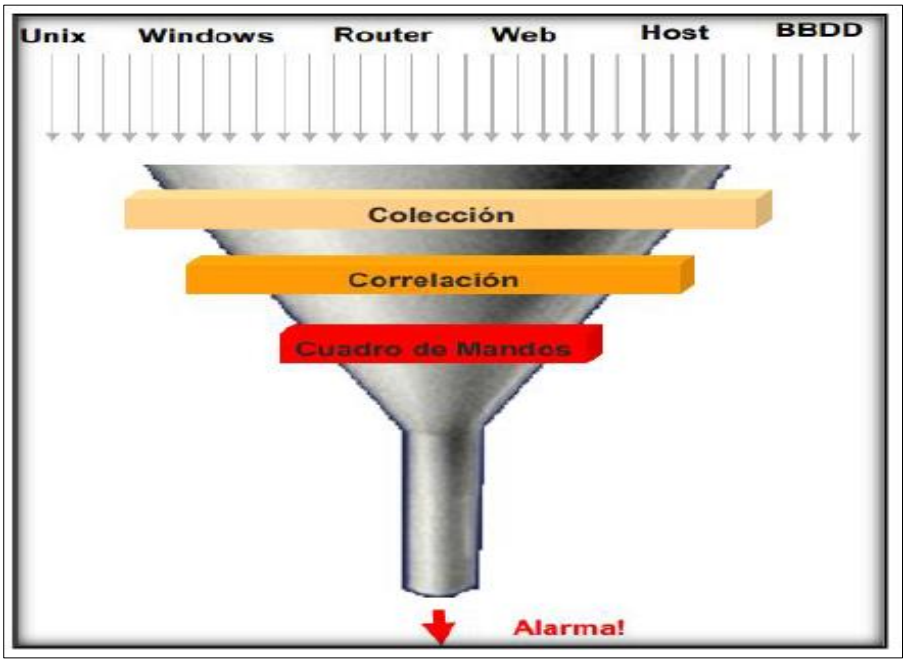


Figura N° 6. Modelo de OSSIM
Fuente: (Bravo Bravo & Villafuerte Quiroz, 2015).

“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, 2018).

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, 2016).

De acuerdo a Alamanni (2014) y *Núñez* (2008), OSSIM tiene 4 componentes principales:

a. ***“Server***

   Es el componente principal de OSSIM. Recibe los eventos enviados por los distintos agentes y realiza además las funciones de priorización y correlación.

   - *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).*

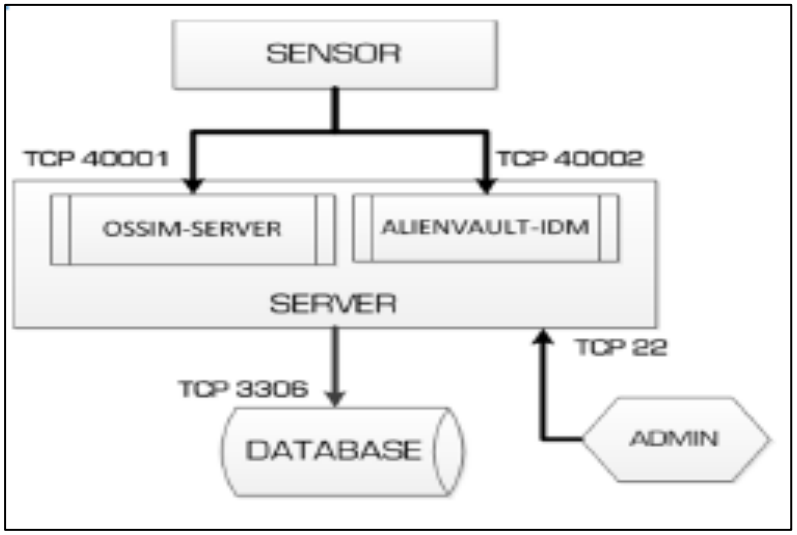


Figura N° 7. AlienVault Server
Fuente: (AlienVault, 2013).

b. 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 (Núñez, 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).*

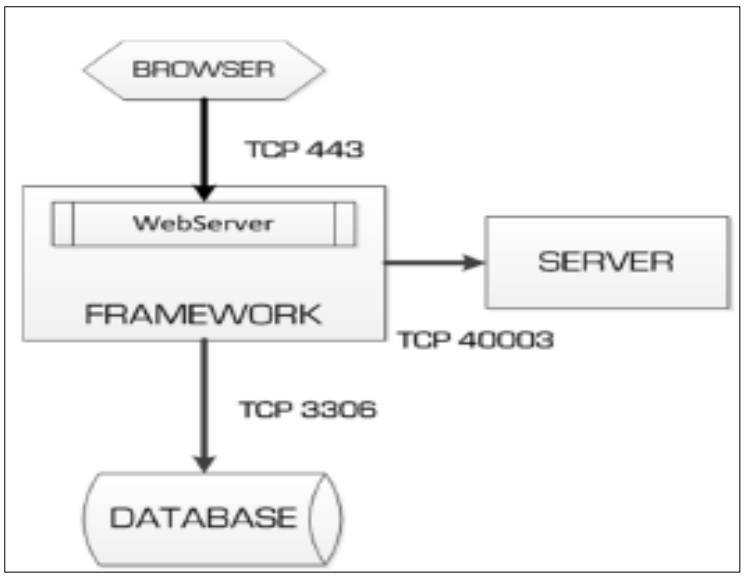


Figura N° 8. AlienVault Framework
Fuente: (AlienVault, 2013).

c. 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.

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).

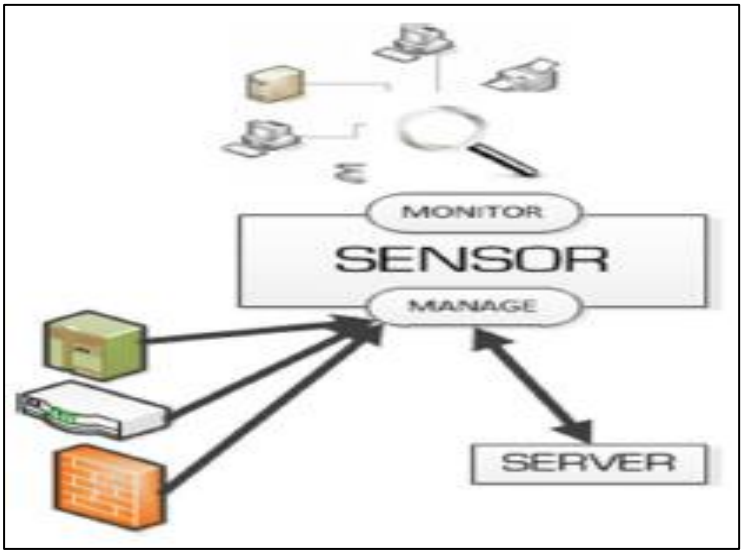


Figura N° 9. AlienVault Sensor (Interfaces de red)
Fuente: (AlienVault, 2013).

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.*

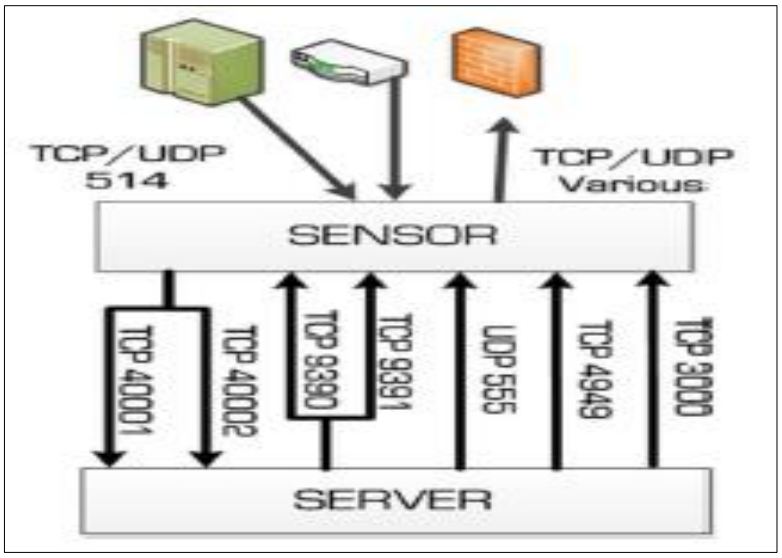


Figura N° 10. Conexiones del sensor
Fuente: (AlienVault, 2013).

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).

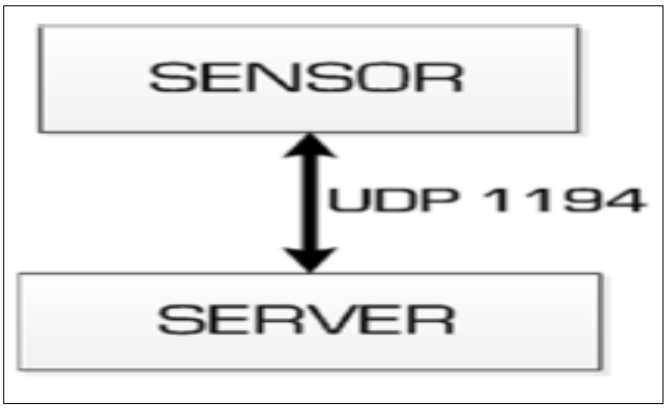


Figura N° 11. Sensor remoto a través de VPN
Fuente: (AlienVault, 2013)

d. 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.

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."

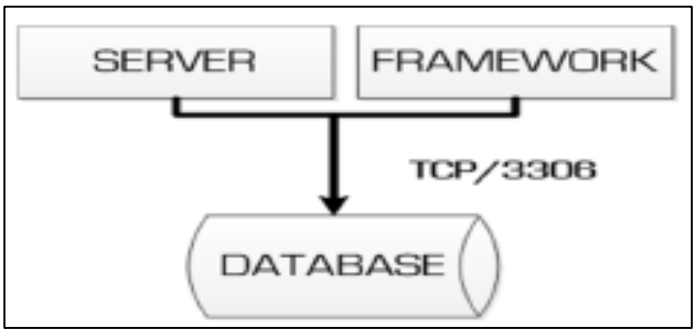


Figura N° 12. Base de Datos AlienVault
Fuente: (AlienVault, 2013).

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

a. EDB Base de datos de eventos, la más voluminosa pues almacena todos los eventos recibidos desde los detectores y monitores.
b. 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.
c. UDB Base de datos de perfiles, almacena todos los datos aprendidos por el monitor de perfiles.

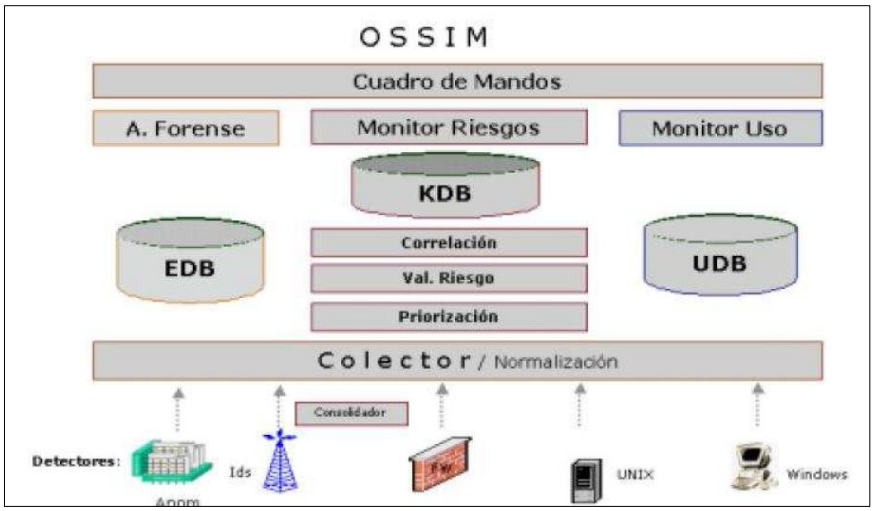


Figura N° 13. Arquitectura de Base de Datos OSSIM
Fuente: (Puchades Olmos, 2018).

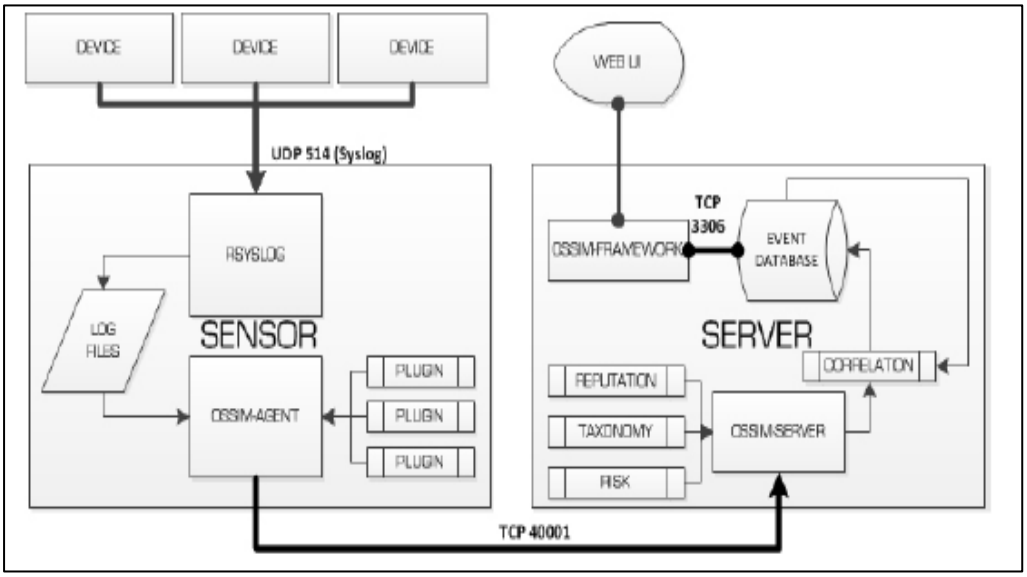


Figura N° 14. OSSIM Architecture
Fuente: (Alamanni, 2014).

2.1.14. Proceso de detección de vulnerabilidades con OSSIM

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.

De acuerdo a Yagual y Chilán (2014) la capacidad de un detector se define mediante 2 variables:

a. “Sensibilidad: Definida como la capacidad de análisis que posee el detector al momento de localizar un posible ataque.
b. Fiabilidad: Definida como el grado de certeza que ofrece el detector ante el aviso de un posible evento.”

Para Canaluisa, Meza y Tasipanta (2012) los detectores en la actualidad tienen dos principales problemas:

a. “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.

b. Falsos Negativos: La incapacidad de detección implicaría que un ataque es pasado por alto.”

Tabla N° 3: Capacidad de los detectores

Propiedad	Descripción	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: (Yagual & Chilán, 2014)

OSSIM cumple las siguientes funciones:

a. 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 (Canaluisa, Meza, & Tasipanta, 2012).

b. 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, ips, macs.

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.
- Pof utilizado para detección de cambios de sistema operativo.
- Nmap utilizado para detectar anomalías en los servicios de red.

c. 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, 2018).

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 registra 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.

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 & Chilán, 2014).

d. 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)

e. Análisis y correlación de eventos

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

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

- **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).

- **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).

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 son 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:

- **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.

f. 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 Incidents→Alarms. 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).

g. 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.

h. 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 enlazará con cada una de las de monitorización para profundizar sobre cualquier problema localizado.

2.1.15. 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:

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
OpenVas	ACTIVA	Escaneo de vulnerabilidades OpenVas realiza escaneos de vulnerabilidades utilizando una serie de firmas Utilidad en OSSIM – Prevención de ataques – Verificar si cumple la política de la organización – 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 tráfico 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)

2.1.16. Flujo de datos en OSSIM

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.

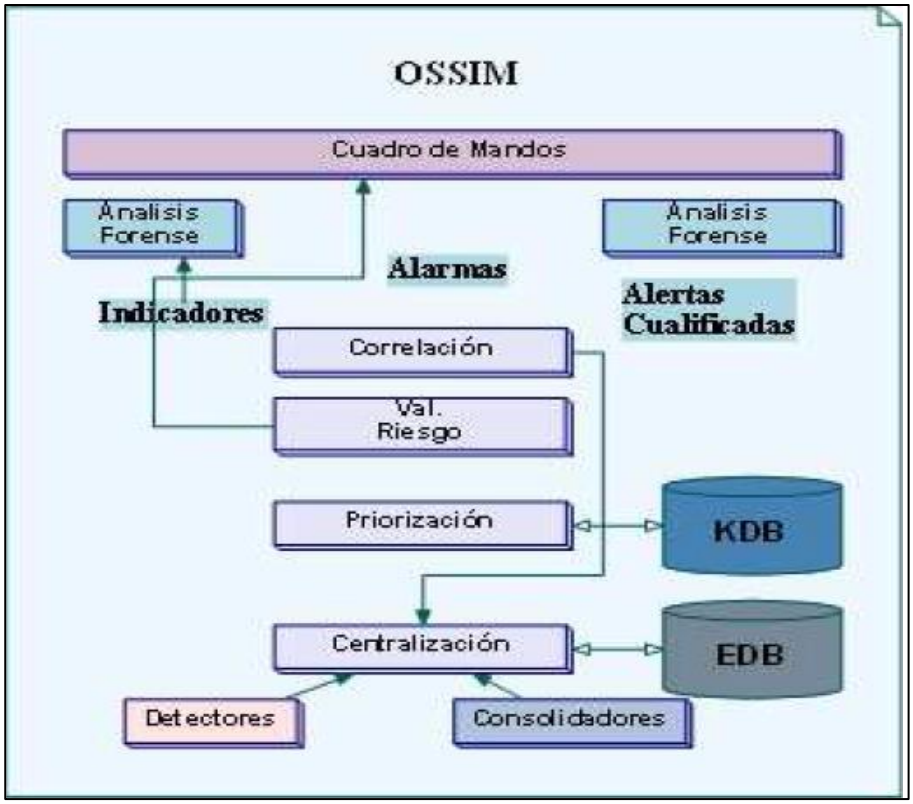


Figura N° 15. Flujo de datos OSSIM
Fuente: (Giménez García, 2015)

La secuencia de pasos de los eventos es:

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.

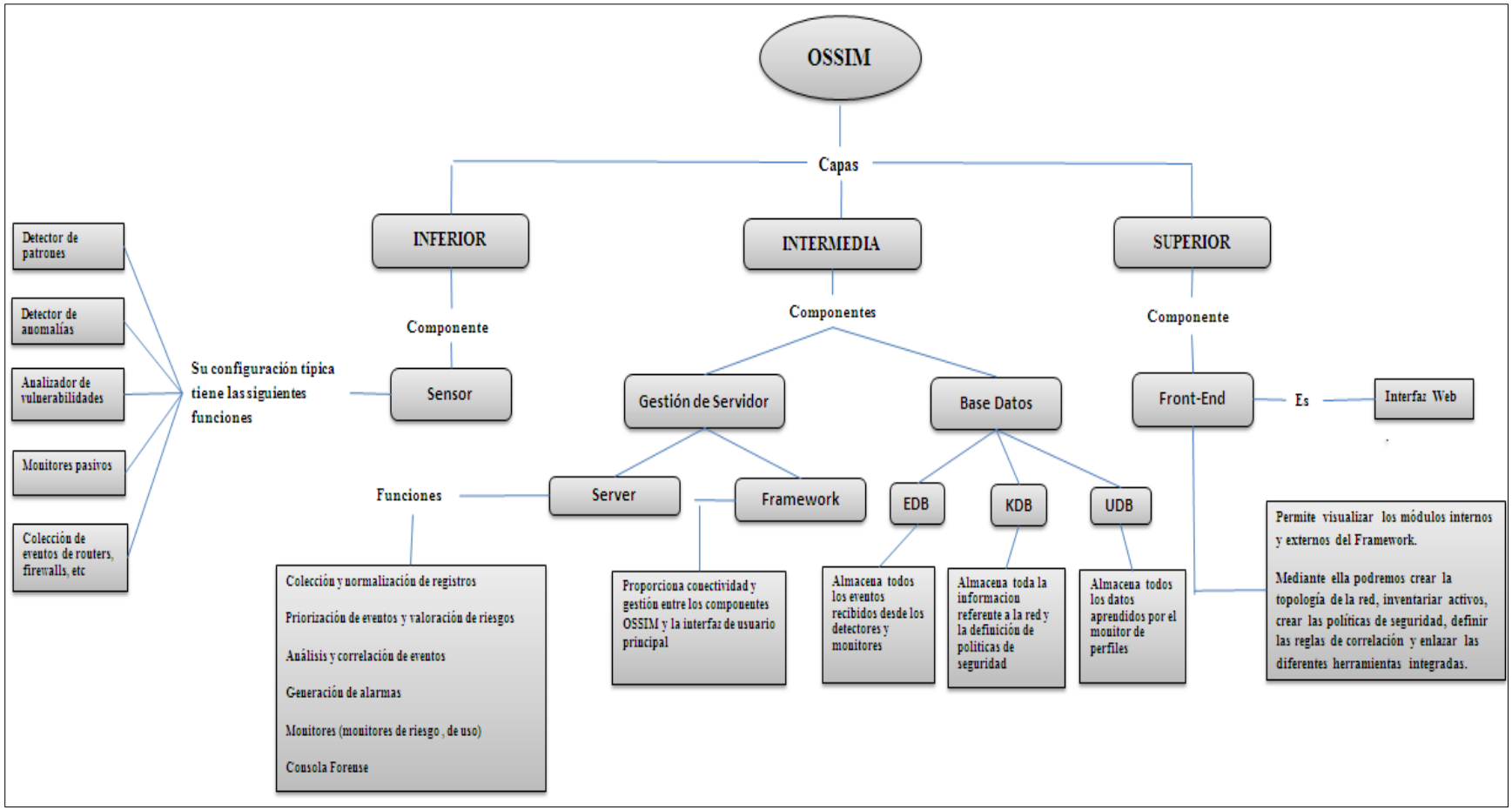


Figura N° 16. Arquitectura lógica de OSSIM y sus componentes
Fuente: (Giménez García, 2015)

2.1.17. Cumplimiento de las normas de seguridad de OSSIM

De acuerdo a Giménez García (2015) el sistema OSSIM tiene un módulo de cumplimiento de normas de seguridad de la información como son:

1. **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.

2. **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.

3. **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.

4. **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.

2.1.18. 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” (Sánchez & Piattini, 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, 2016).

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).

De acuerdo a (Sánchez & Piattini, 2015),

> *“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 explicito, 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.”*

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."*

2.1.19. Procesos COBIT

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).

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:

a. 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.

b. 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.

c. 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.

d. 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.

e. 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.

f. 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. Glosario de términos

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

III. RESULTADOS Y DISCUSIÓN

3.1. Análisis de la situación actual

Para el diagnóstico de la situación actual de la gestión de la seguridad de la información, incluyendo la infraestructura de red de datos, en la Minera Shahuindo, se aplicó un método descriptivo comparativo utilizando como técnica un procedimiento comparativo, tipo auditoría, con los objetivos de control y buenas prácticas definidas en la norma ISO/IEC 27002, en los principales dominios de la seguridad relacionados con los objetivos de la investigación.

Los resultados del análisis se muestran a continuación:

Tabla N° 5: Análisis de la gestión de seguridad de la información en la minera

Ámbito de control	**Políticas del Sistema de gestión de la seguridad de la información**
Objetivo de control	Establecimiento, mantenimiento y documentación de un sistema de gestión de la seguridad de la información en Minera Shahuindo
Prueba	Constatación de la existencia de un conjunto de políticas para la seguridad de la información definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes
Técnica aplicada	– Revisión y análisis documental – Confrontación documental – Entrevistas y descargo de los responsables de la seguridad de la información, gestión de riesgos operativos de TI y Gestión de TI
Hallazgos	
1	**En relación a la disponibilidad de información documentada sobre un sistema de gestión de la seguridad de la información** **Condición encontrada:** – Se constató la existencia de un documento “Políticas sobre tecnologías de la información” cuyo objetivo es definir los estándares mínimos para la seguridad física y lógica para todos los usuarios y recursos de tecnología en Minera Shahuindo. – El documento “Políticas sobre tecnologías de la información” es una declaración de política general sobre seguridad de la información a nivel corporativo. Sin embargo, NO está declarada e implementada como un sistema de gestión de seguridad de la información (SGSI) en la subsidiaria Minera Shahuindo. **Criterio de referencia:** – Control A.5.1.1 Políticas para la seguridad de la información de la ISO/IEC 27001.
2	**En relación al establecimiento del sistema de gestión de la seguridad de la información** **Condición encontrada:** – Se encontró que el documento “Políticas sobre tecnologías de la información” establece lo siguiente: o Se declara a la información como un activo de la Compañía y todo el personal es responsable de salvaguardar el valor, la integridad y la confidencialidad de los activos de información de la Compañía. o Se establece que la información creada, almacenada, procesada, transmitida o impresa por o en nombre de la Compañía es propiedad de la Compañía. o Todo el personal está obligado a proteger los activos de información que están bajo su responsabilidad y que están prohibidos de acceder, usar, modificar, destruir, divulgar o tomar posesión de ellos de manera no autorizada, deliberada o accidental. – El constató que el documento “Políticas sobre tecnologías de la información” se complementa con otras políticas específicas, en los siguientes dominios: o Política de respaldo, gestión y conservación de datos o Política de revisión de acceso de usuario de TI para todas las funciones de administrador en ERP Systems o Política de gestión de cambios **Criterio de referencia:** – Incisos “a”, “b”, “c” y “d” del ítem 5.2 Política del SGSI de la ISO/IEC 27001.

	– Control A.5.1.1 Políticas para la seguridad de la información de la ISO/IEC 27001.
3	**En relación al alcance de las políticas de seguridad de la información** **Condición encontrada:** – El documento "Políticas sobre tecnologías de la información" declara: o que la política de seguridad de la información es aplicable a Minera Shahuindo. o que todo el personal que accede o toma decisiones que afectan la información de la Compañía juega un rol en la protección de esa información. En consecuencia, se espera que todos los empleados y agentes de la compañía, incluidos, los empleados a tiempo completo, los empleados a tiempo parcial, los empleados temporales, los contratistas, los vendedores y los clientes que accedan a los sistemas de la Compañía, son responsables de proteger la información. o Que es responsabilidad de cada empleado que tengan conocimiento de alguna infracción de esta política, la de notificar a su supervisor. – No se encontró sustento que la política general de seguridad de la información y las políticas complementarias hayan sido definidas en base al mapeado de los procesos y sus funciones críticas; así como de la identificación de las expectativas y necesidades de seguridad de la información en cada área de Compañía. **Criterio de referencia:** - Ítem 4.3 Determinar el alcance del sistema de gestión de seguridad de la información de la ISO/IEC 27001.
4	**En relación a los roles, responsabilidades y autoridades organizacionales del sistema de gestión de la seguridad de la información** **Condición encontrada:** - El documento "Políticas sobre tecnologías de la información" NO especifica los roles y responsabilidades en la implementación y aplicación (gestión) del SGSI en Minera Shahuindo. **Criterio de referencia:** - Ítem 5.3 Roles, responsabilidades y autoridades organizacionales de la ISO/IEC 27001.
5	**En relación a la comunicación y publicación del sistema de gestión de la seguridad de la información** **Condición encontrada:** - Se encontró registros que el documento "Políticas sobre tecnologías de la información" ha sido difundido mediante correo electrónico a todos los empleados de Minera Shahuindo. **Criterio de referencia:** - Inciso "f" del Ítem 5.2 Política de la ISO/IEC 27001
Conclusiones	
1	Se ha cumplido con el requerimiento de establecer, mantener y documentar una política general de seguridad de información, a través de su documento "Políticas sobre tecnologías de la información".
3	El no tener mapeado y documentado los procesos de Minera Shahuindo dificulta la definición del alcance del sistema de gestión de la seguridad de la información en esta subsidiaria.
4	La NO definición correcta del alcance del SGSI, podría: - NO permitir a establecer prioridades para la implementación de los controles. - NO cumplirse con las necesidades y expectativas de las partes interesadas (diferentes áreas de Minera Shahuindo) en relación a la seguridad de la información
5	El NO contar con una estructura clara de alineamiento y trazabilidad entre política-objetivo de control-control-indicador para cada dominio de seguridad de la información en el documento "Políticas sobre tecnologías de la información" podría estar ocasionando: - Debilidades en el seguimiento del cumplimiento de las normas, estándares, políticas, procedimientos y otros, así como mantener pistas adecuadas de auditoría - Dificultad para elaborar/mejorar las normas y los procedimientos operativos que permitan llevar a la práctica con efectividad cada una de las políticas declaradas - Ausencia de mediciones de cumplimiento/efectividad de los controles, en base a métricas e indicadores

Valoración del control implantado						
Característica de la información afectada	Disponibilidad		Integridad		Confidencialidad	
	Autenticidad		Trazabilidad	X	Gestión	X
Nivel de madurez del control	Nivel 0 – Nulo		Nivel 1 – Inicial		Nivel 2 – Repetible	X
	Nivel 3 – Definido		Nivel 4 – Gestionado y medible		Nivel 5 – Optimizado	

Ámbito de control	**Políticas del Sistema de gestión de la seguridad de la información**
Objetivo de control	Establecimiento, mantenimiento y documentación de un sistema de gestión de la seguridad de la información en Minera Shahuindo
Prueba	Constatación si la política de seguridad de la información es revisada a intervalos planificados o en el caso de que se produzcan cambios significativos para asegurar su conveniencia, adecuación y efectividad continua.

Técnica aplicada	– Revisión y análisis documental de manera directa – Confrontación documental – Entrevistas y descargo de los responsables de la seguridad de la información, gestión de riesgos operativos de TI y Gestión de TI
Hallazgos	
1	**En relación al mantenimiento de la documentación del sistema de gestión de la seguridad de la información** **Condición encontrada:** – El documento "Políticas sobre tecnologías de la información" tiene carácter corporativo, por tanto, se aprobación corresponde a la matriz de la Compañía. – El documento "Políticas sobre tecnologías de la información" tiene fecha de difusión el 08/16/2017 (versión 17,2). **Criterio de referencia:** – Control A.5.1.2 Revisión de las políticas para la seguridad de la información de la ISO/IEC 27001
2	**En relación a procedimientos de mejora del sistema de gestión de la seguridad de la información** **Condición encontrada:** – No se encontró informes sobre la verificación del cumplimiento de las normas, políticas y procedimientos de seguridad de la información que permitan detectar debilidades en los mismos. **Criterio de referencia:** – Ítem 10 "Mejoras" de la de la ISO/IEC 27001 – Ítem 2 del Artículo 8.2. del documento Políticas de seguridad de la información
3	**En relación al Plan de trabajo en relación procedimientos de mejora del sistema de gestión de la seguridad de la información** **Condición encontrada:** – No se constató la existencia de un Plan de Trabajo de Seguridad de la Información para el año 2018 en Minera Shahuindo, donde las actividades programadas están focalizadas a la evaluación de los riesgos asociados a cada uno de los dominios contemplados en cada uno de los dominios de la seguridad de la información. **Criterio de referencia:** – Artículo 8.4.1. del documento "Políticas de seguridad de la información"
Conclusiones	
1	Las políticas, procedimientos, reglamentos y controles de seguridad de la información NO han sido adecuados a los procesos de negocio de Minera Shahuindo.
2	No existen informes sobre el cumplimiento de las políticas, procedimientos, reglamentos y controles de seguridad de la información en Minera Shahuindo.
3	No existe un Plan de Trabajo de Seguridad de la Información para el año 2018 en Minera Shahuindo.

Valoración del control implantado

Característica de la información afectada	Disponibilidad		Integridad		Confidencialidad	
	Autenticidad		Trazabilidad	X	Gestión	X
Nivel de madurez del control	Nivel 0 – Nulo		Nivel 1 – Inicial		Nivel 2 – Repetible	X
	Nivel 3 – Definido		Nivel 4 – Gestionado y medible		Nivel 5 – Optimizado	

Ámbito de control	**Controles de seguridad de información – Seguridad lógica**
Objetivo de control	Implementar medidas para el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información, para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información.
Pruebas	a. Constatación de la existencia de una política de control de acceso basada en los requisitos de negocio y de seguridad para el acceso b. Constatación de procedimientos formales para la administración de derechos y perfiles c. Constatación de un procedimiento de registro formal de usuarios y de retirada del registro para conceder y revocar el acceso a todos los sistemas y servicios de información d. Verificación si la asignación de contraseñas es controlada a través de un proceso formal de gestión e. Constatación si los usuarios cuentan con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.

	f. Verificación de existencia de revisiones periódicas sobre los derechos concedidos a los usuarios y seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas. g. Verificación de controles para la protección de la información de equipos desatendidos y de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables h. Evaluación de controles especiales sobre pistas de auditoría.
Técnica aplicada	– Comprobación con pruebas sustantivas de campo – Seguimiento de casos (muestra) – Análisis documental (informes) – Entrevistas y descargo de los responsables de la seguridad de la información, gestión de riesgos operativos de TI y Gestión de TI

Hallazgos	
1	**En relación a la existencia de una política de control de acceso lógico a la infraestructura y aplicaciones informáticas** **Condición encontrada:** – Existe la declaración de una política específica para el control de accesos lógicos a las aplicaciones, datos y recursos de tratamiento de la información de Minera Shahuindo, denominada IT User Access Review for all Administrator roles in ERP Systems (includes application and database) – El propósito de esta política es revisar el acceso de todos los usuarios que tienen equivalencia de administrador en cualquier sistema ERP (Ellipse, Foresight, Oracle, Mine Market), para garantizar que el acceso sea apropiado para la lista de usuarios. **Criterio de referencia:** – Ítem A.9.1.1 "Política de control de acceso" de la de la ISO/IEC 27001
2	**En relación a la existencia de un procedimiento formal para la administración de derechos y perfiles** **Condición encontrada:** – Existe un procedimiento operacional formal para controlar la asignación y revisión de derechos de acceso a través del ERP corporativo y para el otorgamiento de cuentas de usuario. – Se encontró un catálogo de perfiles de usuario actualizado. – En el procedimiento operacional para la revisión de accesos especifica los mecanismos para realizar el seguimiento de su cumplimiento. Sin embargo, no se realiza por falta de personal. **Criterio de referencia:** – Ítem A.9.4.1 "Restricción de acceso a la información" de la ISO/IEC 27001
3	**En relación a la existencia de un procedimiento de registro formal de usuarios y de retirada del registro para conceder y revocar el acceso a todos los sistemas y servicios de información** **Condición encontrada:** – Existe un procedimiento operacional formal para la concesión, modificación y revocación de derechos de acceso a través del ERP corporativo y otros recursos de tratamiento de la información de Minera Shahuindo. Allí se establecen los mecanismos de tratamiento para las altas, bajas y modificaciones de cuentas de usuarios. Las solicitudes de cambios en las cuentas de usuarios se realizan mediante el correo institucional. Se utiliza el correo electrónico para el registro de solicitudes de cambio de derechos de acceso (Ver Anexo N° 1) **Criterio de referencia:** – Ítem A.9.2.1 "Registro y baja de usuarios" de la ISO/IEC 27001 – Ítem A.9.2.6 "Remoción o ajuste de derechos de acceso" de la ISO/IEC 27001
4	**En relación a la constatación si los usuarios cuentan con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas** **Condición encontrada:** – Se lleva un registro actualizado del personal de Minera Shahuindo en la que se indica: código de usuario, nombre, puesto de trabajo, fecha de ingreso y de salida de Minera Shahuindo, situación actual. A partir de este registro se elabora la tabla de derechos de acceso de los usuarios a través del ERP corporativo y demás recursos de tratamiento de la información, según su puesto de trabajo. – Se constata que el código de usuario asignado a cada usuario de TI es único. – Se constata que los usuarios, los perfiles de usuario y los derechos de acceso a través del ERP corporativo se realizan en el mismo sistema. Para el caso de los accesos a la red de datos se utiliza un servidor de dominio. **Criterio de referencia:** – Ítem A.9.2.4 "Gestión de información de autentificación secreta de usuarios" de la ISO/IEC 27001
5	**En relación a la gestión y control de la asignación de contraseñas** **Condición encontrada:** – Se constata que se ha definido políticas específicas y controles para la gestión de contraseñas de usuario. – La complejidad de contraseñas se encuentra habilitada en el AD para todos los usuarios.

	– Se evidencia (por comprobación) que se ha establecido un procedimiento específico para la asignación de la contraseña de acceso a la base de datos, el cual es administrado por el responsable de la gestión de la base de datos y el jefe de TI. El procedimiento establece que cualquier acceso o consulta directa a la base de datos que se realice, se registra en una bitácora de control de acceso a la base de datos por el usuario DBA. – Usuarios remotos se conectan mediante VPN Sonicwall – Para la comunicación entre usuarios se gestionan carpetas. Hay un responsable al cual se le proporciona accesos. **Criterio de referencia:** – Ítem A.9.3.1 "Uso de información de autentificación secreta" de la ISO/IEC 27001 – Ítem A.9.4.3 "Sistema de gestión de contraseñas" de la ISO/IEC 27001
6	**En relación al procedimiento de revisión periódica asociados a la seguridad lógica** **Condición encontrada:** – No se realiza las revisiones periódicas sobre los derechos concedidos a los usuarios y seguimiento al uso de sistemas para detectar actividades no autorizadas por falta de personal. **Criterio de referencia:** – Ítem A.9.2.5 "Revisión de derechos de acceso de usuarios" de la ISO/IEC 27001
Conclusiones	
1	Se ha logrado un nivel aceptable de procedimentación para la seguridad lógica, específicamente de los requerimientos para la administración de derechos y perfiles de usuario y para la concesión, modificación y revocación de derechos de acceso
2	Tener procedimientos operativos de "administración de perfiles de usuarios" y de "Altas, bajas y modificación de usuarios" permite: – un correcto seguimiento de los controles – un oportuno y adecuado registro de las incidencias – realizar la trazabilidad de las actividades de los usuarios
3	No se está cumpliendo con lo estipulado en el procedimiento para las revisiones periódicas sobre los derechos concedidos a los usuarios.
4	Se ha logrado un nivel aceptable en el procedimiento para la gestión de contraseñas de usuarios.

Valoración del control implantado						
Característica de la información afectada	Disponibilidad		Integridad	X	Confidencialidad	X
	Autenticidad		Trazabilidad	X	Gestión	
Nivel de madurez del control	Nivel 0 – Nulo		Nivel 1 – Inicial		Nivel 2 – Repetible	
	Nivel 3 – Definido	X	Nivel 4 – Gestionado y medible		Nivel 5 – Optimizado	

Ámbito de control	**Controles de seguridad de información – Seguridad física y ambiental - Áreas seguras/restringidas**
Objetivo de control	Los recursos para el tratamiento de información crítica o sensible para la organización deberían ubicarse en áreas seguras protegidas por un perímetro de seguridad definido, con barreras de seguridad y controles de entrada apropiados. Se debería dar protección física contra accesos no autorizados, daños e interferencias de manera proporcional a los riesgos identificados.
Pruebas	a. Evaluación de los perímetros de seguridad y verificación de la implementación de controles de acceso para proteger las áreas que contienen la información y los recursos de tratamiento de la información b. Verificación y evaluación de los sistemas de protección física contra daño por fuego, inundación, terremoto, malestar social y otras formas de desastres naturales o provocadas por el hombre
Técnica aplicada	– Observación – Comprobación de funcionamiento por muestreo – Registro fotográfico – Entrevistas y descargo de los responsables de la seguridad de la información, gestión de riesgos operativos de TI y Gestión de TI
Hallazgos	
1	**En relación a la existencia a la Seguridad física y control de acceso a las áreas seguras/restringidas** **Condición encontrada:** – No se encontró políticas específicas para la Seguridad física y ambiental – Las áreas críticas de TI están declaradas como zonas seguras con acceso limitado y restringido. o Área de TI. La puerta de acceso permanece cerrada. o Data Center. La puerta de acceso permanece cerrada. o Equipos críticos ubicados en gabinetes con llave. – Sólo en el Data center el control de acceso.

	Criterio de referencia: – Ítem A.11.1.1 “Perímetro de seguridad física” de la ISO/IEC 27001 – Ítem A.11.1.2 “Controles de ingreso físico” de la ISO/IEC 27001 – Ítem A.11.1.3 “Asegurar oficinas, áreas e instalaciones” de la ISO/IEC 27001 – Ítem A.11.1.4 “Protección contra amenazas externas y ambientales” de la ISO/IEC 27001
2	**En relación a Sistemas de protección física contra daño por fuego** **Condición encontrada:** – Se constata que en todas las zonas seguras existen extintores contra incendios de dióxido de carbono CO2. – Se verificó que en todos los casos los equipos extintores tienen fecha de vigencia conforme. – Se constata que en todas las zonas seguras tienen instalado un sistema detector de humo. – No se evidencia entrenamiento de los empleados en el uso de extintores **Criterio de referencia:** – Ítem A.11.1.3 “Asegurar oficinas, áreas e instalaciones” de la ISO/IEC 27001 – Ítem A.11.1.2 “Protección contra amenazas externas y ambientales” de la ISO/IEC 27001
3	**En relación a la señalización** **Condición encontrada:** – Se constata que, en las zonas de TI consideradas como áreas seguras, tienen señalización adosadas a la pared que indican “zonas seguras” de resguardo de personas en caso de sismos y de “salida o rutas de escape”. **Criterio de referencia:** – Ítem A.11.1.3 “Asegurar oficinas, áreas e instalaciones” de la ISO/IEC 27001
Conclusiones	
1	Se ha logrado un nivel aceptable en la implementación de controles para el control de acceso físico y seguridad perimetral a las áreas declaradas como seguras/restringidas.
2	Se ha logrado un nivel aceptable en la implementación de mecanismos de mitigación o extinción de fuego
3	Existe un sistema de señalización en un nivel aceptable para identificar zonas de acceso restringido y rutas de salida/escape, concordante con NTP 399.010.1:2004 sobre Señales de Seguridad.

Valoración del control implantado						
Característica de la información afectada	Disponibilidad	X	Integridad		Confidencialidad	
	Autenticidad		Trazabilidad		Gestión	
Nivel de madurez del control	Nivel 0 – Nulo		Nivel 1 – Inicial		Nivel 2 – Repetible	
	Nivel 3 – Definido	X	Nivel 4 – Gestionado y medible		Nivel 5 – Optimizado	

Ámbito de control	**Controles de seguridad de información – Seguridad física y ambiental - Seguridad y uso de equipos de cómputo**
Objetivo de control	Implementar mecanismos -generalmente de prevención y detección- destinados a proteger físicamente los recursos de TI con los que cuenta Minera Shahuindo.
Pruebas	a. Verificación si los equipos están protegidos y usados de tal forma que reduzcan los riesgos de las amenazas y los riesgos del entorno b. Verificación si los equipos están protegidos contra fallos de energía y de otras interrupciones causadas por fallos en las instalaciones de suministro. c. Verificación si el cableado eléctrico y de telecomunicaciones que transmiten datos a los servicios de soporte de la información están protegido de interceptación o de daños d. Comprobación si los equipos han sido mantenidos de una manera correcta para asegurar su continuidad, disponibilidad e integridad.
Técnica aplicada	– Revisión documental – Observación – Comprobación de funcionamiento por muestreo – Registro fotográfico – Entrevistas y descargo de los responsables de la seguridad de la información, gestión de riesgos operativos de TI y Gestión de TI
Hallazgos	
1	**En relación a la existencia de una política de protección y uso de equipos** **Condición encontrada:** – Existen políticas específicas para la seguridad y uso de equipos de uso oficial de la minera, como: o Los empleados con computadoras portátiles pueden comunicarse con miembros de la familia o para asuntos personales, según sea necesario, mientras viajan. o Los teléfonos celulares de la compañía se pueden usar para llamadas personales limitadas y necesarias para eliminar la necesidad de que el empleado lleve dos teléfonos celulares. Al viajar al

	extranjero, el empleado debe ser consciente de los costos de voz y datos y mantener las llamadas personales al mínimo. o Los empleados renuncian a su derecho de privacidad a todo lo que se cree, almacene, envíe, visualice o reciba en los equipos informáticos de la empresa. Los empleados dan su consentimiento para que la administración supervise o acceda a los elementos que un empleado crea, almacena, envía, visualiza o recibe en el equipo de TI. – Las siguientes actividades están estrictamente prohibidas en los equipos informáticos de la empresa o mediante equipos informáticos de propiedad personal mientras se accede a banda ancha o Internet de la empresa: o Enviar, recibir, exhibir, imprimir, diseminar o publicar material que sea fraudulento, acosador, sexualmente explícito, perjudicial, difamatorio, intimidante o vergonzoso para la Compañía a la vista del público. o Enviar, recibir, exhibir, imprimir, diseminar o publicar material que viole la propiedad intelectual, marca registrada o derechos de autor de otros. o Enviar, recibir, exhibir, imprimir, diseminar o publicar material que viole las leyes locales, estatales o internacionales en cualquier otra jurisdicción donde opera Tahoe. **Criterio de referencia:** – Ítem A.11.2.1 “Emplazamiento y protección de los equipos” de la ISO/IEC 27001 – Ítem A.11.2.2 “Servicios de suministro” de la ISO/IEC 27001 – Ítem A.11.2.3 “Seguridad del cableado” de la ISO/IEC 27001 – Ítem A.11.2.4 “Mantenimiento de equipos” de la ISO/IEC 27001
2	**En relación a la Ubicación de los recursos de TI críticos** **Condición encontrada:** Se constató que: – Los recursos críticos principales: servidores, switch principal, router, están ubicados en el Data Center, en un ambiente aislado y hermetizado del Área de TI, cuyo acceso es restringido sólo para el personal autorizado del Área de TI. – Los equipos de comunicación secundarios (de borde) están ubicados en gabinetes cerrados con llave, ubicados en zonas de acceso restringido, independientes y aisladas.
3	**En relación a la Protección contra amenazas ambientales** **Condición encontrada:** Se constató que: – El ambiente del Data Center se encuentra climatizado mediante un sistema de aire acondicionado, manteniendo el ambiente en promedio a 18-22 °C, temperatura adecuada para el funcionamiento de los servidores y equipos de comunicación de centrales.
4	**En relación a la Protección contra fallos de energía y de otras interrupciones causadas en las instalaciones de suministro** **Condición encontrada:** Se constató que: – El ambiente del Data Center: o cuentan con un sistema de red múltiple de alimentación de energía estabilizada que evita el fallo de suministro: hay una toma de línea para UPS y otra línea que abastece de energía a los equipos informáticos o cuentan con interruptores (llaves cuchilla) diferenciales térmicas que desconecta el circuito cuanto existe cualquier derivación o cuentan con sistemas de conexión a tierra (pozo a tierra) o cuentan con sistema ininterrumpido de energía (UPS) que proporcionan energía con una autonomía de 30 minutos a los equipos del gabinete de comunicaciones y servidores o la acometida de la instalación eléctrica es área y canalizada por tubo empotrado hasta el punto de alimentación o cuentan con un sistema generador de energía
5	**En relación al Cableado de datos** **Condición encontrada:** Se constató que: – El sistema de cableado estructurado o El tendido de cables de datos es de Cat 6 y 6ª, 2012, y 2016, a través de piso técnico y canaleteado. Todos los cables están canalizados desde el rack de comunicaciones hasta cada una de las estaciones de trabajo. o En las estaciones de trabajo los adaptadores y patch cord corresponden a la categoría de cable tendido: cat 6. o los patch cord en el patch panel y en las tomas de usuario están etiquetados
Conclusiones	
1	Los equipos críticos de tratamiento de la información están ubicados en zonas seguras y de acceso restringido de forma aceptable.

2	Las salvaguardas y controles en relación a la Protección de los equipos, Protección contra amenazas ambientales, Protección contra fallos de energía han logrado niveles aceptables en la seguridad física y ambiental.
3	El tendido de cable de datos en las diferentes agencias de Minera Shahuindo cumple aceptablemente la norma ANSI/TIA/EIA-569-A referente los recorridos del cableado de datos y espacios de telecomunicaciones.

Valoración del control implantado						
Característica de la información afectada	Disponibilidad	X	Integridad	X	Confidencialidad	
	Autenticidad		Trazabilidad		Gestión	
Nivel de madurez del control	Nivel 0 – Nulo		Nivel 1 – Inicial		Nivel 2 – Repetible	
	Nivel 3 – Definido	X	Nivel 4 – Gestionado y medible		Nivel 5 – Optimizado	

Ámbito de control	**Controles de seguridad de información – Gestión de activos – Inventario de activos**
Objetivo de control	Identificar y valorar todos aquellos recursos de TI (bases de datos, acuerdos y/o contratos, documentos del sistema, ficheros, aplicaciones, software de información, equipos informáticos, entre otros) con los que cuenta Minera Shahuindo, que posee algún valor que permita implementar mecanismos para su protección y asignar responsabilidades para el mantenimiento de su seguridad.
Pruebas	a. Comprobación si todos los activos han sido claramente identificados y si se ha preparado y mantiene un inventario de todos los activos importantes. b. Verificación si toda la información y los activos asociados con los recursos para el tratamiento de la información han sido asignados a un propietario de Minera Shahuindo. c. Constatación si se ha identificado, documentado e implantado reglas de uso aceptable de la información y de los activos asociados con el tratamiento de la información.
Técnica aplicada	– Revisión y análisis documental – Confrontación documental – Comprobación de aplicación de la política o norma mediante evidencias documentadas – Entrevistas y descargo de los responsables de la seguridad de la información, gestión de riesgos operativos de TI y Gestión de TI
Hallazgos	
1	**En relación a la existencia de un inventario de activos de TI** **Condición encontrada:** – Existe un inventario de equipos de TI, en formato digital (MS Excel) denominado “Inventario hardware”, clasificado por subsidiaria y actualizado hasta junio 2018, donde se registra las características técnicas, su condición y el área a la cual fue asignada. – Se evidencia la existencia de un inventario de software instalado en cada equipo, en formato digital (MS Excel) denominado “Inventario software” y actualizado hasta junio 2018, donde se registra el fabricante, el producto, el tipo de licenciamiento y el total de licencias. – Se declara que cada área es responsable de uso de los equipos de TI que están bajo se gestión. – No se declara la criticidad de los equipos de hardware. **Criterio de referencia:** – Ítem A.8.1.1 “Inventario de activos” de la ISO/IEC 27001 – Ítem A.8.1.2 “Propiedad de los activos” de la ISO/IEC 27001
3	**En relación al procedimiento para actualizar el inventario de activos de TI** **Condición encontrada:** – No existe documentación que especifique el procedimiento y la periodicidad de actualización de los inventarios de TI. **Criterio de referencia:** – Ítem A.8.1.1 “Inventario de activos” de la ISO/IEC 27001
4	**En relación a las reglas de uso aceptable de la información y de los activos asociados con el tratamiento de la información** **Condición encontrada:** – Se constató que se han descrito y aplicado reglas y políticas de uso aceptable de la información y de los activos, como: formas de uso de los recursos, inventario, control y niveles de acceso, antivirus, uso de archivos de imágenes y videos, acceso a internet, instalación/desinstalación de software, uso de dispositivos de almacenamiento secundarios, instalación de periféricos, copias de respaldo, uso de claves y códigos de usuarios para el acceso a la red y a las aplicaciones, etc.

	Criterio de referencia: – Ítem A.8.1.2 “Propiedad de los activos” de la ISO/IEC 27001
Conclusiones	
1	Minera Shahuindo ha cumplido parcialmente con las exigencias de realizar y mantener un inventario de activos asociados a la tecnología de información y la asignación de responsabilidades respecto a la protección de estos activos. Queda pendiente: – la clasificación del hardware de acuerdo a su criticidad – establecer de manera formal un procedimiento y la periodicidad de actualización de los inventarios de TI
2	Clasificar la información que se gestiona en cada área (física y digital) de tal forma que permita determinar mecanismos para su tratamiento y protección

Valoración del control implantado						
Característica de la información afectada	Disponibilidad	X	Integridad		Confidencialidad	X
	Autenticidad		Trazabilidad	X	Gestión	X
Nivel de madurez del control	Nivel 0 – Nulo		Nivel 1 – Inicial		Nivel 2 – Repetible	
	Nivel 3 – Definido	X	Nivel 4 – Gestionado y medible		Nivel 5 – Optimizado	

Ámbito de control	**Controles de seguridad de información – Gestión de las comunicaciones y las operaciones – Procedimientos y responsabilidades operativas**
Objetivo de control	Implementar mecanismos de asignación de responsabilidades y procedimientos de operación, de gestión de los servicios con terceros, para la protección contra código malicioso, para las copias de seguridad, la seguridad de redes, el intercambio de información, que aseguren el cumplimiento de las políticas y controles de seguridad de la información.
Pruebas	a. Constatación si se ha implantado y mantenido procedimientos operacionales y están disponibles para todos los usuarios que lo necesiten b. Verificación si se controlan los cambios en los recursos y sistemas de tratamiento de la información c. Verificación si las tareas y áreas de responsabilidad están segregados para reducir la posibilidad de modificaciones no autorizadas e intencionadas o el mal uso de los activos de la organización d. Verificación si se ha separado los recursos para el desarrollo, las pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema operativo.
Técnica aplicada	– Revisión documental – Observación – Comprobación de funcionamiento – Entrevistas y descargo de los responsables de la seguridad de la información, gestión de riesgos operativos de TI y Gestión de TI
Hallazgos	
2	**En relación a la implantación de procedimientos y responsabilidades operativas** **Condición encontrada:** – Todos los procedimientos operativos y sus correspondientes reglamentos son elaborados y aprobados de manera corporativa – Existe de manera documentada y aprobada procedimientos operacionales de TI relacionados con: o Control de cambios o Gestión de accesos lógicos o Generación de respaldos de la información – No existen procedimiento operativos relacionados con: **Desarrollo** o Procedimiento para el Desarrollo de software o Procedimiento para la Atención de Requerimientos de Módulos-Adecuaciones o Procedimiento para la Certificación de módulos antes de puesta en producción o Procedimiento para la Generación y gestión de base de datos de desarrollo **Producción y Soporte** o Procedimiento para el registro de incidentes de seguridad de la información o Procedimiento para altas, bajas y modificación de usuarios de los sistemas o Procedimiento para administración de perfiles de usuarios o Reglamento para el uso del correo electrónico institucional

3	**En relación al Control de cambios** **Condición encontrada:** – Se constata documentación sobre procedimientos de control de cambios que garantiza que los cambios realizados en los recursos tecnológicos de la Compañía se evalúen, graben, testean, autoricen y divulguen de forma coherente y adecuada.
4	**En relación a la segregación de funciones y separación de los recursos para el desarrollo de sistemas, las pruebas y operación** **Condición encontrada:** – La segregación de cambios se gestiona y determina desde Tahoe en Reno. No se realiza de manera local. – Se constata que el área de desarrollo trabaja con una red de datos independiente y separada a la red de datos corporativa de Minera Shahuindo, con su propio servidor preparado para sus propósitos. – Existe un procedimiento operativo y una aplicación para la generación de una base de datos con el que trabaja el personal del Área de Desarrollo de sistemas, tanto para la programación como para las pruebas de las aplicaciones desarrolladas y/o modificadas.
Conclusiones	
1	Se ha logrado documentar en un nivel aceptable los procedimientos operacionales de: o Control de cambios o Gestión de accesos lógicos o Generación de respaldos de la información Falta contar con la documentación de los procedimientos operativos de la evidencia 1, que son básicos para una buena gestión de las TI.
2	Se ha logrado implantar controles de cambios en los principales procesos de TI de Minera Shahuindo en un nivel aceptable, de tal forma que permiten: - justificar los cambios, debidamente sustentados con las autorizaciones de peticiones de cambio - registrar, clasificar y documentar los cambios aprobados - testear y probar los cambios en entorno de prueba
3	Se ha logrado segregarlas funciones de las Áreas de Desarrollo de sistemas y de Producción y soporte; así como se ha separado los recursos, específicamente la red de datos y la base de datos, para el cumplimiento de las actividades de desarrollo de sistemas, pruebas y operación, lográndose controles de un nivel aceptable que evita, se vulnere el principio de confidencialidad de la información en este aspecto.

Valoración del control implantado						
Característica de la información afectada	Disponibilidad	X	Integridad	X	Confidencialidad	X
	Autenticidad		Trazabilidad	X	Gestión	
Nivel de madurez del control	Nivel 0 – Nulo		Nivel 1 – Inicial		Nivel 2 – Repetible	
	Nivel 3 – Definido	X	Nivel 4 – Gestionado y medible		Nivel 5 – Optimizado	

Ámbito de control	**Controles de seguridad de información – Gestión de las comunicaciones y las operaciones – Planificación y aceptación de sistemas, Protección contra software malicioso y Copias de seguridad**
Objetivo de control	Implementar mecanismos de asignación de responsabilidades y procedimientos de operación, de gestión de los servicios con terceros, para la protección contra código malicioso, para las copias de seguridad, la seguridad de redes, el intercambio de información, que aseguren el cumplimiento de las políticas y controles de seguridad de la información.
Pruebas	a. Verificación si se ha establecido un criterio de aceptación para los nuevos sistemas, las actualizaciones y las nuevas versiones; así como llevarse a cabo las pruebas adecuadas del (de los) sistema(s) durante el desarrollo y previamente a la aceptación. b. Verificación si se ha implementado controles de detección, prevención y recuperación para proteger contra código malicioso c. Constatación de la existencia de copias de seguridad de la información y del software y verificación si se comprueban regularmente de acuerdo con la política específica sobre de copias de seguridad.
Técnica aplicada	– Revisión documental – Observación – Comprobación de funcionamiento – Entrevistas y descargo de los responsables de la seguridad de la información, gestión de riesgos operativos de TI y Gestión de TI
Hallazgos	

<table>
<tr><td>2</td><td>En relación a los controles de detección, prevención y recuperación para proteger contra código malicioso
Condición encontrada:

– Se constata que se ha implementado los siguientes controles para la protección contra código malicioso:
o Instalación de un sistema licenciado de antivirus, que abarca todas las PC’s clientes y Servidores, con actualización automática de la base de datos de firmas
o Definición de usuarios y grupos de usuarios de la red de datos de Minera Shahuindo a través de Directorio Activo, reduciendo el mantenimiento y configuración de los usuarios y grupos de usuarios. Para ello se han definido dominios por tipo de usuario y/o servicio. Con ello se asigna permisos a las aplicaciones/servicios autorizadas a los usuarios o grupos de usuarios de forma predefinida.
o Políticas de firewall y acceso a internet de los usuarios de la red interna a través, donde se establecen restricciones de acceso a Internet por equipo y nombre de usuario, reglas de acceso VPN para controlar conexión con otras dependencias, reglas de acceso y salidas DNS, POP3, SMTP, FTP.
o Reglas de directiva del sistema en Activity Directory para permitir/restringir el acceso a los servicios por equipo y nombre de usuario, como: el acceso a la red y sistema operativo está definido autenticado (nombre de usuario y password), habilitación/deshabilitado los puertos USB, lectoras/reproductores de CD o DVD y otras posibilidades de lectura/escritura de data y programas a las terminales, imposibilidad de instalación de programas en general, imposibilidad de modificación de parámetros del sistema: fecha, hora y otros; así como acceso a entornos de configuración del computador, imposibilidad de agregar nuevos dispositivos externos conectados a los terminales, la opción “ejecutar” está deshabilitada, la opción de acceso al sistema operativo DOS está deshabilitada, el acceso a la red de datos mediante el explorador de Windows está restringido, se ha ocultado las unidades específicas de Mi PC, el acceso a la unidad C:\ mediante el explorador está restringido, URL de la barra de búsqueda está deshabilitado, se ha desactivado la reproducción automática en todas las terminales, se ha quitado "Conectar a unidad de red" y "Desconectar de unidad de red, se ha quitado Documentos compartidos de Mi PC, etc.

Criterio de referencia:
– Ítem A.12.2.1 “Controles contra códigos maliciosos” de la ISO/IEC 27001</td></tr>
<tr><td>3</td><td>En relación a las copias de seguridad de la información y del software
Condición encontrada:
– Existen políticas y un reglamento específico sobre la generación de respaldos de la información en el documento, donde se establece el procedimiento, los roles, responsabilidades y funciones específicas para su cumplimiento, la periodicidad y frecuencia de su ejecución, forma de su etiquetado, tipo de información que se copia.
– Se generan backups completos e incrementales a discos y luego a cintas (una sola), de manera semanales (completa) y entre semana (incrementales en disco). La oficina de Lima es la que se encarga de esta tarea.
– No se constata la existencia de un procedimiento de restauración de las copias de respaldo en el caso de fallos o desastres que afecten la base de datos en producción.

Criterio de referencia:
– Ítem A.12.3.1 “Respaldos de la información” de la ISO/IEC 27001</td></tr>
<tr><td colspan="2">Conclusiones</td></tr>
<tr><td>1</td><td>Se cumple en un nivel aceptable establecer procedimientos de respaldos regulares y periódicamente validados y de medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre.</td></tr>
<tr><td>2</td><td>Se cumple en un nivel aceptable la conservación de la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación del centro principal de procesamiento.</td></tr>
<tr><td>3</td><td>Se ha logrado implementar controles en un nivel aceptable que eliminan las aplicaciones no deseadas o desconocidas en la red de datos, reduciendo el riesgo de la ejecución de código malintencionado o espía y mejorando la estabilidad de la red, como:
– una política formal de cumplimiento de las licencias de software y la prohibición del uso de software no autorizado
– la instalación y administración de un sistema contra malware
– implementación de reglas de directivas y políticas de acceso a Internet, a los servicios de la red de datos y al sistema operativo, mediante la administración de los inicios de sesión en los equipos conectados a la red, así como también de la administración de políticas en toda la red por Activity Directory o sistema antivirus.</td></tr>
<tr><td colspan="2">Valoración del control implantado</td></tr>
<tr><td colspan="2"><table><tr><td></td><td>Disponibilidad</td><td>X</td><td>Integridad</td><td>X</td><td>Confidencialidad</td><td>X</td></tr></table></td></tr>
</table>

Característica de la información afectada	Autenticidad	X	Trazabilidad		Gestión	
Nivel de madurez del control	Nivel 0 – Nulo		Nivel 1 – Inicial		Nivel 2 – Repetible	
	Nivel 3 – Definido	X	Nivel 4 – Gestionado y medible		Nivel 5 – Optimizado	

Ámbito de control	**Controles de seguridad de información – Gestión de las comunicaciones y las operaciones – Gestión de la seguridad de red**
Objetivo de control	Implementar mecanismos de asignación de responsabilidades y procedimientos de operación, de gestión de los servicios con terceros, para la protección contra código malicioso, para las copias de seguridad, la seguridad de redes, el intercambio de información, que aseguren el cumplimiento de las políticas y controles de seguridad de la información.
Pruebas	a. Evaluación de la gestión y control de la red de datos, en relación a la protección de amenazas y el mantenimiento de la seguridad de los sistemas y aplicaciones que usan la red. b. Verificación de los controles para la evaluación de las características de seguridad, los niveles de servicio y los requisitos de gestión de los servicios de red subcontratados.
Técnica aplicada	– Revisión documental – Comprobación de funcionamiento – Uso de software específico para testeo de penetración – Entrevistas y descargo de los responsables de la seguridad de la información, gestión de riesgos operativos de TI y Gestión de TI
Hallazgos	
1	**En relación a la gestión y control de la red de datos** **Condición encontrada:** – Se ha diagramado la arquitectura de la red de datos, horizontal y vertical en Minera Shahuindo; llevándose un registro actualizado de las características técnicas de cada uno de los equipos tecnológicos que lo conforman. – Para proteger la red de datos de amenazas y para mantener la seguridad de los sistemas y aplicaciones que usan estas redes, incluyendo la información en tránsito, se ha implementado un firewall Sonic, gestionado por empresa extrajera Reno EEUU. – En relación a la gestión de la red se constató que: o Se permite o deniega el acceso a la red gestionando los inicios de sesión de los equipos conectados a la red a través de un servidor de dominio. o Se ha definido perfiles de acceso a los recursos de la red. Los perfiles de acceso a la red se han definido en un servidor de dominio o Se analiza el tráfico de la red y servicio VPN. o Se realiza gestión remota de terminales. – Se comprobó que se ha restringido el acceso a laptops u otros equipos a las que no les haya sido asignada una IP previamente, verificándose que la asignación de direcciones IP a los diversos equipos en la red de Minera Shahuindo, se da de manera estática. Para ello se ha generado un mapa de direcciones IP utilizadas para llevar un control más adecuado de direcciones IP asignadas por equipo. – Se cuenta con apliance Sonicwall UTM para el filtrador de accesos y aplicativos de red **Criterio de referencia:** – Ítem A.13.1.1 “Controles de la red” de la ISO/IEC 27001 – Ítem A.13.1.2 “Seguridad de servicios de red” de la ISO/IEC 27001 – Ítem A.13.1.3 “Segregación en redes” de la ISO/IEC 27001
Conclusiones	
1	Se evidencia que se ha cumplido en un nivel aceptable con seguridad sobre la red de datos

Valoración del control implantado						
Característica de la información afectada	Disponibilidad	X	Integridad	X	Confidencialidad	X
	Autenticidad		Trazabilidad		Gestión	
Nivel de madurez del control	Nivel 0 – Nulo		Nivel 1 – Inicial		Nivel 2 – Repetible	
	Nivel 3 – Definido	X	Nivel 4 – Gestionado y medible		Nivel 5 – Optimizado	

Ámbito de control	**Controles de seguridad de información – Gestión de incidentes de seguridad de la información**
Objetivo de control	Lograr la revisión y la mejora continua del servicio de TI en Minera Shahuindo para garantizar la disponibilidad, integridad y confidencialidad de la información, a través de la notificación oportuna de eventos y el establecimiento de procedimientos y responsabilidades para el registro, escalonamiento, tratamiento, seguimiento y cierre de incidentes de seguridad de la información.
Pruebas	a. Constatación si se ha establecido responsabilidades y procedimientos de gestión para garantizar el registro y comunicación oportuna y de una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información
Técnica aplicada	– Análisis documental – Comprobación – Seguimiento de casos (muestra) – Entrevistas y descargo de los responsables de la seguridad de la información, gestión de riesgos operativos de TI y Gestión de TI

Hallazgos	
1	**En relación a la Política de gestión de incidentes de seguridad de la información** **Condición encontrada:** – Las políticas y controles para la gestión de los incidentes de TI se elaboran a nivel corporativo. Allí se definen: o Los roles y responsabilidades o El procedimiento para la gestión de incidentes o Clasificación de incidentes y eventos o El escalado para el tratamiento de los incidentes o Tiempos de resolución de los incidentes por tipo o indicadores **Criterio de referencia:** – Ítem A.16.1.1 “Responsabilidades y procedimientos” de la ISO/IEC 27001
2	**En relación al Procedimiento para la gestión de incidentes de seguridad de la información** **Condición encontrada:** – Los reportes de eventos y debilidades de seguridad de la información se gestionan a través del sistema SYSAID. **Criterio de referencia:** – Ítem A.16.1.2 “Reporte de eventos de seguridad de la información” de la ISO/IEC 27001 – Ítem A.16.1.3 “Reporte de debilidades de seguridad de la información” de la ISO/IEC 27001

Conclusiones	
1	Para la gestión de incidentes de TI se utiliza un sistema SYSAID que cubre todas las actividades necesarias para asegurar la atención de los incidentes reportados y su trazabilidad: registro, clasificación de incidentes, priorización, seguimiento y cierre.

Valoración del control implantado						
Característica de la información afectada	Disponibilidad	X	Integridad	X	Confidencialidad	X
	Autenticidad		Trazabilidad	X	Gestión	X
Nivel de madurez del control	Nivel 0 – Nulo		Nivel 1 – Inicial		Nivel 2 – Repetible	X
	Nivel 3 – Definido		Nivel 4 – Gestionado y medible		Nivel 5 – Optimizado	

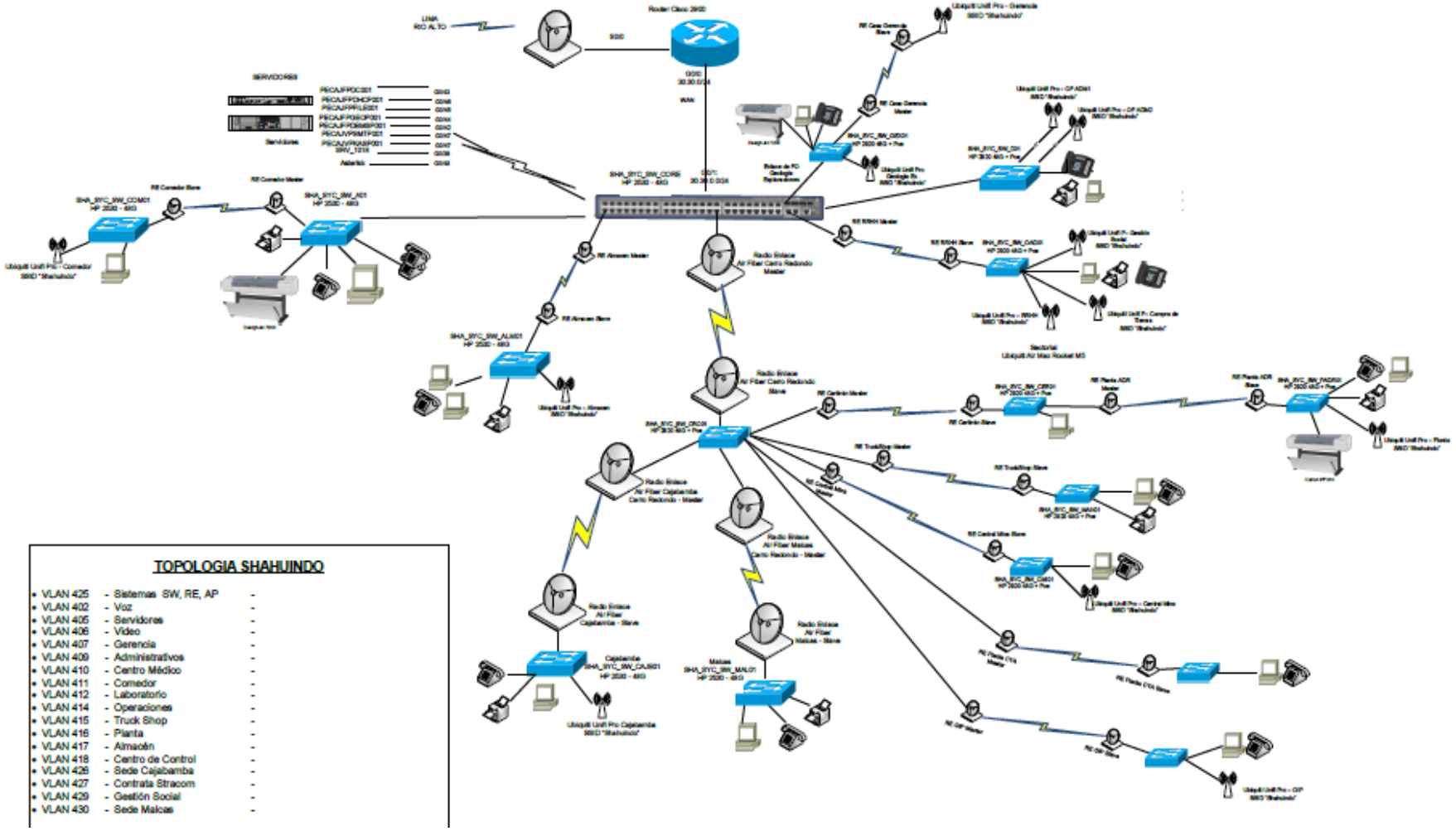


Figura N° 17. Diagrama de red de datos de la minera

Tabla N° 6: Catálogo de APs de la minera

DEVICE NAME	IP ADDRESS	STATUS	MODEL	VERSION	CLIENTS	DOWN	UP	CHANNEL	ACTIONS ↔
AP_1ER_PISO_1		CONNECTED	UniFi AP-AC-Pro	3.9.19.8123	1	996 MB	214 MB	11 (ng), 44 (ac)	LOCATE
AP_1ER_PISO_2		CONNECTED	UniFi AP-AC-Pro	3.9.19.8123	1	59.2 MB	35.1 MB	6 (ng), 36 (ac)	LOCATE
AP_ALMACEN_CENTRAL		CONNECTED	UniFi AP-Pro	3.7.5.4969	2	17 MB	1.82 MB	1 (ng), 64 (na)	LOCATE
AP_CAJABAMBA		CONNECTED	UniFi AP-Pro	3.9.19.8123	0	16.1 MB	1.64 MB	6 (ng), 149 (na)	LOCATE
AP_CAMARAS_COMEDOR		CONNECTED	UniFi AP-AC-Pro	3.9.19.8123	4	6.08 MB	8.95 MB	1 (ng), 157 (ac)	LOCATE
AP_CASA_GERENCIA		CONNECTED	UniFi AP-AC-Pro	3.9.19.8123	0	30.8 KB	19.3 KB	1 (ng), 36 (ac)	LOCATE
AP_CENTRAL_MINA		CONNECTED	UniFi AP-AC-Pro	3.9.19.8123	0	0 B	0 B	11 (ng), 44 (ac)	LOCATE
AP_COMPRA_TIERRAS		CONNECTED	UniFi AP-Pro	3.8.14.6780	0	134 MB	408 MB	1 (ng), 149 (na)	LOCATE
AP_EXPLORACIONES		CONNECTED	UniFi AP-AC-Pro	3.9.19.8123	1	1.2 GB	72.9 MB	6 (ng), 36 (ac)	LOCATE
AP_GERENCIA_A		CONNECTED	UniFi AP-AC-Pro	3.9.19.8123	3	1.65 GB	225 MB	1 (ng), 36 (ac)	LOCATE
AP_GERENCIA_B		CONNECTED	UniFi AP-AC-Pro	3.9.19.8123	3	337 MB	34 MB	6 (ng), 149 (ac)	LOCATE
AP_GESTION_SOCIAL		CONNECTED	UniFi AP-Pro	3.9.3.7537	0	59.7 MB	23.1 MB	11 (ng), 149 (na)	LOCATE
AP_MODULO_A_1		CONNECTED	UniFi AP-Pro	3.9.19.8123	3	623 MB	81.7 MB	11 (ng), 44 (na)	LOCATE
AP_MODULO_A_2		CONNECTED	UniFi AP-AC-Pro	3.9.19.8123	0	34.6 MB	2.38 MB	6 (ng), 44 (ac)	LOCATE
AP_OPI		CONNECTED	UniFi AP-AC-Pro	3.9.19.8123	0	0 B	0 B	1 (ng), 149 (ac)	LOCATE
AP_PLANTA_PROCESOS		CONNECTED	UniFi AP-AC-Pro	3.9.19.8123	1	551 MB	21.4 MB	1 (ng), 36 (ac)	LOCATE
AP_STRACONGYM		CONNECTED	UniFi AP-Pro	3.9.3.7537	2	1.04 GB	48.6 MB	11 (ng), 149 (na)	LOCATE
AP_TALENTO_HUMANO		CONNECTED	UniFi AP-Pro	3.9.3.7537	4	893 MB	117 MB	6 (ng), 149 (na)	LOCATE

3.2. Análisis de las herramientas de monitorización actuales

En la actualidad, la monitorización de la infraestructura de red se realiza a nivel de hardware dedicado (IDS e IPS de CISCO) y de algunas herramientas Open Source implementadas (como NAGIOS), 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 de la minera.

3.3. Selección de entorno aislado para pruebas

Debido a la complejidad de la infraestructura tecnológica de toda la minera y de acuerdo a los objetivos propuestos en la presente investigación, fue 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.

3.4. Alineamiento de los objetivos de TI con los objetivos de COBIT 5.0

3.4.1. Definición de los objetivos organizacionales

Primero se identificaron los objetivos organizacionales de la minera en relación al propósito de este estudio. Es importante mencionar, que éstos fueron definidos teniendo en cuenta las normas y políticas internas de la minera, así como de los objetivos internos que define y persigue el área de TI para el desarrollo de sus funciones.

Los objetivos organizacionales identificados fueron:

- OBJETIVO A: Lograr una expansión estratégica de los procesos de la minera.

- OBJETIVO B: Lograr el reconocimiento a la excelencia en cuanto a la atención y servicios brindados en la minera.
- 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 minera.
- 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.

3.4.2. Alineamiento entre los objetivos organizacionales y las metas corporativas definidas por Cobit 5

Para lograr el alineamiento entre los objetivos organizacionales de la minera y las metas corporativas definidas por Cobit 5, se tomó como referencia los mapeados de alineamiento descritos en el framework de Cobit 5.0, el mismo que se muestra en el Anexo 1. Cobit 5.0 plantea 17 metas corporativas que pueden ser logradas con el apoyo de la implementación de procesos de TI.

Como resultado del análisis realizado en un trabajo cooperativo con el personal de TI de la minera, el resultado de este alineamiento se muestra en la tabla siguiente.

Tabla N° 7: Alineamiento de los objetivos organizacionales de la minera con las metas corporativas definidas en COBIT

Objetivos organizacionales de la minera		**Metas corporativas de Cobit 5.0 (1)**	
Código	**Descripción**	**Número**	**Descripción**
A	Lograr una expansión estratégica de los procesos de la minera.	2	Cartera de productos y servicios competitivos.
B	Lograr el reconocimiento a la excelencia en cuanto a la atención y servicios brindados en la minera	6	Cultura de servicio orientada al cliente.
C	Asegurar el cumplimiento de las políticas y normas internas.	15	Cumplimiento con las políticas internas.
D	Asegurar el cumplimiento de las políticas y normas externas que rijan los procesos de TI aplicados.	4	Cumplimiento de leyes y regulaciones externas.
E	Asegurar la optimización y funcionalidad de los procesos implementados en la minera.	11	Optimización de la funcionalidad de los procesos de negocio.
F	Asegurar el resguardo de los activos mediante la gestión de riesgos.	3	Riesgos de negocio gestionados (salvaguarda de activo).
G	Mantener la continuidad y disponibilidad de los servicios brindados.	7	Continuidad y disponibilidad del servicio de negocio.
H	Tomas decisiones estratégicas en base a información confiable.	9	Toma estratégica de Decisiones basadas en información.
I	Asegurar la capacitación al personal para el logro de los objetivos establecidos.	16	Personas preparadas y motivadas.

(1) El código y la descripción de las metas corporativas de Cobit 5 se obtuvieron del anexo 1

3.4.3. Justificación del alineamiento entre los objetivos organizacionales y las metas corporativas definidas por Cobit 5

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 minera 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 minera 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 minera 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 minera, asegurando así el resguardo de los activos. El objetivo 3 que propone COBIT se relaciona directamente.

Objetivo "H" a objetivo 7

Este es una de las principales iniciativas estratégicas de la minera 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 define en su objetivo 7.

Objetivo "I" a objetivo 9

A fin de tomar decisiones acertadas y eficientes que favorezcan a la minera, 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 "J" 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.

3.4.4. Alineamiento de las metas corporativas seleccionadas con las metas relacionadas con TI, según Cobit 5.0

Como resultado de la tarea anterior, se pudo identificar que las metas corporativas seleccionas de Cobit 5.0, relacionadas con el propósito de la investigación fueron: 2, 3, 4, 6, 7, 9, 11, 15, y 16.

Utilizando el Anexo 1, se realizó el alineamiento y selección de las metas relacionadas con TI, según Cobit 5.0. Los resultados de esta tarea se muestran en las tablas siguientes. Debe tenerse en cuenta, que este alineamiento considera la existencia de una relación principal ("P") o una secundaria ("S") entre ambos constructos relacionados.

Tabla N° 8: Alineamiento de la meta corporativa 2 con las metas relacionadas con TI, según Cobit 5.0

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**

Tabla N° 9: Alineamiento de la meta corporativa 3 con las metas relacionadas con TI, según Cobit 5.0

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**

Tabla N° 10: Alineamiento de la meta corporativa 4 con las metas relacionadas con TI, según Cobit 5.0

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**

Tabla N° 11: Alineamiento de la meta corporativa 6 con las metas relacionadas con TI, según Cobit 5.0

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**

Tabla N° 12: Alineamiento de la meta corporativa 11 con las metas relacionadas con TI, según Cobit 5.0

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**

Tabla N° 13: Alineamiento de la meta corporativa 9 con las metas relacionadas con TI, según Cobit 5.0

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**

Tabla N° 14: Alineamiento de la meta corporativa 11 con las metas relacionadas con TI, según Cobit 5.0

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**

Tabla N° 15: Alineamiento de la meta corporativa 15 con las metas relacionadas con TI, según Cobit 5.0

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**

Tabla N° 16: Alineamiento de la meta corporativa 16 con las metas relacionadas con TI, según Cobit 5.0

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**

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 las siguientes metas 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° 17: Metas de TI seleccionadas a las necesidades de la minera

Perspectiva	Metas de TI Cobit
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

3.4.5. Justificación de las metas de TI seleccionadas

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 minera 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.

3.4.6. Identificación de métricas para las metas de TI

Para cada meta de TI seleccionada se identificaron sus métricas o indicadores que verifican el cumplimiento de las mismas.

Tabla N° 18: Métricas relacionadas con las metas de TI seleccionadas, según COBIT 5

Perspectiva	Objetivos de TI	METRICAS
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 negocio	Nivel de concienciación y comprensión de la alta dirección del negocio sobre las posibilidades de innovación TI
		Nivel de satisfacción de los interesados con los niveles de experiencia e ideas de innovación de TI

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.

3.5. Análisis de procesos de COBIT aplicables

El propósito de esta fase es llegar a identificar a los procesos habilitadores de acuerdo a la metodología de la cascada de objetivos de control definida por Cobit 5, tomando como insumo los resultados de la fase anterior, que son las metas de TI seleccionadas.

De acuerdo a lo propuesto por Cobit 5, para cada objetivo de TI le corresponden procesos habilitadores que serán analizados a fin de realizar un primer filtro que determinará su correcta aplicabilidad de acuerdo al propósito de esta investigación. Luego, se procederá a realizar un segundo filtro de los procesos habilitadores (por dominio), relacionados a la seguridad de la información, de tal manera que justifiquen el logro final de los objetivos de la investigación.

3.5.1. Aplicación de los procesos habilitadores

Como resultado de la tarea anterior, se identificó que las metas de TI Cobit, relacionadas al propósito de la investigación son: 2, 4, 7, 8, 9, 10, 11, 14, 15 y 17.

Para cada meta de TI seleccionada se procedió 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:

Meta de TI 2: Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas

Tabla N° 19: Procesos habilitadores para la meta 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**

Meta de TI 4: Riesgos de negocio relacionados con las TI gestionados

Tabla N° 20: Procesos habilitadores para la meta 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 Transición	**S**
	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**

Meta de TI 7: Entrega de servicios de TI de acuerdo a los requisitos del negocio

Tabla N° 21: Procesos habilitadores para la meta 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**

Meta de TI 8: Uso adecuado de aplicaciones, información y soluciones tecnológicas

Tabla N° 22: Procesos habilitadores para la meta 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**

Meta de TI 9: Agilidad de las TI

Tabla N° 23: Procesos habilitadores para la meta 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**
	Gestionar la Definición de Requisitos	**S**

Construir, Adquirir e Implementar (BAI)	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**

Meta de TI 10: Seguridad de la información, infraestructuras de procesamiento y aplicaciones

Tabla N° 24: Procesos habilitadores para la meta 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**

Meta de TI 11: Optimización de activos, recursos y capacidades de las TI

Tabla N° 25: Procesos habilitadores para la meta 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**

Meta de TI 14: Disponibilidad de información útil y relevante para la toma de decisiones

Tabla N° 26: Procesos habilitadores para la meta 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**

Meta de TI 15: Cumplimiento de TI con las políticas internas

Tabla N° 27: Procesos habilitadores para la meta 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**

Meta de TI 17: Conocimiento, experiencia e iniciativas para la innovación de negocio

Tabla N° 28: Procesos habilitadores para la meta 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**

3.5.2. 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° 29 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 e Implementar (BAI)	Gestionar la Disponibilidad y la Capacidad
	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

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 minera, así como de los objetivos internos que define y persigue el área de TI 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.

3.6. Seguridad de la Información según el enfoque de COBIT 5

3.6.1. Identificación de los procesos Cobit relacionados a la seguridad de la información

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 minera 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 de datos 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° 30 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

3.6.2. 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 TI de la minera.

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 minera. 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:

a. 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 de datos, 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.

b. 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 minera, 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 optima 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.

c. 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.

d. 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.

e. 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 minera.

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.

f. 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° 31 Procesos habilitadores de seguridad de la información seleccionados con sus 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 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

3.7. Definición de las herramientas OSSIM 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 de los procesos seleccionados en la etapa anterior. Se analizaró las funciones esenciales de seguridad que brinda como consola única, así como también, la utilidad de cada una de ellas.

Las sunciones seleccionadas de OSSIM necesarias para cumplir con el propósito de la investigación fueron las siguientes:

a. Descubrimiento de activos
b. Evaluación de vulnerabilidades
c. Detección de intrusiones
d. Monitoreo del comportamiento
e. SIEM

El flujo de trabajo con OSSIM se muestra a continuación:

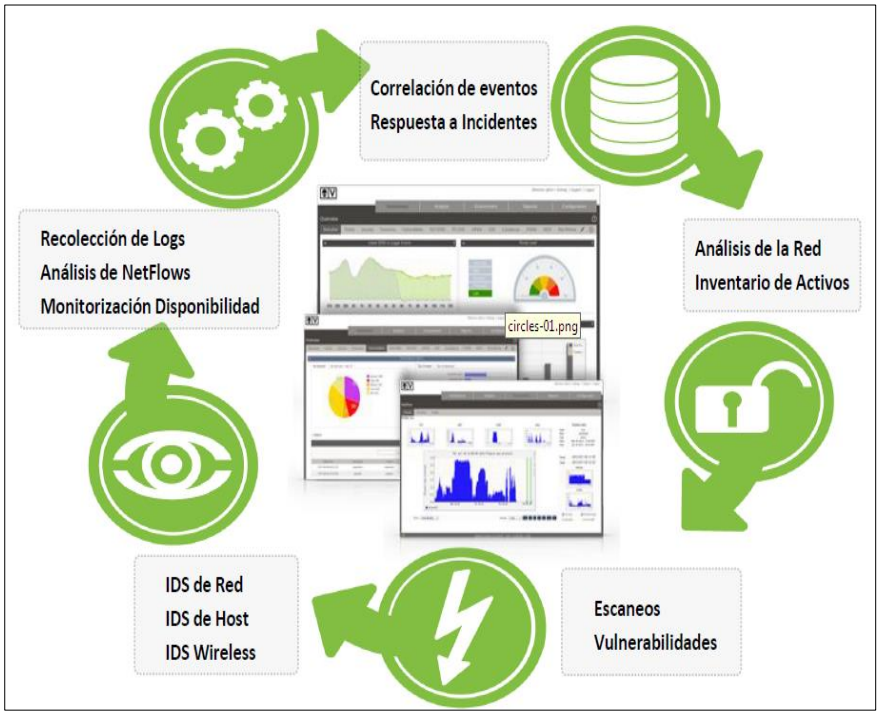


Figura N° 18. Flujo de trabajo con OSSIM

3.8. 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.

3.8.1. Identificación de los indicadores para los procesos de COBIT seleccionados

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:

a. Gestión de la disponibilidad y capacidad
b. Gestión de los activos
c. Gestión de la configuración
d. Gestión de incidentes de servicio
e. Gestión de servicios de seguridad
f. Gestión de las operaciones

Según ISACA (2012), cada proceso habilitador propuesto en el marco de referencia cuenta con indicadores o metricas relacionadas que facilitan su evaluacion en base a la informacion 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 continuacion se basan en los objetivos organizacionales y en la herramienta de gestion, quien se encargara de obtener los valores deseados.

a. Gestion de la disponiblidad 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 limites planificados.

b. Gestión de los activos

- Número de activos no utilizados.
- Número de activos obsoletos.

c. Gestión de la configuración

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

d. 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.

e. 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.

f. Gestión de las 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.

Estos son los indicadores evaluados durante la fase de implementación y, su monitoreo se realizó con la plataforma Open Source propuesta.

3.8.2. Integración de las funciones de seguridad y herramientas de soporte de OSSIM

Las funciones y herramientas OSSIM seleccionadas para lograr los indicadores seleccionados fueron:

a. 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)

b. Evaluación de vulnerabilidades

- OPENVAS (Sistema abierto de evaluación de vulnerabilidades)

c. Detección de intrusiones

- SNORT (Sistema de detección de intrusiones)
- OSSEC (Sistema de detección de intrusiones basada en host)
- KISMET (Detector de redes inalámbricas, snifer e IDS)

d. 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)

e. SIEM

- Correlación
- Directivas
- Cálculo de riesgo
- Informes

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

3.9. Implementación de la solución

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.

El siguiente procedimiento desarrollado en 8 fases, fue 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 minera. A continuación, se describe cada fase de la implementación:

3.9.1. Fase 1: Definición del tramo de red y recolección de información en base a la topología lógica 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.).

Procedimiento:

- 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:

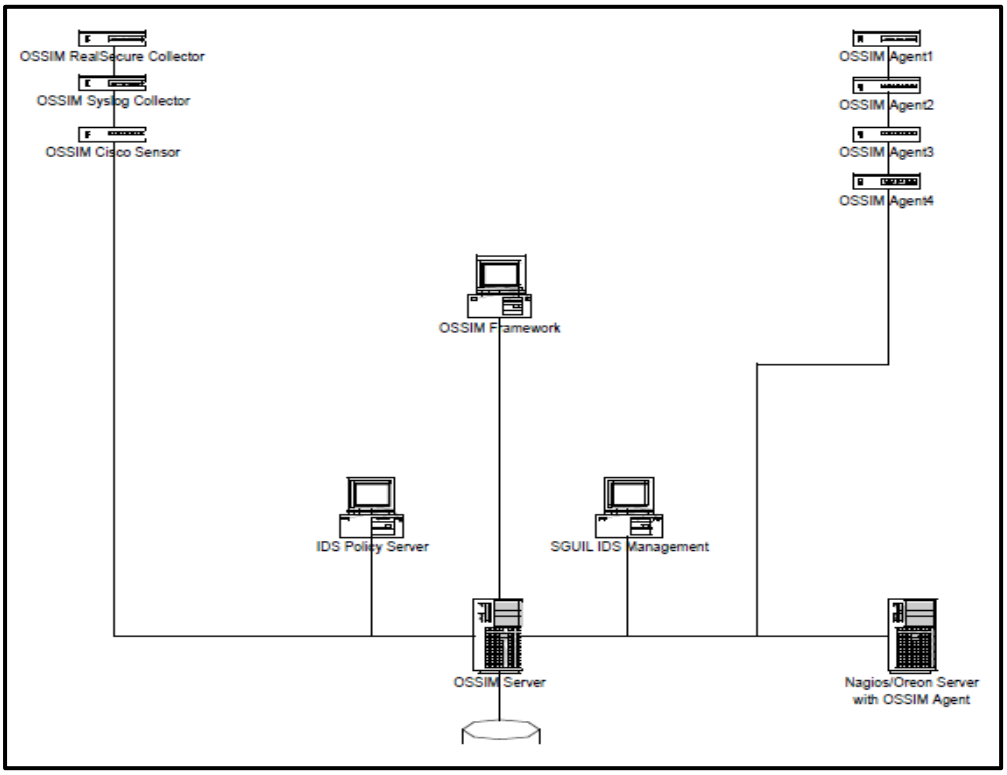


Figura N° 19. Ejemplo de aplicación de OSSIM distribuido

Fuente: (Karg, 2006)

Resultados:

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

3.9.2. Fase 2: Preparación 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, fue 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 necesario 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 de datos y preparar, junto con el administrados 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.

3.9.3. Fase 3: Instalación 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 procedió 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.).

Procedimiento:

- 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.

3.9.4. Fase 4: Instalación y configuración 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.

Procedimiento:

- 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.

3.9.5. Fase 5: Definición de políticas 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 de datos.
- 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.

3.9.6. Fase 6: Configuración de tickets de incidencia y pruebas de envío

La definición e implementación de políticas de seguridad en la plataforma OSSIM deja casi al sistema en completo funcionamiento. Sin embargo, las alertas producidas deben 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.

Procedimiento:

- 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.

3.9.7. Fase 7: Análisis de cuadros de mando integrados

En esta fase, se analizó 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.

Procedimiento:

- 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.

3.9.8. Fase 8: Evaluación final del impacto alcanzado

Finalmente, se realizará una evaluación de la situación actual en la red de datos 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.

3.10. 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.

3.10.1. 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.

Proceso habilitador: 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° 20. 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

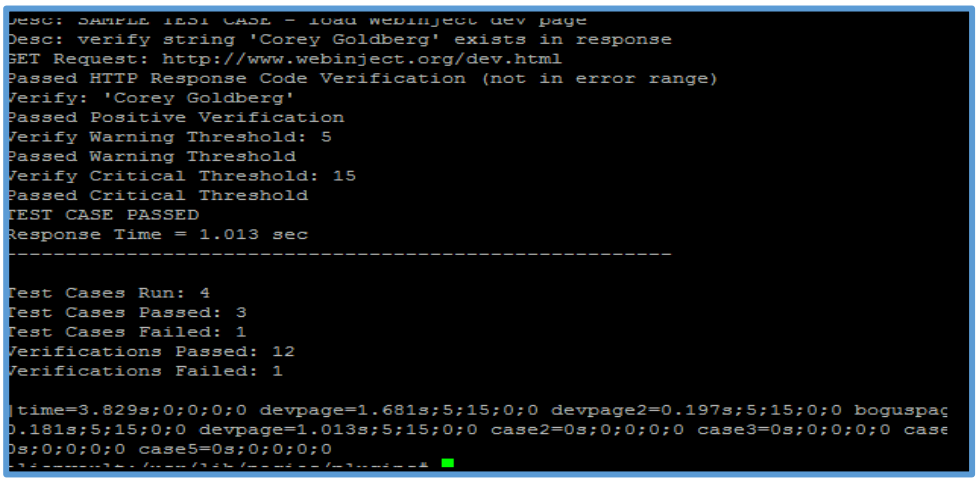


Figura N° 21. Webinject integrado a OSSIM como plugin de Nagios
Fuente: Resultados obtenidos por OSSIM

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° 22. 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 ayudarán a tomar una decisión acertada para evitar que el equipo se sobrecargue y los servicios dejen de operar.

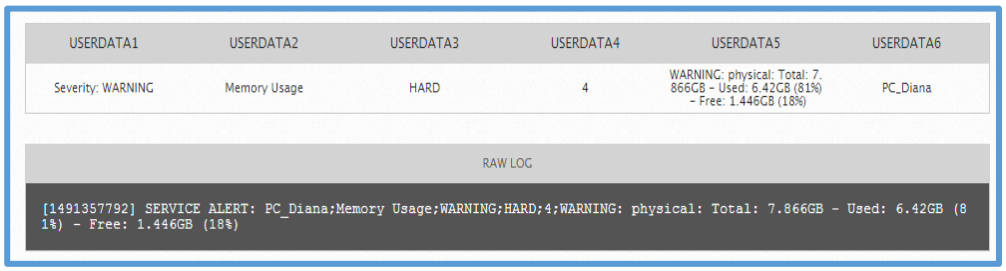


Figura N° 23. Monitoreo del uso de memoria RAM
Fuente: Resultados obtenidos por OSSIM

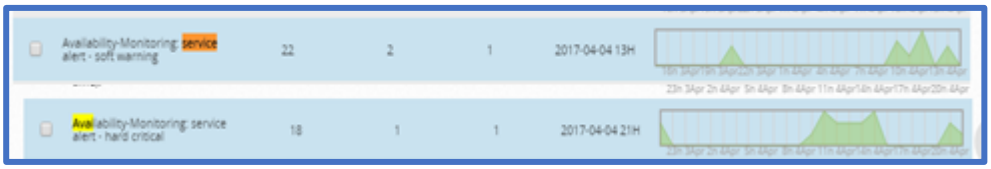


Figura N° 24. Número de eventos de disponibilidad de hardware hay en red
Fuente: Resultados obtenidos por OSSIM

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.

Proceso habilitador: GESTIÓN DE ACTIVOS

4. Número de activos no utilizados

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

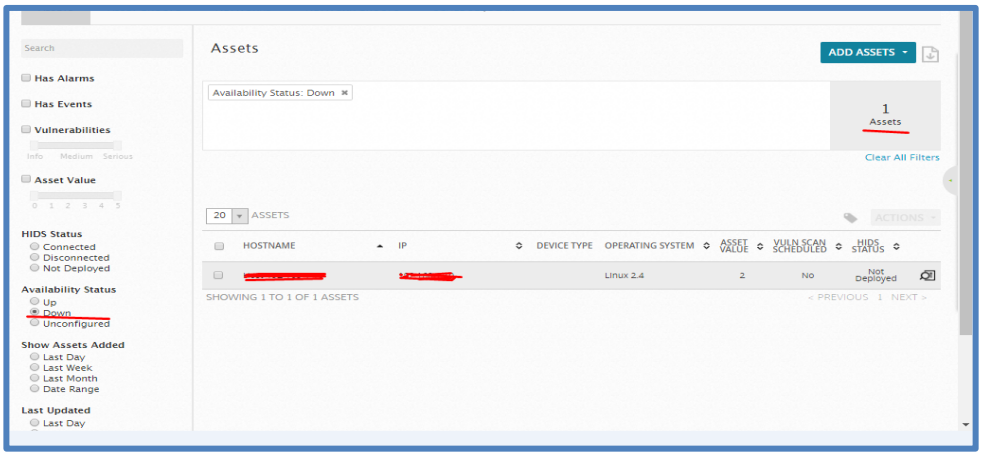


Figura N° 25. Descubrimiento de activos Ossim
Fuente: Resultados obtenidos por OSSIM

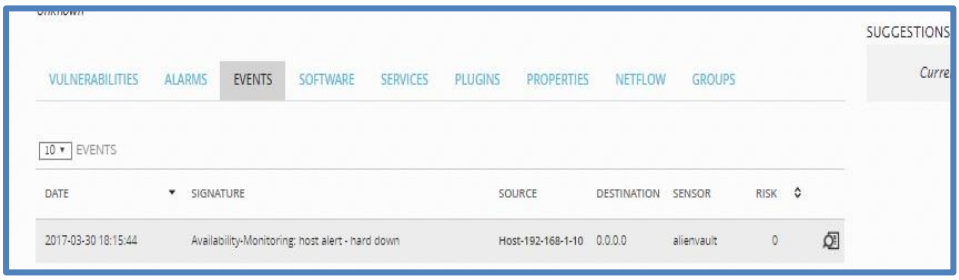


Figura N° 26. Detalle de eventos ocurridos en nuestro equipo
Fuente: Resultados obtenidos por OSSIM

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.

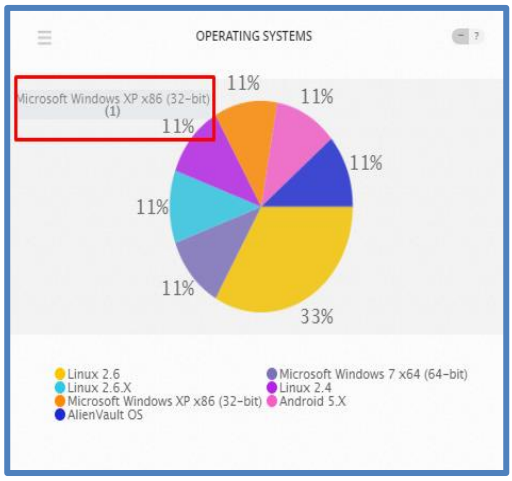


Figura N° 27. Dashboard según sistema operativo de los equipos en red
Fuente: Resultados obtenidos por OSSIM

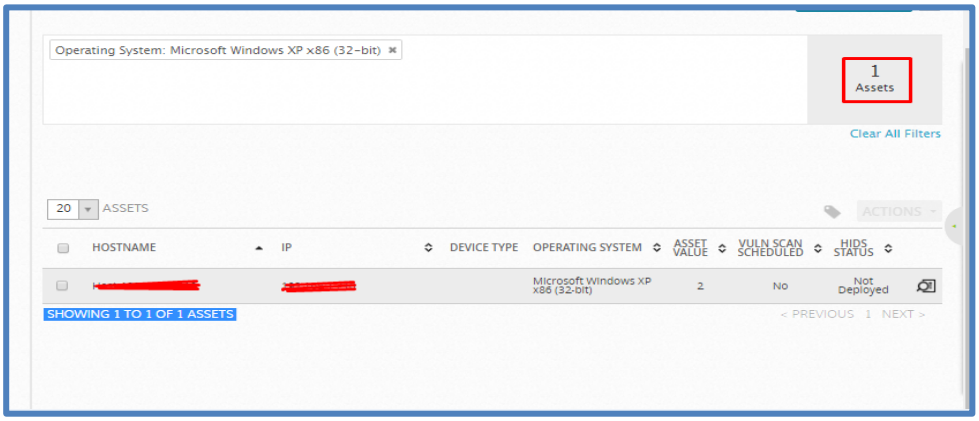


Figura N° 28. Consulta de número de equipos en red según sistema operativo
Fuente: Resultados obtenidos por OSSIM

Proceso habilitador: 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.

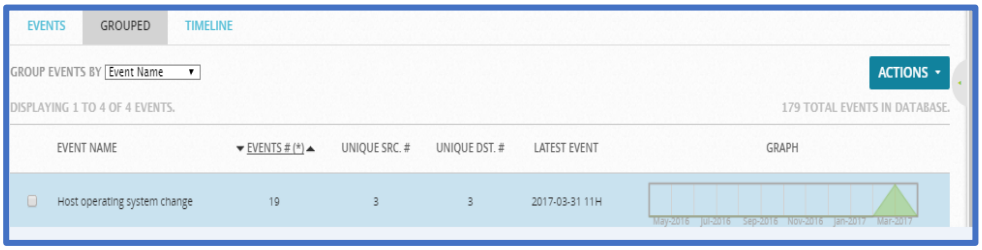


Figura N° 29. Número de eventos de cambio de sistema operativo en los hosts
Fuente: Resultados obtenidos por OSSIM

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

Proceso habilitador: 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.

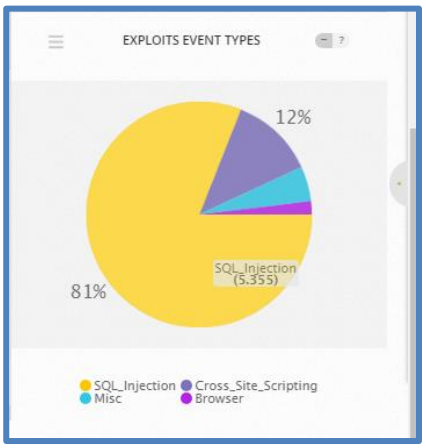


Figura N° 30. Número de eventos de exploits
Fuente: Resultados obtenidos por OSSIM

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

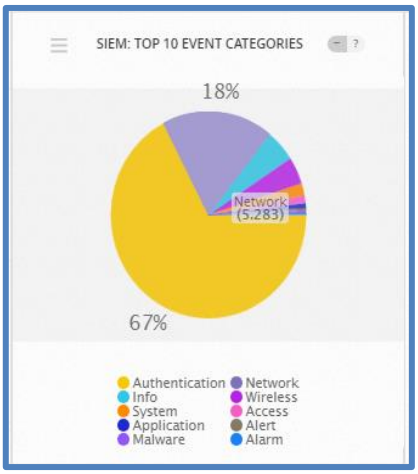


Figura N° 31. Eventos por categorías
Fuente: Resultados obtenidos por OSSIM

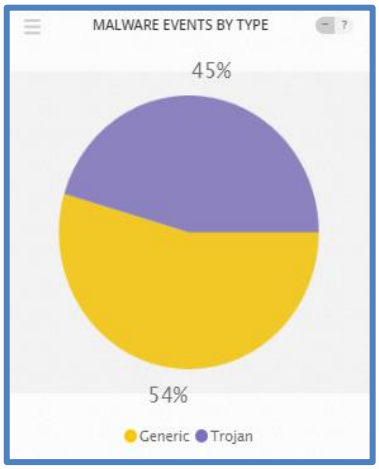


Figura N° 32. Eventos por Malware
Fuente: Resultados obtenidos por OSSIM

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.

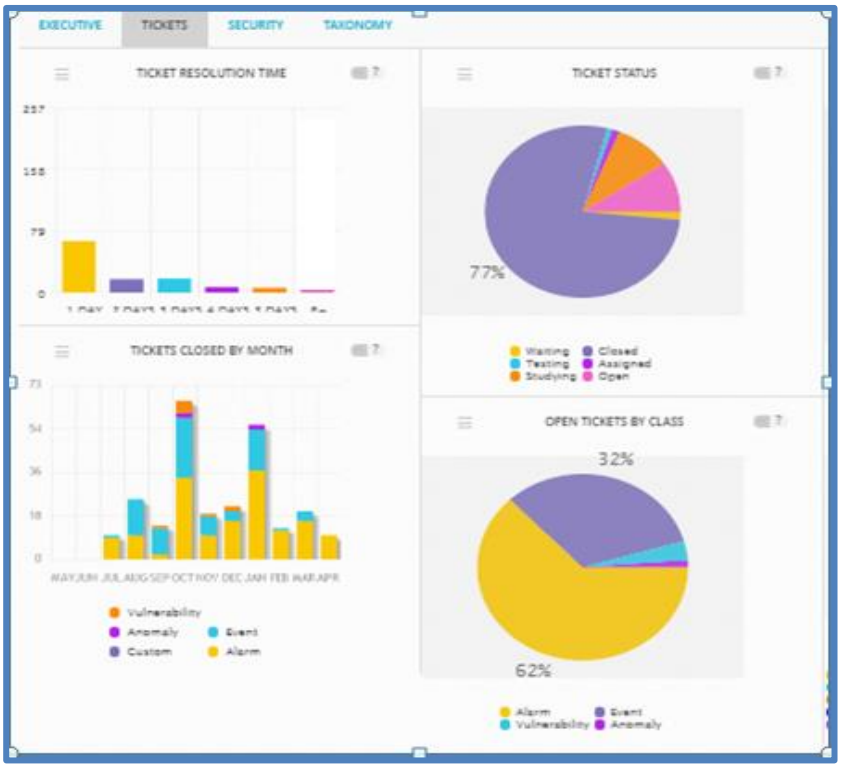


Figura N° 33. Dashboard de tickets de incidencias
Fuente: Resultados obtenidos por OSSIM

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.

Proceso habilitador: GESTIÓN DE SERVICIOS DE SEGURIDAD

10. Número de vulnerabilidades descubiertas

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

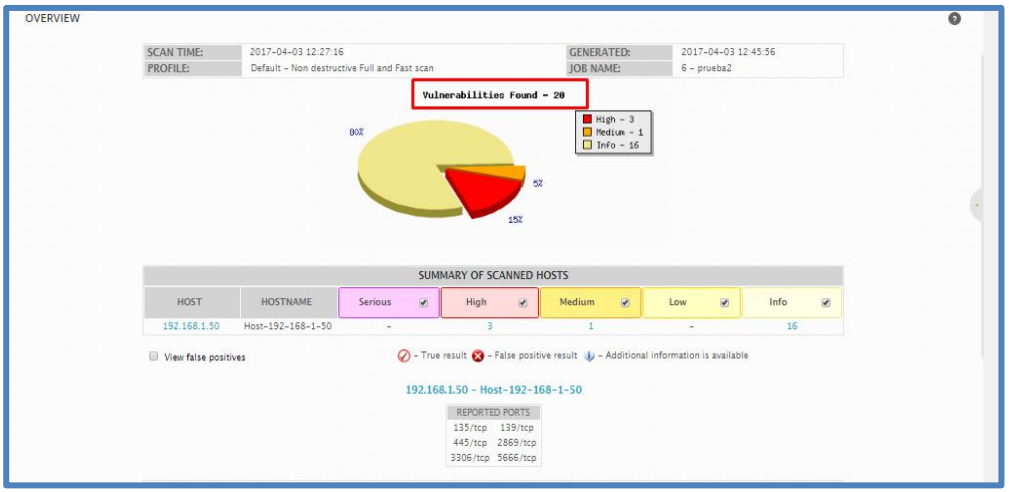


Figura N° 34. Vulnerabilidades detectadas por niveles
Fuente: Resultados obtenidos por OSSIM

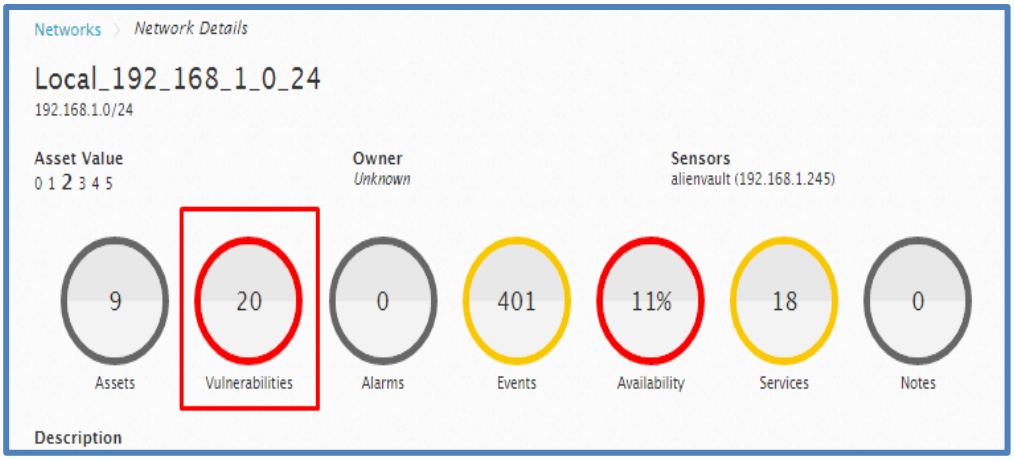


Figura N° 35. Número de vulnerabilidades en red
Fuente: Resultados obtenidos por OSSIM

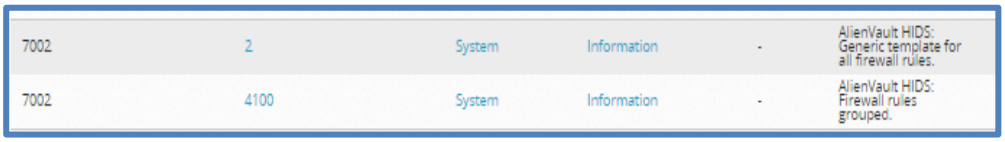
Como apreciamos en la imagen, al escanear nuestro entorno de red se detectaron 20 vulnerabilidades que deben ser solucionadas.

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 causada 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° 36. 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.

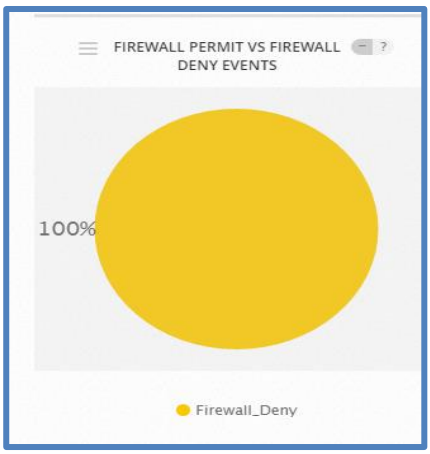
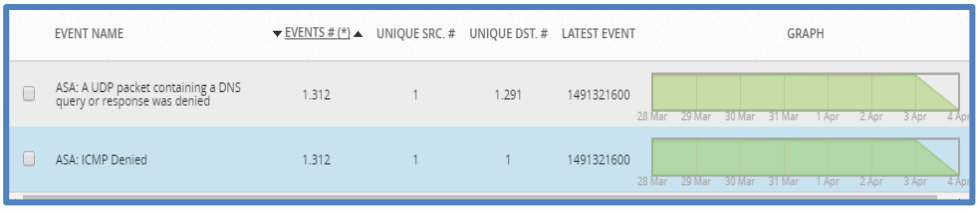


Figura N° 37. Eventos de accesos permitidos y denegados por el firewall
Fuente: Resultados obtenidos por OSSIM



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	
ASA: ICMP Denied	1.312	1	1	1491321600	

Figura N° 38. 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.

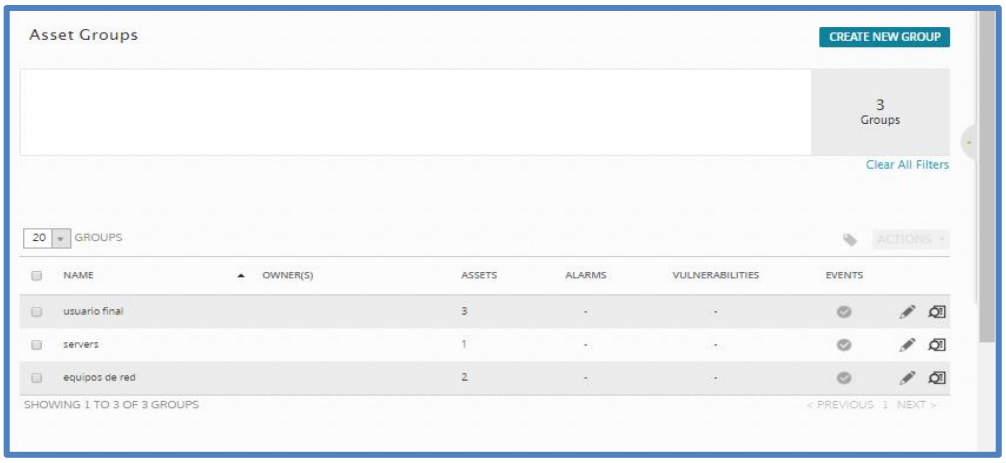


Figura N° 39. Grupos de activos en la red
Fuente: Resultados obtenidos por OSSIM

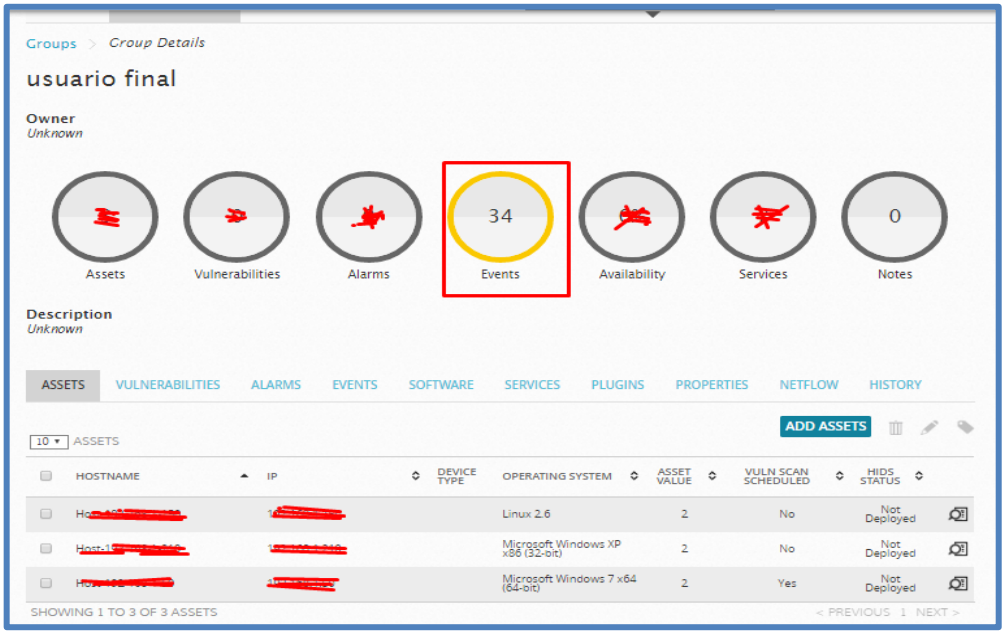


Figura N° 40. Activos de usuario final y eventos ocurridos en ese grupo de activos
Fuente: Resultados obtenidos por OSSIM

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.

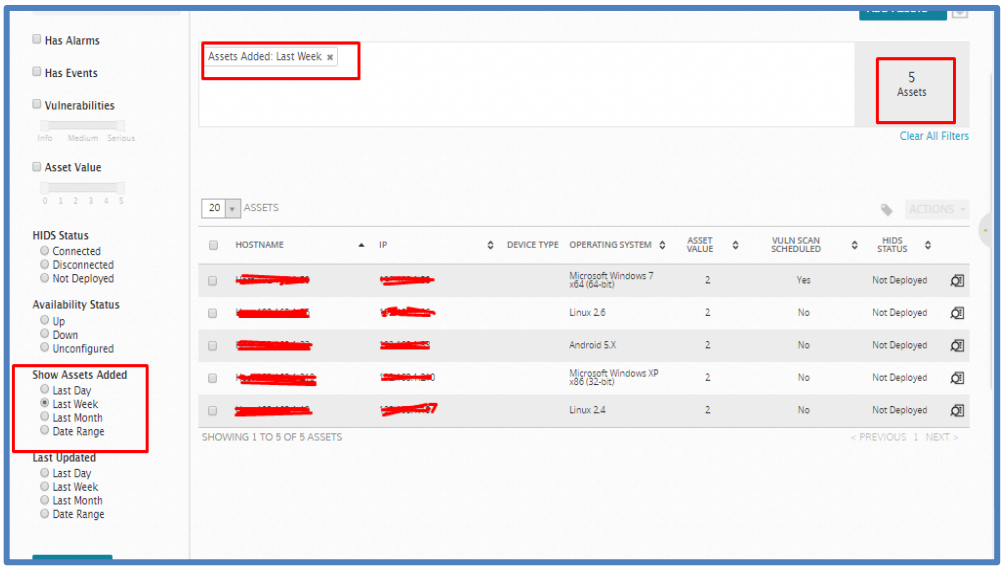


Figura N° 41. Activos agregados a la red últimamente
Fuente: Resultados obtenidos por OSSIM

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.

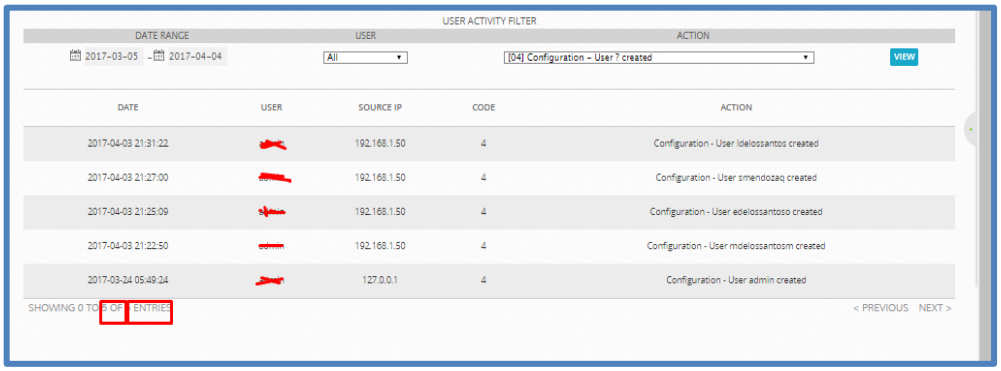


Figura N° 42. Actividad de usuarios
Fuente: Resultados obtenidos por OSSIM

Figura N° 43. 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.

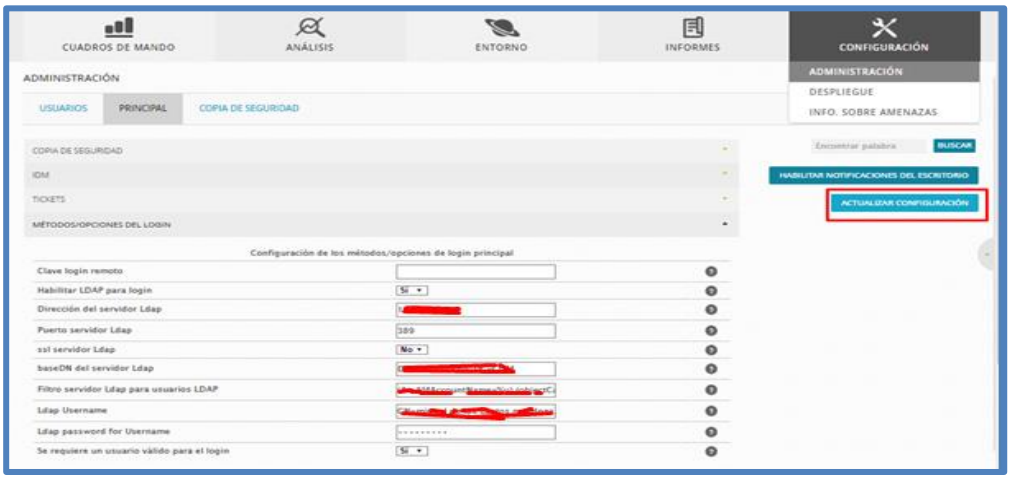


Figura N° 44. Integración OSSIM con LDAP
Fuente: Resultados obtenidos por OSSIM

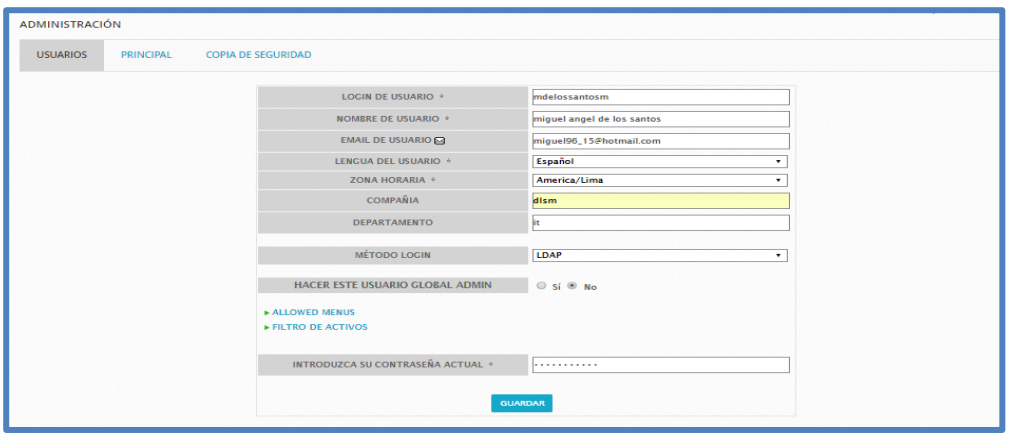


Figura N° 45. Creación de cuentas de usuarios mediante LDAP
Fuente: Resultados obtenidos por OSSIM

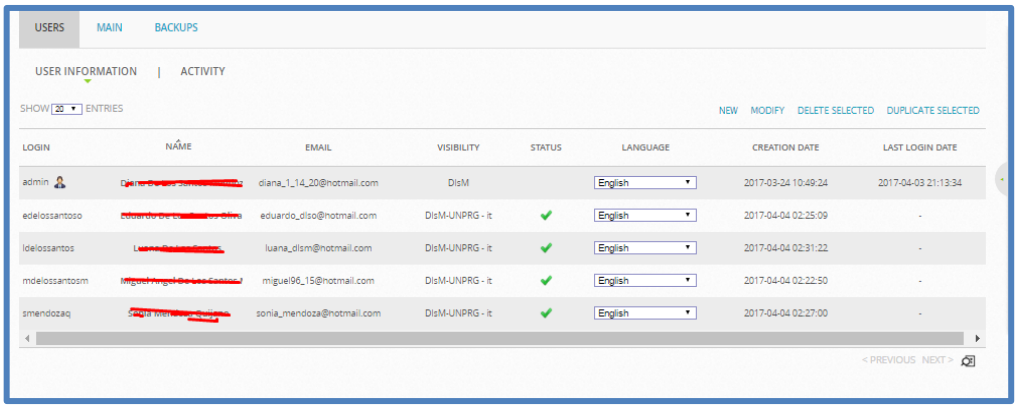


Figura N° 46. Números de cuentas de usuarios
Fuente: Resultados obtenidos por OSSIM

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)

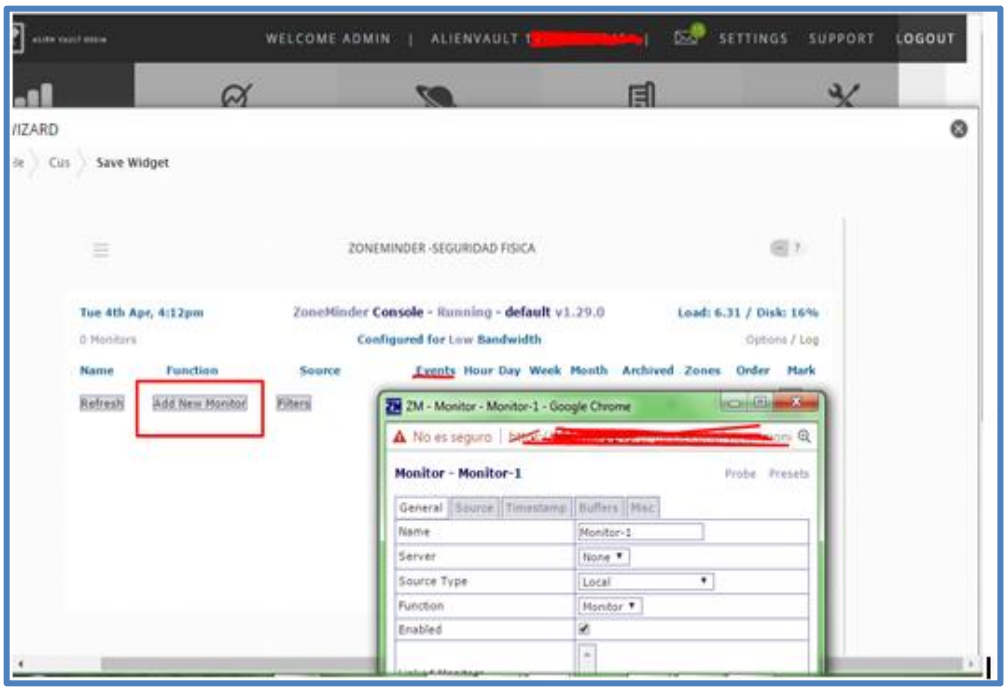


Figura N° 47. Integración ZoneMinder - OSSIM
Fuente: Resultados obtenidos por OSSIM

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.

Figura N° 48. UBS conectados / desconectados a los hosts
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.

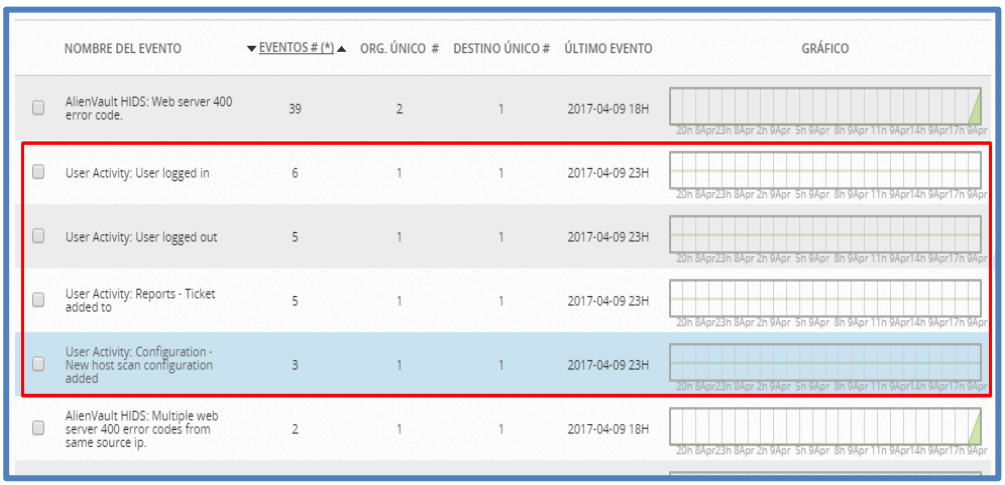


Figura N° 49. Cambios de configuración del sistema realizado por los usuarios
Fuente: Resultados obtenidos por OSSIM

Figura N° 50. Dashboard de actividad de usuario
Fuente: Resultados obtenidos por OSSIM

Proceso habilitador: 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° 51. Regla de Puerto de switch DOWN
Fuente: Resultados obtenidos por OSSIM

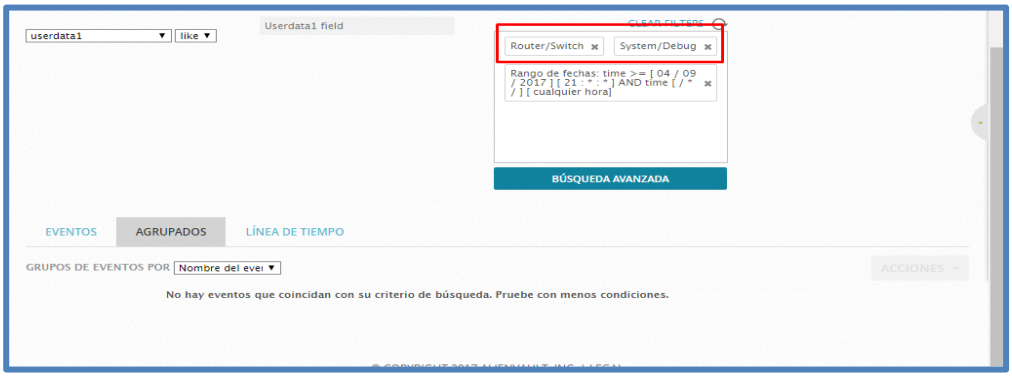


Figura N° 52. Número de eventos donde el puerto del swicht es DOWN
Fuente: Resultados obtenidos por OSSIM

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.

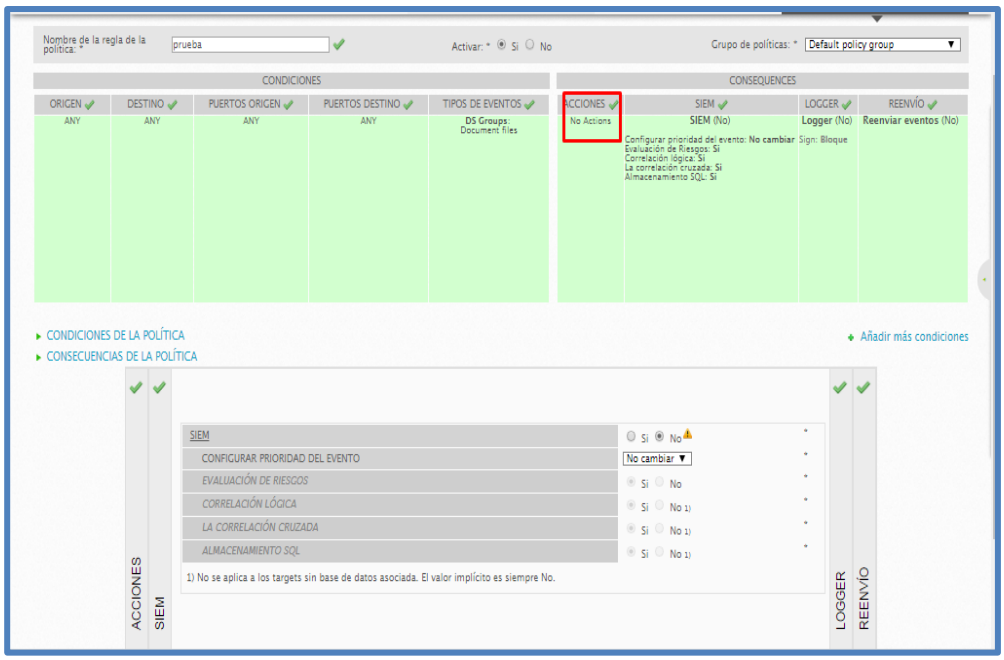


Figura N° 53. Políticas de Ossim
Fuente: Resultados obtenidos por OSSIM

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° 54. 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. Asi, cuando el sistema descubre una vulnerabilidad, relaciona esta informacion 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.

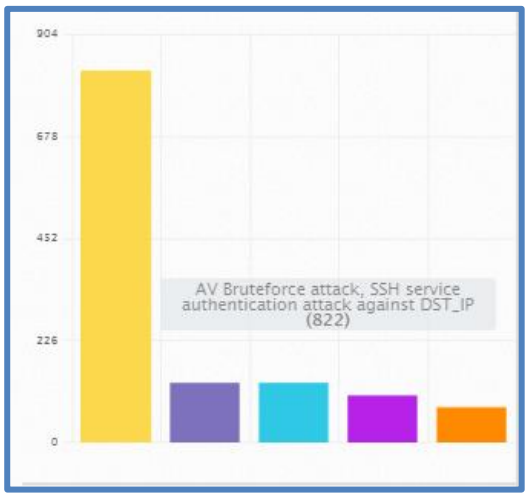


Figura N° 55. Ataques de fuerza bruta
Fuente: Resultados obtenidos por OSSIM

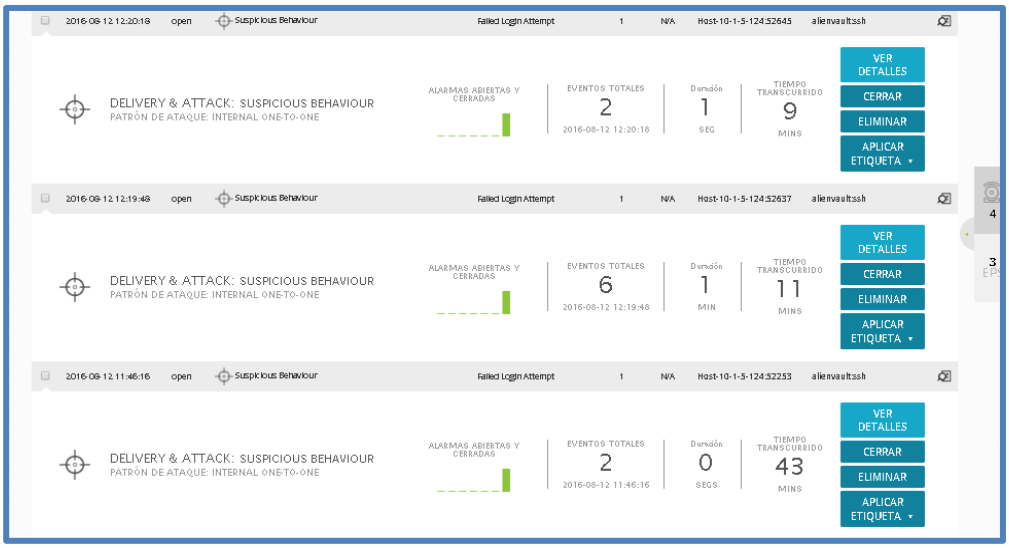


Figura N° 56. Alarmas de fuerza bruta
Fuente: Resultados obtenidos por OSSIM

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.

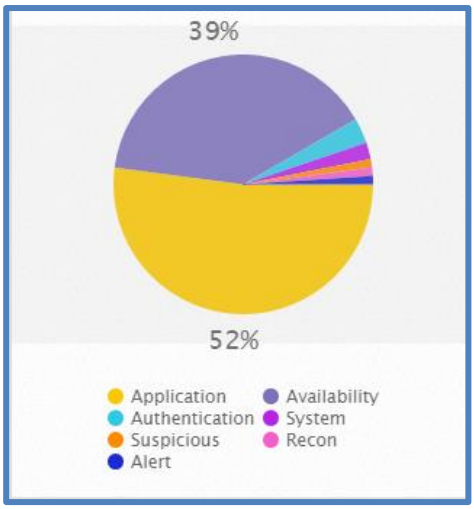


Figura N° 57. Eventos críticos en la red
Fuente: Resultados obtenidos por OSSIM

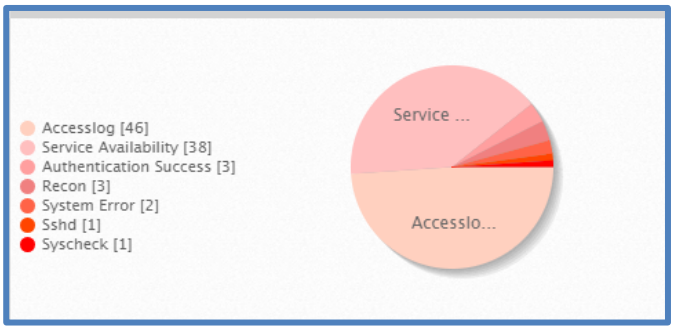


Figura N° 58. HIDS monitoreo
Fuente: Resultados obtenidos por OSSIM

3.11. 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.

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° 32: 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

3.11.1. 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.

Proceso habilitador: Gestión de la Disponibilidad y Capacidad

Tabla N° 33: 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, teniendo en cuenta los cambios en el entorno.	CUUMPLE
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 capacidad	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 y capacidad de todos los recursos relacionados con la información.	CUMPLE
	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

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.

Proceso habilitador: Gestión de activos

Tabla N° 34: 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
Optimiza	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 menores costos.	NO CUMPLE
	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

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.

Proceso habilitador: Gestión de la configuración

Tabla N° 35: Evaluación de cumplimiento para proceso habilitador BAI10: Gestión de la configuración

BAI10	Sub-actividades	Estado de cumplimiento
Establecer un modelo de	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	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

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.

Proceso habilitador: Gestión de operaciones

Tabla N° 36: Evaluación de cumplimiento para proceso habilitador DSS01: Gestión de operaciones

DSS01	Sub-actividades	Estado de cumplimiento
Ejecutar procedimientos	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 o que tiene una protección alternativa adecuada.	NO CUMPLE
	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

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.

Proceso habilitador: Gestión de incidencias de servicio

Tabla N° 37: 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	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, apro	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 apropiado, cuando sea necesario.	CUMPLE
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.

Proceso habilitador: Gestión de servicios de seguridad

Tabla N° 38: Evaluación de cumplimiento para proceso habilitador DSS05: Gestión de servicios de seguridad

DSS05	Sub-actividades	Estado de cumplimiento
Proteger contr	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
Gestionar la seguridad de los puestos de usuario	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

	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

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.

3.12. 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° 39: 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

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- El diagnóstico de la situación actual de la gestión de la seguridad de la información fueron evaluados en base a los objetivos de control que propone la ISO 27002, encontrándose la siguiente situación:

  En el dominio “Políticas del Sistema de gestión de la seguridad de la información”, aunque existe una política general establecida, hay deficiencias en el mapeo de procesos, y en el alineamiento de la política general y los controles.

  En el dominio “Controles de seguridad de información – Seguridad lógica”, se ha implementado adecuadamente la administración de derechos y perfiles de usuario, sin embargo, no se cumplen regularmente las revisiones periódicas de los derechos concedidos a los usuarios.

  En el dominio “Controles de seguridad de información – Seguridad física y ambiental - Áreas seguras/restringidas”, se han establecido controles efectivos para el control de acceso físico y señalización adecuada conforme a normativas específicas.

  En el dominio “Controles de seguridad de información – Seguridad física y ambiental - Seguridad y uso de equipos de cómputo”, los equipos críticos están ubicados en áreas seguras. Se han establecido salvaguardas contra amenazas y fallos, y el tendido de cable cumple con normas ANSI/TIA/EIA-569-A.

  En el dominio “Controles de seguridad de información – Gestión de activos – Inventario de activos”, se ha cumplido parcialmente con las exigencias de realizar y mantener un inventario de activos asociados a las TI y la asignación de responsabilidades para su protección.

  En el dominio “Controles de seguridad de información – Gestión de las comunicaciones y las operaciones – Procedimientos y responsabilidades operativas”, se han segregado funciones y recursos, logrando un nivel de control aceptable para proteger la confidencialidad. Además, se han establecido controles para la gestión de cambios en procesos TI.

En el dominio “Controles de seguridad de información – Gestión de las comunicaciones y las operaciones – Planificación y aceptación de sistemas, Protección contra software malicioso y Copias de seguridad”, Existen procedimientos para respaldos regulares y medidas contra software malicioso. Los controles implementados aseguran la recuperación de información esencial y reducen riesgos de códigos malintencionados.

En el dominio “Controles de seguridad de información – Gestión de las comunicaciones y las operaciones – Gestión de la seguridad de red”, Se ha implementado seguridad de red a un nivel aceptable, cumpliendo con criterios establecidos por la norma ISO.

En el dominio “Controles de seguridad de información – Gestión de incidentes de seguridad de la información”, Se utiliza el sistema SYSAID para gestionar incidentes de TI, cubriendo actividades desde el registro hasta el cierre, garantizando la trazabilidad y atención adecuada.

- El tramo de red seleccionado para la etapa experimental de la investigación fue una VLAN específica para este propósito, mediante pruebas piloto. Los criterios de selección de dicho tramo estuvo condicionada por la complejidad de la infraestructura tecnológica de la minera; así como, por las restricciones de acceso de las políticas emitidas desde la sede central ubicada en EEUU (Tahoe Resources). El tramo de red seleccionado consideró activos y áreas críticas suficientes para obtener información relevante para las pruebas piloto realizadas de las funcionalidades de OSSIM. La administración de la habilitó un puerto en el switch de capa3 (capa de distribución), donde se configuró la VLAN de gestión y servicio; a partir de ahí se configuró sobre los dispositivos de red de las áreas de finanzas y TI (áreas críticas de la minera) que cuentan con las especificaciones técnicas necesarias para la implementación de OSSIM.

- Aplicando las buenas prácticas de COBIT para la identificación de los procesos habilitadores que fueron seleccionados con el propósito de su evaluación, nos permitió determinar un conjunto de indicadores, los cuales fueron medidos en relación los criterios y funciones que están implementadas en OSSIM, encontrándose los siguientes resultados:

Gestión de la disponibilidad y capacidad: los indicadores seleccionados nos mostraron información de los picos transaccionales de la BD que superaron el rendimiento del sistema, así como incidentes de disponibilidad que se presentaron en un periodo de tiempo y que comprometieron el comportamiento de la red así como la disponibilidad de la RAM de los servidores de monitoreo.

Gestión de los activos: los indicadores seleccionados nos permitieron realizar un escaneo de los equipos que fueron parte de la red piloto, realizando un descubrimiento de equipo activos, así como los que no se encontraban en uso y obsoletos.

Gestión de la configuración: el indicador seleccionado nos permitió validar las desviaciones entre el repositorio de configuración y las configuraciones reales, para ellos se realizó el uso de Prads y Arpwatch, herramientas de OSSIM que nos permitió mantenernos alertas ante posibles cambios.

Gestión de las operaciones: los indicadores seleccionados nos permitieron identificar el número de incidentes causados por problemas operativos, así como nos mostró información importante sobre aplicaciones, disponibilidad y autenticación del sistema.

Gestión de incidentes de servicio: los indicadores seleccionados nos permitieron verificar los incidentes que se presentaron en la red, así como de manera automática la herramienta OSSIM generó un ticket para registrar cada incidencia y tener un control de los incidentes abiertos/cerrados y el tiempo de resolución, guardando un histórico de los mismos.

Gestión de servicios de seguridad: Con la herramienta Open Vas de OSSIM, nos permitió realizar el escaneo de vulnerabilidades en la red y equipos agregados a la red sin autorización, y LDAP nos permitió la creación de usuarios únicamente que pertenecen al dominio de la minera.

- Tras la selección del tramo idóneo para la prueba piloto y los procesos habilitadores e indicadores a medir, se procedió con la correcta configuración y pruebas de funcionamiento de la plataforma OSSIM (Servidor, sensor, BD y cuadro integral de mando) sobre la red de datos de la minera, obteniendo como resultado que la integración de 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.

- Aplicando los criterios de la norma ISO/IEC 15504 para evaluar los niveles de madurez de los procesos habilitadores seleccionados, se pudo lograr los siguientes resultados de integración de OSSIM – COBIT:

  Gestión de la disponibilidad y capacidad: se determinó que las subactividades de este proceso se cumplieron cabalmente, garantizando la correcta supervisión, evaluación, recolección y emisión de informes respecto a los eventos críticos que pudieron afectar la disponibilidad y capacidad de las operaciones de la minera, concluyendo que el proceso fue cubierto íntegramente por el modelo de gestión propuesto.

  Gestión de los activos: se determinó que las subactividades de este proceso fueron cubiertas parcialmente, tras la evaluación se validó un cumplimiento de hasta el 50%, donde se consideró el registro y la continua validación de la operatividad/vida útil de los activos funcionales de la minera, lo que nos dice que el proceso fue cubierto por el modelo de gestión propuesto.

  Gestión de la configuración: las subactividades de este proceso se cumplieron en su totalidad, validando un correcto modelo lógico de gestión de la configuración donde se incluye el registro, recopilación, clasificación y comparación de los elementos de configuración respecto a la base de referencia, garantizando su integridad y precisión, concluyendo acertadamente que el proceso fue cubierto íntegramente por el modelo de gestión propuesto.

  Gestión de operaciones: en su mayoría las subactividades de este proceso se cumplieron, validando una correcta supervisión de la infraestructura de TI a través de los procedimientos establecidos para el registro de activos, eventos, violaciones de umbrales y otros que puedan afectar la infraestructura de la minera así como de los datos que se procesan sobre ella, lo que nos dice que el proceso fue cubierto por el modelo de gestión propuesto.

Gestión de incidentes de servicio: se determinó que las subactividades se cumplieron en su gran mayoría, validando el registro, la clasificación y priorización de incidencias, permitiendo la investigación, diagnóstico y resolución, las mismas que fueron registradas para su análisis y emisión de informes a las partes interesadas, con lo que se concluyó que el proceso fue cubierto por el modelo de gestión propuesto.

Gestión de servicios de seguridad: se determinó que las subactividades se cumplieron parcialmente, tras la evaluación de las mismas se observó un cumplimiento de hasta el 50%, donde se consideró la correcta instalación y activación de herramientas de protección que resguarden los equipos de la red de datos de la minera contra incidentes de seguridad, estableciendo controles, políticas y protocolos de seguridad para filtrar y proteger el tráfico entrante/saliente de la red, concluyendo que el proceso fue cubierto por el modelo de gestión propuesto.

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 minera.

- 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.

BIBLIOGRAFÍA

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 informacion en TIC.* Chile: Departamento de tecnologias y sistemas de informacion.

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 informacion.

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.

ANEXOS

Anexo 1: Mapeo de las relaciones de las metas corporativas versus las metas de TI, según COBIT 5.0

			META CORPORATIVA																
			Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basada en Información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de .	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
META RELACIONADA CON LAS TI			**FINANCIERA**					**CLIENTE**					**INTERNA**					**APRENDIZAJE Y CRECIMIENTO**	
FINANCIERA	**1**	Alineamiento de TI y la estrategia de negocio	P	P	**S**			P	S	P	P	S	P	S	P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S

	6	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P						
CLIENTE	**7**	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S	
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S	
INTERNA	**9**	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P	
	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P			
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S	
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S	
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	S			S				S		S	P					
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S							
	15	Cumplimiento de TI con las políticas internas			S	S											P			
APRENDIZAJE y CRECIMIENTO	**16**	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S	
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P	

Fuente: (ISACA, 2012)

CONSTANCIA DE APROBACION DE ORIGINALIDAD DE TESIS

Según Res. N° 626-2021-CU

Yo, ERNESTO KARLO CELI ARÉVALO, asesor de tesis de las bachilleres en Ingeniería de Sistemas: **TAHNEE LILIBETH LUJÁN FLORES y VERÓNICA ELIZABETH HUANCAS SAMILLÁN**

TITULADA:

Gestión de la seguridad de la información de la infraestructura de red datos de la minera Shahuindo mediante OSSIM Y COBIT

Luego de la revisión exhaustiva del documento constato que la misma tiene un índice de similitud de **17**% verificable en el reporte de similitud del programa TURNITIN.

El suscrito analizó dicho reporte y concluyó que cada una de las coincidencias detectadas NO CONSTITUYEN PLAGIO. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Nacional Pedro Ruiz Gallo.

Se expide la presente según lo dispuesto en la RESOLUCION N° 626-2021-CU - Directiva para la evaluación de originalidad de los documentos académicos y de investigación, de la Universidad Nacional Pedro Ruiz Gallo.

Lambayeque, 29 de enero del 2024

Atentamente,

Tahnee Lilibeth Luján Flores
DNI. 45531579

Ing. Ernesto Karlo Celi Arévalo
DNI. 18068078

Verónica Elizabeth Huancas Samillán
DNI. 47246959

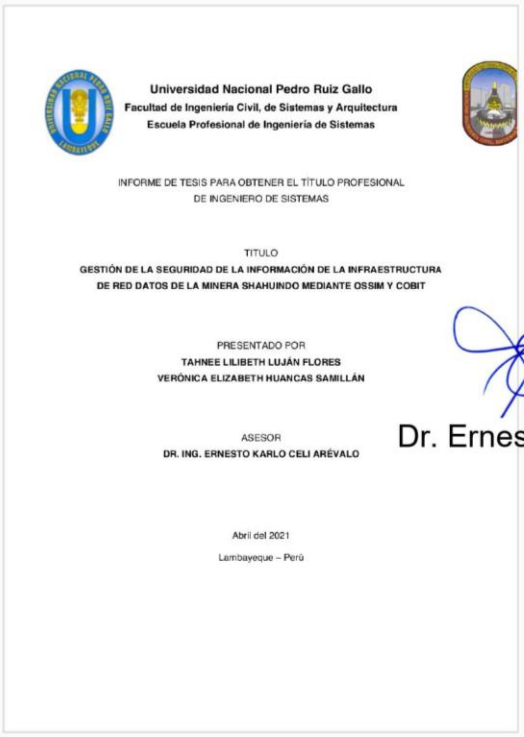
Se adjunta:
Recibo digital de Turnitin
Revisión de informe en Turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Tahnee Lujan & Verónica Huancas
Título del ejercicio:	Quick Submit
Título de la entrega:	Informe final de tesis
Nombre del archivo:	InformeFinalTesis.docx
Tamaño del archivo:	4.74M
Total páginas:	159
Total de palabras:	43,122
Total de caracteres:	235,978
Fecha de entrega:	29-ene.-2024 09:33a. m. (UTC-0500)
Identificador de la entre...	2281198699



Universidad Nacional Pedro Ruiz Gallo
Facultad de Ingeniería Civil, de Sistemas y Arquitectura
Escuela Profesional de Ingeniería de Sistemas

INFORME DE TESIS PARA OBTENER EL TÍTULO PROFESIONAL
DE INGENIERO DE SISTEMAS

TITULO
GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA INFRAESTRUCTURA
DE RED DATOS DE LA MINERA SHAHUINDO MEDIANTE OSSIM Y COBIT

PRESENTADO POR
TAHNEE LILIBETH LUJÁN FLORES
VERÓNICA ELIZABETH HUANCAS SAMILLÁN

ASESOR
DR. ING. ERNESTO KARLO CELI ARÉVALO

Abril del 2021
Lambayeque – Perú

Dr. Ernesto Celi Arévalo

Informe final de tesis

INFORME DE ORIGINALIDAD

17%	13%	6%	8%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

Dr. Ernesto Celi Arévalo

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	3%
2	pdfcoffee.com Fuente de Internet	2%
3	tesis.pucp.edu.pe Fuente de Internet	2%
4	dspace.udla.edu.ec Fuente de Internet	1%
5	manglar.uninorte.edu.co Fuente de Internet	<1%
6	repositorio.espe.edu.ec Fuente de Internet	<1%
7	repositorio.unprg.edu.pe:8080 Fuente de Internet	<1%
8	Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD Trabajo del estudiante	<1%
9	blplegal.net Fuente de Internet	

Dr. Ing. Ernesto Karlo Celi Arévalo

		< 1 %
10	docplayer.es Fuente de Internet	< 1 %
11	e-archivo.uc3m.es Fuente de Internet	< 1 %
12	Submitted to CONACYT Trabajo del estudiante	< 1 %
13	repositorio.ufpso.edu.co Fuente de Internet	< 1 %
14	Submitted to Universidad Pontificia Bolivariana Trabajo del estudiante	< 1 %
15	polux.unipiloto.edu.co:8080 Fuente de Internet	< 1 %
16	vbook.pub Fuente de Internet	< 1 %
17	Submitted to Universidad ICESI Trabajo del estudiante	< 1 %
18	Submitted to Universidad Andina del Cusco Trabajo del estudiante	< 1 %
19	Submitted to Universidad de Lima Trabajo del estudiante	< 1 %
20	repositorio.uta.edu.ec Fuente de Internet	

Dr. Ing. Ernesto Karlo Celi Arévalo

		< 1 %
21	repositorio.utc.edu.ec Fuente de Internet	< 1 %
22	repository.upb.edu.co Fuente de Internet	< 1 %
23	repositorio.uisrael.edu.ec Fuente de Internet	< 1 %
24	Submitted to Universidad Tecnica De Ambato-Direccion de Investigacion y Desarrollo , DIDE Trabajo del estudiante	< 1 %
25	Submitted to Universidad Europea de Madrid Trabajo del estudiante	< 1 %
26	Sussy, Bayona, Chauca Wilber, Lopez Milagros, and Maldonado Carlos. "ISO/IEC 27001 implementation in public organizations: A case study", 2015 10th Iberian Conference on Information Systems and Technologies (CISTI), 2015. Publicación	< 1 %
27	repositorio.unicauca.edu.co:8080 Fuente de Internet	< 1 %

Excluir citas	Activo	Excluir coincidencias	< 15 words
Excluir bibliografía	Activo		