

UNIVERSIDAD INTERNACIONAL SEK

DIGITAL SCHOOL

TRABAJO DE FIN DE CARRERA

TITULADO:

SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD (SIEM) DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD

INTERNACIONAL SEK DEL ECUADOR

Realizado por:

Ing. Jorge Danilo Añazco Bedón

Directora del proyecto:

Ing. Verónica Rodríguez Arboleda, MBA.

Como requisito para la obtención del título de: MAGISTER EN CIBERSEGURIDAD

QUITO, septiembre 2021

DECLARACION JURAMENTADA

Por la presente, yo, JORGE DANILO AÑAZCO BEDÓN, con cédula de ciudadanía N°. 1724515596, declaro bajo juramento, que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento. A través de esta declaración cedo mis derechos de propiedad intelectual de autora a la UNIVERSIDAD INTERNACIONAL SEK UISEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente

JORGE DANILO AÑAZCO BEDÓN

CC: 1724515596

DECLARACIÓN DE DIRECTOR DE TESIS

El presente que el presente trabajo de investigación titulado:

"SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD (SIEM) DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD INTERNACIONAL SEK DEL ECUADOR"

Realizado por:

Ing. Jorge Danilo Añazco Bedón

Como requisito para la obtención del título de

MÁSTER EN CIBERSEGURIDAD

Ha sido dirigido por mi persona a través de reuniones periódicas con la estudiante y cumple con todas las disposiciones que rigen los trabajos de titulación.

Ing. Verónica Rodríguez Arboleda,

MBA. DIRECTORA DEL PROYECTO

CC: 1707522312

LOS PROFESORES INFORMANTES

Los profesores informantes:

Ing, José Vinicio Freire Rumazo, Mgtr.

MSc Ing. Joe Carrión Jumbo, PhD

Después de revisar el trabajo, lo han calificado como apto para su defensa oral ante el tribunal examinador

El profesor informante:

Ing. Joe Carrión Jumbo, PhD

Ing, José Vinicio Freire Rumazo, Mgtr.

Quito, septiembre de 2021

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es de mi autoría, que se han citado las fuentes correspondientes y que en su desarrollo se respetaron las disposiciones legales vigente, que protegen los derechos

de autor.

Duren

Jorge Danilo Añazco Bedón

CC: 1724515596

AGRADECIMIENTO

A mi esposa Priscila por estar siempre a mi lado y ser un pilar fundamental para mi formación profesional, y a mis hijas Daniela y Alejandra les dedico este trabajo ya que por ellas tengo la determinación para cursar la maestría.

A mis padres Jorge y María que por su esfuerzo, sacrificio y paciencia pude estudiar la carrera que siempre me interesó, contando siempre con su apoyo incondicional en los momentos que más lo necesité.

A mi tía Enmita ya que fue una de las personas que ha confiado en mí dándome su cariño y apoyo para lograr mis objetivos.

A los docentes de la facultad Digital School de la Universidad Internacional Sek, por haber impartido sus conocimientos a lo largo de la preparación de esta maestría, de manera especial, a la Ing. Verónica Rodríguez Arboleda tutora de este proyecto de investigación quien me ha guiado con sus conocimientos, paciencia y rectitud como docente.

RESUMEN

In the following project, the implementation of a Security Information and Event Management System (SIEM) was carried out, due to the need to optimize and improve the cybersecurity of the technology infrastructure of the SEK International University, in addition control and monitoring procedures were defined of computer incidents that are detected through customized developments for monitoring with the availability module of the OSSIM AlienVault tool. Previously, with the 20 Center for Internet Security, an analysis was carried out to obtain indicators of the current state of the institution's information security, with which it was possible to determine the systems and unprotected areas that needed the immediate intervention of the module of availability or monitoring that the OSSIM AlienVault tool has integrated.

Finally, this document explains a guide for the development of a server and services monitoring script, which facilitates obtaining the necessary information to define alert states and notify when there is a risk in computer security.

Palabras claves: SIEM, OSSIM AlienVault, 20 controles de la CIS

ABSTRACT

In the following project, the implementation of a Security Information and Event Management System (SIEM) was carried out, due to the need to optimize and improve the cybersecurity of the technology infrastructure of the SEK International University, in addition control and monitoring procedures were defined of computer incidents that are detected through customized developments for monitoring with the availability module of the OSSIM AlienVault tool. Previously, with the 20 controls of the CIS Center for Internet Security, an analysis was carried out to obtain indicators of the current state of the institution's information security, with which it was possible to determine the systems and unprotected areas and which they needed the immediate intervention of the availability or monitoring module that has integrated the OSSIM AlienVault tool.

Finally, this document explains a guide for the development of a server and services monitoring script, which facilitates obtaining the necessary information to define alert states and notify when there is a risk in computer security.

Keywords: SIEM, OSSIM AlienVault, 20 CIS controls.

ÍNDICE DE CONTENIDOS

CAP	ÍTULO I	20
INT	ODUCCIÓN	20
1.	Planteamiento del Problema	20
1.	Formulación del Problema	
1.	Objetivo general	
1.	Objetivos específicos	
1.	Justificación	23
	Técnica	
	Social	
1.	Estado del arte	24
CAP	TULO II	27
MA	CO TEÓRICO	27
2.	Seguridad informática	27
	Amenaza informática	27
	Vulnerabilidad	27
	Impacto	
	Riesgo	
	Políticas de Seguridad	
2.	SIEM	

OSSIM AlienVault	29
2.3 20 Controles de la CIS	30
2.4 Script	33
Características	33
Lenguaje Shell	33
CAPÍTULO III	35
ANÁLISIS Y SITUACIÓN ACTUAL	35
3.1 Universidad Internacional Sek (UISEK)	35
Misión:	36
Visión:	36
Historia	36
3.2 Situación Tecnológica de la Universidad Internacional SEK	37
3.3 Descripción de la infraestructura	38
3.4 Usuarios	39
3.5 Operatividad de los portales o aplicativos web	39
3.6 Módulos críticos	40
Módulo de inicio de sesión	40
Módulo de hoja de vida e información del estudiante	40
Módulo de certificados	41
Módulo de Pagos	41
Módulo de notas y asistencia	42
3.7 Riesgos indirectos	43

3.8	20 0	controles de la CIS
3.8	8.1	Posible escenario de mejora
CAPÍT	ULO	9 IV
PROPL	JEST	^C A
4.1	Inst	alación/configuración de la herramienta OSSIM47
4.1	1.1	Instalación47
4.1	1.2	Configuración e instalación del OSSIM AlienVault61
4.2	Ges	stión de activos
4.3	Ges	stión de disponibilidad70
4.4	Ges	stión de notificaciones74
4.5	Ges	stión de vulnerabilidades77
4.6	Ges	stión de riesgos
4.7	Def	inición, desarrollo e implementación de scripts en el Módulo de Disponibilidad
	84	
4.7	7.1	Tipos de script según su funcionamiento
4.7	7.2	Scripts de monitoreo por servicio
4.7	7.3	Scripts de monitoreo en servidor (obtención de estados)
4.7	7.4	Scripts de monitoreo por análisis de datos
4.7	7.5	Scripts de monitoreo por interacción
4.7	7.6	Scripts de monitoreo por consumo de microservicios
4.8	Cre	ación de scripts para el módulo de Nagios91
4.8	8.1	Características de un script para funcionar con Nagios91

4.8.2	Agregar un nuevo comando-script a Nagios para monitoreo
4.9 Noti	ficaciones y alertas a través de Telegram96
4.9.1	Instalación telegram-cli en CentOS 897
4.9.2	Script de comunicación para envió de alerta y notificaciones por telegram-cli
	99
4.9.3	Script Telegram 100
4.9.4	Configuración Nagios para el envío de notificaciones o alertas por Telegram
	101
4.10 So	cripts desarrollados
4.10.1	Script para la obtención de la temperatura del sistema de enfriamiento de un
Data Cente	er 103
4.10.2	Script para la obtención de un archivo .csv donde se detalla número de
snapshots	de un hipervisor, para el análisis y él envió de los estados
4.10.3	Script que analiza el log de acceso del servicio de apache 105
4.10.4	Script que analiza los tamaños de los directorios y logs de la base de datos
Postgresql	107
4.10.5	Script que analiza el número de tickets de la mesa de servicio 108
CAPÍTULO	V
CONCLUSI	ONES Y RECOMENDACIONES
5.1 Con	clusiones110
5.2 Rec	omendaciones
BIBLIOGRA	AFÍA114

ÍNDICE DE FIGURAS

Figura 1: Infecciones de 'malware' en empresas de tres países latinoamericanos	20
Figura 2: Herramientas de OSSIM AlienVault	29
Figura 3: Modelo de relación OSSIM	30
Figura 4: 20 Controles de la CIS v7	32
Figura 5: Logo Universidad Internacional Sek	35
Figura 6: Inicio de sesión Portal Alumnos UISEK	40
Figura 7: Módulo de hoja de vida UISEK	41
Figura 8: Módulo de certificados UISEK	41
Figura 9: Módulo de pagos UISEK	42
Figura 10: Módulo de notas y asistencia UISEK	43
Figura 11: Análisis de los 20 controles de las CIS	44
Figura 12: Configuración OSSIM AlienVault: Versión Sistema Operativo	48
Figura 13: Configuración OSSIM AlienVault: Configuración memoria RAM	48
Figura 14: Configuración OSSIM AlienVault: Tamaño de disco duro	49
Figura 15: Configuración OSSIM Alien Vault: Configuración máquina virtual	49
Figura 16: Configuración OSSIM AlienVault: Selección de la imagen OSSIM Alier	ıVault
 	49
Figura 17: Configuración OSSIM AlienVault: Pantalla de instalación OSSIM Alier	ıVault
 	50
Figura 18: Configuración OSSIM AlienVault: Selección idioma.	50
Figura 19: Configuración OSSIM AlienVault: Selección país	51
Figura 20: Configuración OSSIM AlienVault: Selección zona horaria	51
Figura 21: Configuración OSSIM AlienVault: Distribución teclado.	52
Figura 22: Configuración OSSIM AlienVault: Instalación componentes	52

Figura 23: Configuración OSSIM AlienVault: Configuración de tarjeta de red (Virtual
Box)	53
Figura 24: Configuración OSSIM AlienVault: Configuración IP (OSSIM AlienVau	lt)53
Figura 25: Configuración OSSIM AlienVault: Configuración mascara de red	54
Figura 26: Configuración OSSIM AlienVault: Configuración Gateway	54
Figura 27: Configuración OSSIM AlienVault: Configuración DNS	55
Figura 28: Configuración OSSIM AlienVault: Configuración de usuarios	55
Figura 29: Configuración OSSIM AlienVault: Instalación	56
Figura 30: Configuración OSSIM AlienVault: Ingreso al sistema (Pantalla de inicio)56
Figura 31: Configuración OSSIM AlienVault: Levantamiento de servicios	57
Figura 32: Configuración OSSIM AlienVault: Entorno web	57
Figura 33: Configuración OSSIM AlienVault: Creación de cuenta	58
Figura 34: OSSIM AlienVault : Ingreso AlienVault.	58
Figura 35: OSSIM AlienVault : Pantalla de inicio.	59
Figura 36: OSSIM AlienVault: Configuración interface de red.	59
Figura 37: OSSIM AlienVault: Configuración de asset.	60
Figura 38: OSSIM AlienVault: Desplegar HIDS	60
Figura 39: OSSIM AlienVault: Manejo y configuración de los logs	61
Figura 40: OSSIM AlienVault: Configuración OTX	61
Figura 41: OSSIM AlienVault: Configuraciones de preferencias del sistema (Alie	enVault
Setup)	62
Figura 42: OSSIM AlienVault : Configuración de los sensores	62
Figura 43: OSSIM AlienVault : Guardado de configuraciones	63
Figura 44: OSSIM AlienVault : Configuración Jailbreak System	63
Figura 45: OSSIM AlienVault : Conexión por ssh.	64

Figura 46: Gestión de activos: Consola	64
Figura 47: Gestión de activos: Escáner.	65
Figura 48: Gestión de activos: Búsqueda rápida	65
Figura 49: Gestión de activos: Update Maneger Assets.	66
Figura 50: Gestión de activos: Creación de grupos activos.	66
Figura 51: Gestión de activos: Módulos.	67
Figura 52: Gestión de activos: Redes	67
Figura 53: Gestión de activos: Estadísticas	68
Figura 54: Gestión de activos: Dashboard	68
Figura 55: Gestión de activos: Editar	69
Figura 56: Gestión de activos: Editar y actualizar.	69
Figura 57: Gestión de disponibilidad: Activación	70
Figura 58: Gestión de disponibilidad: Editar servicios.	71
Figura 59: Gestión de disponibilidad: Servicios.	71
Figura 60: Gestión de disponibilidad: Paneles de información	71
Figura 61: Gestión de disponibilidad: Estadísticas globales	72
Figura 62: Gestión de disponibilidad: Dashboard	72
Figura 63: Gestión de disponibilidad: Verificación de servicios	73
Figura 64: Gestión de disponibilidad: Informes	73
Figura 65: Gestión de notificaciones: Configuración.	74
Figura 66: Gestión de notificaciones: Configuración nagios	74
Figura 67: Gestión de notificaciones: Configuración correo nombre del sistema (1)	75
Figura 68: Gestión de notificaciones: Configuración correo remitente (2)	75
Figura 69: Gestión de notificaciones: Configuración correo dominio (3)	75
Figura 70: Gestión de notificaciones: Configuración correo redes (4)	76

Figura 71: Gestión de notificaciones: Configuración correo protocolo de internet (5).	76
Figura 72: Gestión de notificaciones: Envió de prueba de correo	76
Figura 73: Gestión de notificaciones: Correo de prueba	77
Figura 74: Gestión de notificaciones: Configuración correo reglas nagios	77
Figura 75: Gestión de vulnerabilidades: Ingreso	78
Figura 76: Gestión de vulnerabilidades: Dashboard	78
Figura 77: Gestión de vulnerabilidades: Escaneo de vulnerabilidades	79
Figura 78: Gestión de vulnerabilidades: Programar un trabajo de escaneo	79
Figura 79: Gestión de vulnerabilidades: Progreso de escaneo	80
Figura 80: Gestión de vulnerabilidades: Escaneo completado	80
Figura 81: Gestión de vulnerabilidades: Informe de escaneo	80
Figura 82: Gestión de vulnerabilidades: Representación de las vulnerabilidades	81
Figura 83: Gestión de riesgos: Ingreso	81
Figura 84: Gestión de riesgos: Dashboard	82
Figura 85: Gestión de riesgos: Prueba de detección.	82
Figura 86: Gestión de riesgos: Evento de seguridad	83
Figura 87: Gestión de riesgos: Filtrar eventos.	83
Figura 88: Gestión de riesgos: Línea de tiempo	84
Figura 89: Funcionamiento de un script	85
Figura 90: Scripts de monitoreo por servicio	86
Figura 91: Scripts de monitoreo en servidor (obtención de estados)	87
Figura 92: Scripts de monitoreo por análisis de datos	88
Figura 93: Scripts de monitoreo por interacción	89
Figura 94: Ejemplo del comando expect	90
Figura 95: Scripts de monitoreo por consumo de microservicios	91

Figura 96: Características de un script: Creación91
Figura 97: Características de un script: Ubicación92
Figura 98: Características de un script: Cuerpo/código92
Figura 99: Características de un script: Mensajes92
Figura 100: Depuración/Debug: Comando bash93
Figura 101: Depuración/Debug: Comando echo \$?93
Figura 102: Agregar un nuevo comando Nagios: Creación nuevo archivo de configuración.
Figura 103: Agregar un nuevo comando Nagios: Estructura de creación de un nuevo
comando
Figura 104: Agregar un nuevo comando Nagios: Agregar nuevo archivo/directorio de
configuración
Figura 105: Agregar un nuevo comando Nagios: Agregar comandos al host
Figura 106: Agregar un nuevo comando Nagios: Errores de compilación Nagios96
Figura 107: Agregar un nuevo comando Nagios: Reinicio del servicio de Nagios96
Figura 108: Agregar un nuevo comando Nagios: Nuevo servicio
Figura 109: Descargar telegram-cli
Figura 110: Prerrequisito para la instalación de telegram-cli en Centos 8
Figura 111: Instalación telegram-cli
Figura 112: Comando local para el envío un mensaje en telegram-cli 100
Figura 113: Comando remoto para el envío un mensaje en telegram-cli100
Figura 114: Flujo script SendMessageTelegram.sh101
Figura 115: Configuración del comando para el envío de mensajes por Telegram 101
Figura 116: Plantilla para el envío de mensajes por Telegram por contacto
Figura 117: Configuración del contacto para el envío de mensajes por Telegram 102

Figura 118: Ejemplo de envío de notificación por Telegram102
Figura 119: Flujo script para la obtención de la temperatura del sistema de enfriamiento de
un Data Center
Figura 120: Flujo script para la obtención de un archivo .csv donde se detalla número de
snapshots que tiene en las máquinas virtuales de un hipervisor, para luego analizarlo y mandar
los estados
Figura 121: Flujo script que analiza e l log de acceso del servicio de apache106
Figura 122: Script que analiza los tamaños de los directorios y logs de la base de datos
Postgresql 108
Figura 123: Script que analiza el número de tickets de la mesa de servicio

ÍNDICE DE TABLAS

Tabla 1: Descripción campus UISEK	. 38
Tabla 2: Cantidad de usuarios UISEK	. 39
Tabla 3: Descripción análisis de los controles de las CIS v7 (1-5)	45
Tabla 4: Descripción análisis de los controles de las CIS v7 (6-12)	46
Tabla 5: Descripción análisis de los controles de las CIS v7 (13-20)	. 47
Tabla 6: Características de un script: Estados Nagios	93
Tabla 7: Agregar un nuevo comando Nagios: Descripción de comandos	. 94
Tabla 8: Agregar un nuevo comando Nagios: Comandos para agregar servicios al host.	. 95

CAPÍTULO I

INTRODUCCIÓN

1.1 Planteamiento del Problema

Ecuador se encuentra en una situación compleja en relación a temas de ciberseguridad, debido a que se ha convertido en un objetivo de ataques cibernéticos, el cual ha incrementado a partir del retiró de asilo político a Julián Assange, programador, periodista y activista de internet australiano, conocido por ser el fundador, editor y portavoz del sitio web WikiLeaks. En el año 2019 según el Ministerio de Telecomunicaciones y de la Sociedad de la Información se confirmaron alrededor de 40 millones de ataques cibernéticos a entidades públicas y privadas (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2019), así como también se ha detectado un incremento anual de infecciones de malware en empresas ecuatorianas comparado a otros países de la región (El Comercio, 2021).



Figura 1: Infecciones de 'malware' en empresas de tres países latinoamericanos Fuente: El Comercio (2021)

Por este motivo, Ecuador actualmente se encuentra entre los 32 países más atacados a nivel mundial según Kaspersky (Kaspersky, 2021), lo cual demuestra no estar preparado para

afrontar este volumen de ataques. Como antecedente, el pasado 23 de julio del 2021 CNT (Corporación Nacional de Telecomunicaciones) confirmó un ataque informático a sus sistemas con el virus de la familia RansomEXX, con el cual se sustrajeron y secuestraron información de los servidores (El Comercio, 2021).

Las Instituciones de Educación Superior (IES) no están libres de ataques a sus sistemas de información y manejan datos sensibles relacionados con aspectos económicos, información académica y del personal en general.

Este es el caso de la Universidad Internacional SEK, que desde la pandemia y el confinamiento el personal docente y administrativo ha tenido que adaptarse a trabajar desde casa, lo que ha conllevado a realizar la mayor parte de sus actividades de forma remota, de tal manera que ha aumentado considerablemente los riesgos de sufrir ataques informáticos, por la falta de familiaridad que existe con el teletrabajo y el bajo nivel de medidas de seguridad de la información.

El departamento de Recursos Tecnológicos de la Universidad Internacional SEK, no cuenta con un sistema que permita verificar el estado de la infraestructura tecnológica y a definir la situación actual de la mayoría de estos sistemas, por lo que, se ha presentado varios inconvenientes, como incidentes de seguridad de la información.

La falta de un sistema de análisis y monitoreo a las incidencias de seguridad que incluya el registro, detección, clasificación, priorización, resolución, seguimiento y cierre de la incidencia, repercute en problemas de funcionamiento de los sistemas informáticos, exponiendo la información sensible de la institución, además se desconoce la interacción de los sistemas tecnológicos con las actividades de la Universidad, ya sea de los estudiantes como del personal administrativo, por este motivo no es posible detectar fallos de rendimiento o mal funcionamiento, errores e intrusiones.

21

1.2 Formulación del Problema.

El departamento de Recursos Tecnológicos de la Universidad Internacional SEK, carece de un sistema de análisis y monitoreo de ficheros de registro (logs), que permita la atención a los posibles riesgos, incidencias o requerimientos a nivel de seguridad informática de la comunidad universitaria de una manera ordenada, oportuna y formal.

1.3 Objetivo general

Integrar un sistema de Gestión de Eventos e Información de Seguridad (SIEM), a través de la herramienta libre OSSIM AlienVault, para la detección de fallos de rendimiento y posibles ataques de seguridad a la infraestructura tecnológica de la Universidad Internacional SEK del Ecuador.

1.4 Objetivos específicos

- Analizar el estado actual de la infraestructura tecnológica de la Universidad Internacional SEK mediante *CIS Critical Security Control v6.1 Assessment Tool* para la determinación de los riesgos de seguridad que posee la entidad.
- Implementar un servidor Linux con la herramienta OSSIM AlienVault y las respectivas configuraciones de seguridad, acceso para monitoreo y control de riesgos de seguridad.
- Establecer los métodos para el comportamiento de los scripts, utilizando herramientas y tecnologías de monitoreo y obtención de datos, que permitan su eficiente desarrollo.
- Desarrollar scripts personalizados en lenguaje SHELL, a través del módulo de disponibilidad de la herramienta OSSIM AlienVault para la obtención de información de los posibles fallos de rendimiento, mal funcionamiento y

detección de posibles ataques de seguridad a la infraestructura tecnológica de la Universidad Internacional SEK del Ecuador.

1.5 Justificación

Técnica

En la actualidad, la mayoría de los sistemas tecnológicos generan registros, bitácoras relacionadas con su funcionamiento, toda esta información brinda indicios de posibles eventos que podrían ser catalogados como un riesgo para la entidad donde funciona, por esta razón, se han desarrollado y liberado herramientas que pueden ser personalizadas y adaptadas a las necesidades de la institución, lo cual permite analizar en qué estado de operatividad y seguridad se encuentra el sistema tecnológico, y así tomar acciones oportunas. En base a estas consideraciones se realiza el presente trabajo, en el que se implementa la herramienta OSSIM AlienVault de acceso libre, que obtiene y genera información para el análisis y control de los eventos e incidentes de seguridad, según los requerimientos de los sistemas tecnológicos de la Universidad Internacional SEK del Ecuador.

Social

De acuerdo a los objetivos de estudio, esta investigación se realiza debido a que es necesario conocer el estado de los sistemas tecnológicos de la Universidad Internacional SEK del Ecuador y su comportamiento de manera detallada, ya que podrían presentar riesgos en seguridad informática, que impacten al desarrollo de la información académica que manejan los estudiantes y personal administrativo, toda vez que dificultaría el cumplimiento de los objetivos institucionales, lo cual no es favorable para su prestigio.

Por esta razón, se desarrollan scripts personalizados para los diferentes servicios de la institución, lo que permite monitorear y alertar los posibles riesgos de seguridad y resguardar la información que se genera.

1.6 Estado del arte

Existen varias investigaciones con diferentes perspectivas de monitoreo de servicios y Gestión de Eventos de seguridad, a continuación, se indica algunos ejemplos:

En la investigación realizada en el año 2015, por Diana Joselyn Espinoza Villón, en su documento "Estudio de la herramienta de seguridad Open Source Security Information Management (OSSIM) en la Universidad Tecnológica Empresarial de Guayaquil (UTEG)" se manifiesta:

- El software OSSIM AlienVault puede indicar posibles riesgos de seguridad así como también la fuente de origen dentro de la infraestructura y parque tecnológico de la institución.
- Gracias a la herramienta se pudo gestionar de mejor manera los incidentes de seguridad y especialmente en lo que corresponde a la fase reactiva.
- Los reportes de OSSIM AlienVault dan claramente información de lo que está ocurriendo en la infraestructura de la organización.

En el artículo científico del año 2015, de Ángel Heraldo Bravo Bravo, Álvaro Luis Villafuerte Quiroz, Ing. José Patiño S. "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" se indica:

- Que al implementar una herramienta OSSIM se redujo el tiempo necesario para la gestión y resolución de incidentes.
- Que las herramientas OSSIM otorgan un aporte invaluable al administrador de red, brindándole información útil para la toma de decisiones en el campo de la

seguridad y que enfocados en la visión principal hemos logrado integrar varios dispositivos de red.

• Que este tipo de herramientas ayudan sobre todo a empresas medianas para optimizar su gestión y el control de incidentes.

En el estudio de Alexis Fernando Balarezo Chávez y Diego Xavier Poveda Pilatasig "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" se señala:

- Que, el monitoreo de incidentes a través de una herramienta OSSIM es una excelente respuesta para robustecer la seguridad en la infraestructura haciendo uso del control del hardware o software que garanticen medidas efectivas ante los ataque o daños.
- Además, la herramienta OSSIM permite verificar las amenazas en tiempo real y trabaja de forma inteligente ya que es capaz de correlacionar eventos en busca de patrones.
- Para implementar este tipo de herramientas en una empresa se requiere conocer detalles sobre aplicaciones o servicios de la organización con el fin de aplicar al máximo la seguridad de acuerdo a las necesidades del negocio.

Por lo manifestado en las diferentes investigaciones se puede concluir que el implementar la herramienta OSSIM AlienVault permitirá minimizar el tiempo de respuesta a los incidentes presentados a la infraestructura tecnológica de la Universidad, así como también contribuye a mantener un adecuado control y monitoreo de los sistemas.

Adicionalmente el desarrollo e implementación de scripts de monitoreo que cumplan con las necesidades de la institución, permitirá robustecer la seguridad en la infraestructura tecnológica de la UISEK.

CAPÍTULO II

MARCO TEÓRICO

A continuación, se describe la teoría que sustenta el trabajo realizado:

2.1 Seguridad informática

Podemos definir la Seguridad Informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integrada, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios no autorizados al sistema. (Gómez, 2011, p. 38)

Amenaza informática

Se puede considerar como amenaza informática a cualquier evento accidental, intencionado que pueda ocasionar algún daño a la infraestructura informática provocando pérdidas materiales, financieras o de otro tipo a la organización (Gómez, 2011; Noguera, 2011).

Vulnerabilidad

Una vulnerabilidad es una debilidad del sistema informático que puede ser explotada por un atacante para obtener acceso no autorizado o realizar acciones no autorizadas que pueden causar daños y pérdidas en una organización (Gómez, 2011).

Impacto

El impacto es la medición y valoración del daño tangible como el daño intangible (Información) que podría producir a la organización un incidente de seguridad, el impacto se categorizar como: bajo, medio y alto (Gómez, 2011).

Riesgo

El riesgo es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad previo a un análisis al sistema informático, causando un determinado impacto en la organización, el riego se categorizar como: bajo, medio y alto (Gómez, 2011).

Políticas de Seguridad

Las políticas de seguridad son reglas establecidas para el dominio de la empresa. Existen políticas de usuarios y de equipos. Las primeras restringen las acciones de los usuarios una vez que ingresan en la red, los equipos y a los servicios; por ejemplo, se puede evitar que se ejecuten ciertos programas en los equipos y realizar muchas otras configuraciones como acciones. Al aplicar políticas de máquinas, permite la opción de estandarizar las propiedades de las PCs de escritorio y los servidores para que tengan una configuración general única; es decir que cualquier usuario que use la máquina tendrá las mismas configuraciones (Marchionni, 2011, p. 72).

Las políticas son reglas, normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de los datos y minimizar los posibles riesgos que puedan presentar.

2.2 **SIEM**

Gestión de Eventos e Información de Seguridad o por sus siglas en *ingles Security Information and Event Management es un tipo de software que tiene como objetivo* centralizar y brindar a las organizaciones información útil sobre potenciales amenazas de seguridad de sus redes críticas, a través de la estandarización de datos y priorización de amenazas. Esto es posible mediante un análisis centralizado de datos de seguridad, obtenidos desde múltiples sistemas, que incluyen soluciones de prevención de intrusiones (helpsystem, 2020).

Este aplicativo es capaz de detectar rápidamente, responder y neutralizar las amenazas informáticas, protegiendo a la empresa de posibles riegos y disminuyendo el impacto en los datos y enfocar los esfuerzos del equipo hacia donde puedan tener mayor nivel de impacto.

OSSIM AlienVault

Open Source Security Information Management en sus siglas en inglés, es una herramienta de código abierto y gestión de eventos (SIEM), con funciones de recopilación, normalización y correlación de eventos. Lanzado por la falta de productos de código abierto especializados en esta rama, OSSIM AlienVault se creó específicamente para abordar la realidad que enfrentan muchos profesionales de la seguridad hoy en día (AT&T, 2021, p. 1).

OSSIM AlienVault es un conjunto de herramientas centralizada que ayuda la administración de eventos de seguridad, las herramientas integradas son:



Figura 2: Herramientas de OSSIM AlienVault Elaborado por: Jorge Añazco

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



Figura 3: Modelo de relación OSSIM Fuente: 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 (Bravo, Villafuerte, & Patiño, 2015)

2.3 20 Controles de la CIS

CIS ControlsTM es un conjunto de acciones priorizadas que colectivamente forman un conjunto de mejores prácticas de defensa que mitigan los ataques más comunes contra sistemas y redes. Los Controles CIS son desarrollados por una comunidad de expertos en TI que aplican su experiencia de primera mano cómo defensores cibernéticos para crear estas mejores prácticas de seguridad aceptadas globalmente. Los expertos que desarrollan los Controles CIS provienen de una amplia gama de sectores que incluyen *retail*, fabricación, salud, educación, gobierno, defensa y otros (CIS Controls, 2018, p. 5). Los controles son actividades que aseguran buenas prácticas ya que son un conjunto de acciones priorizadas y altamente focalizadas compatibles con todos los requerimientos de seguridad gubernamental o industrial (CIS Controls, 2018). los controles son los siguientes:

- Control 1: Inventario y control de activos de hardware.
- Control 2: Inventario y control de activos de software.
- Control 3: Gestión continua de vulnerabilidades.
- Control 4: Uso controlado de los privilegios administrativos.
- Control 5: Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores.
- Control 6: Mantenimiento, monitoreo y análisis de logs de auditoría.
- Control 7: Protección de correo electrónico y navegador web.
- Control 8: Defensas contra malware.
- Control 9: Limitación y control de puertos de red, protocolos y servicios.
- Control 10: Funciones de recuperación de datos.
- Control 11: Configuración segura para dispositivos de red, tales como firewalls, routers y switches.
- Control 12: Protección perimetral.
- Control 13: Protección de datos.
- Control 14: Control de acceso basado en la necesidad de saber.

- Control 15: Control de acceso inalámbrico.
- Control 16: Monitoreo y control de cuentas.
- Control 17: Implementar un programa de concienciación y capacitación en seguridad.
- Control 18: Seguridad del software de aplicación.
- Control 19: Respuesta y gestión de incidentes.
- Control 20: Pruebas de penetración y ejercicios de equipo rojo.



Figura 4: 20 Controles de la CIS v7 Fuente: CIS Controls (2018)

Los Controles CIS v7 se nutren de información de ataques reales y defensas efectivas y reflejan el conocimiento combinado de expertos de cada parte del ecosistema. Esto asegura que los Controles CIS v7 son el conjunto más efectivo y específico de medidas

técnicas disponibles para detectar, prevenir, responder y mitigar el daño desde el más común al más avanzado de esos ataques (CIS Controls, 2018, p. 6).

2.4 Script

Un script es un documento con instrucciones, ordenes o sentencias que tienen un objetivo específico, se considera pequeños programas que son parte de un sistema más grande (Noguera, 2011).

Características

- Cada script tiene una función a cumplir.
- Combinación de elementos, tecnologías y lenguajes.
- Interacción especifica con el usuario o en otro caso con el propio sistema operativo.
- Controla una decretada aplicación o programa en específico.
- Configuración como al mismo tiempo instalación de distintos sistemas de operación.

Los scripts son ampliamente utilizados dentro del diseño y desarrollo de páginas web, para el monitoreo de redes y servidores, manipulación de datos como generación de informes, para cumplir procesos y servicios *serverless, haking*, para inteligencia artificial y *BigData*, y por su versatilidad se puede utilizar en varios lenguajes de programación como de tecnologías.

Lenguaje Shell

El intérprete de mandatos o "shell" es la interfaz principal entre el usuario y el sistema, permitiéndole a aquél interactuar con los recursos de éste. El usuario introduce sus órdenes, el intérprete las procesa y genera la salida correspondiente. Por lo tanto, un intérprete de mandatos de Unix es tanto una interfaz de ejecución de órdenes y utilidades, como un lenguaje de programación, que admite crear nuevas órdenes – denominadas guiones o "shellscripts"–, utilizando combinaciones de mandatos y estructuras lógicas de control, que cuentan con características similares a las del sistema y que permiten que los usuarios y grupos de la máquina cuenten con un entorno personalizado.

En Unix existen 2 familias principales de intérpretes de mandatos: los basados en el intérprete de Bourne (BSH, KSH o BASH) y los basados en el intérprete C (CSH o TCSH) (Labrador, 2003, p. 4).

CAPÍTULO III

ANÁLISIS Y SITUACIÓN ACTUAL

3.1 Universidad Internacional Sek (UISEK)

La Universidad Internacional SEK es un centro de educación superior laica y privada con 30 años de trayectoria en Ecuador y como Institución SEK con 125 años en experiencia educativa, actualmente sus 3 campus funcionan en la ciudad de Quito, en las siguientes direcciones, Miguel de Cervantes, al norte de la ciudad sector Carcelén, el Campus Juan Montalvo, se encuentra en el Monasterio de Guápulo, zona céntrica de la ciudad además de que es considerada como Patrimonio de la Humanidad y el Campus Felipe Segovia Olmo que se encuentra ubicada en la parte centro norte de la ciudad, actualmente la universidad por su función académica ofrece 21 carreras de pregrado y 24 programas de posgrado tratando de ampliar las propuestas académicas según las necesidades del país.



Figura 5: Logo Universidad Internacional Sek **Fuente:** Universidad Internacional Sek (2021)

"La Universidad Internacional SEK (UISEK), es una institución de Educación Superior que se encuentra encaminada en alcanzar la excelencia educativa y que viene paso a paso consolidando la mejora continua" (Universida Internacional SEK, 2021).
"La Planificación Estratégica, como uno de sus procesos clave, ha sido instituida bajo parámetros de reflexión y respaldo institucional" (Universida Internacional SEK, 2021).

"Su formulación está diseñada con la convicción, el interés y el absoluto compromiso de cada autoridad, directivo, decano, docente, estudiante y personal administrativo, en pro de la sociedad ecuatoriana y de la UISEK" (Universida Internacional SEK, 2021).

Misión:

"Desarrollar sus actividades de docencia, investigación y vinculación, con los más altos estándares de calidad y pertinentes para la solución de problemas de la sociedad de manera sostenible" (Universida Internacional SEK, 2021).

Visión:

"Ser una universidad referente de calidad acreditada, apoyada en políticas de mejora continua, comprometida con la generación y transferencia del conocimiento en beneficio de la sociedad" (Universida Internacional SEK, 2021).

Historia

En 1892, nace en Madrid la Institución SEK, oficialmente reconocida en 1905, y al finalizar la Guerra Española en 1939 inicia su expansión educativa y en 1960 las innovaciones pedagógicas guían el proyecto educativo, a partir de 1982 adquiere proyección internacional mediante la creación de centros educativos en diversos países: SEK-Chile (Santiago y Viña del Mar) y SEK- Ecuador (Quito y Guayaquil), a partir de 1986 se vinculan otros países a la red: SEK-Panamá, SEK-Paraguay, SEK-Costa Rica, en España se amplía a Coruña y Valencia, en 1996 se inauguró SEK-República Dominicana, en 1997 SEK- Hungría, en 1999 SEK- EE.UU, en 2001 SEK-Guatemala, en 2003 SEK-Sud África y en 2005 SEK- México.

La Institución Internacional SEK concreta su proyecto educativo universitario a partir de 1990 con la creación de la UISEK- Santiago de Chile, en 1993 la UISEK-Quito y, en 1997 la UISEK- Segovia. La afinidad cultural y lingüística ha propiciado el afianzamiento de lazos educativos en 15 países sobre la base del aprendizaje de calidad, en busca de la excelencia académica (Universidad Internacional Sek, 2021).

3.2 Situación Tecnológica de la Universidad Internacional SEK

La Universidad Internacional SEK para sus actividades necesita sistemas o módulos informáticos que den soporte a los procesos diarios de la universidad, actualmente no existe un rol de Oficial de Seguridad de la Información responsable de aplicar todas las normas y buenas prácticas de seguridad informática, así como también no se encuentra implementado un sistema de gestión de eventos e información de seguridad (SIEM), que permita la detección de fallos de rendimiento y posibles ataques de seguridad a la infraestructura tecnológica.

No cuenta con un comité de seguridad de la información, integrado por los responsables de las áreas administrativas de la Universidad, con el fin de diseñar los requerimientos y procesos que cada área necesita, con el fin de precautelar la información y el funcionamiento de la Universidad, además no se ha definido los procesos de los diferentes módulos y subsistemas que cuenta la entidad para su funcionamiento, por ejemplo, el Portal Alumnos (https://portalalumnos.uisek.edu.ec/Account/Login.aspx), el Portal de Docentes (https://portaldocentes.uisek.edu.ec), Aulas Virtuales Canvas (https://canvas.uisek.edu.ec/, portales de la biblioteca (https://repositorio.uisek.edu.ec/, http://biblioteca.uisek.edu.ec/home/index.php) y otros aplicativos internos como externos que maneja la institución. Al no contar con una estructura organizada, coherente y optimizada no se ha logrado expandir el grado de seguridad de los aplicativos como de la infraestructura de la universidad y la de sus proveedores de servicios.

No se ha implementado una norma estándar de seguridad que permita unificar los criterios de evaluación de los riesgos asociados al manejo de la información de la Universidad, el objetivo principal del Sistema de Gestión de Seguridad de la Información es preservar la confidencialidad, integridad y disponibilidad de la información.

3.3 Descripción de la infraestructura

La UISEK funciona en tres campus:

- 1. Campus Felipe Segovia Olmo: Calle Italia N31-125 y Av. Mariana de Jesús.
- 2. Campus Miguel de Cervantes: Calle Alberto Einstein s/n y 5ta. transversal (Carcelén).
- 3. Campus Juan Montalvo: El Calvario s/n y Fray Francisco Compte.

Tabla 1: Descripe	ción campus UISE	K				
Campus	Edificio	Aulas				
	1	3				
	2	18				
Campus Juan Montalvo	3	2				
	4	6				
	5	9				
Campus Felipe Segovia		7				
Campus Juan Montalvo		19				
Elaborado por: Jorge Añazco						

Cada campus dispone de su propia infraestructura tecnológica y su respectivo proveedor de internet, las 64 aulas de los 3 campus cuentan con su proyector, computador para el profesor y un dispositivo wifi, con respecto al ingreso a la red es abierta para los estudiantes como para los profesores.

Es importante mencionar que no se ha implementado una herramienta que detecte riesgos de seguridad en tiempo real, esto es un punto importante, ya que, un ataque que no puede ser detectado de manera inmediata, puede afectar el desarrollo normal de las actividades académicas.

3.4 Usuarios

Es importante definir el tipo de usuario que tiene la institución, ya que, como entidad de educación existe un considerable flujo de personas, las cuales pueden ser un potencial riesgo de seguridad, la UISEK cuenta con un flujo aproximado de usuarios de acuerdo al siguiente detalle:

Tabla 2: Cantidad de usuarios UISEK				
Descripción	Cantidad			
Personal Administrativo	80			
Estudiantes	2.000			
Profesores	164			
Total	2.244			
Flaharada nar	Jorgo Añazoo			

Elaborado por: Jorge Añazco

Con estas estadísticas, se puede obtener un alcance de la población que sería afectada en un ataque informático, así como también, puede ser considerada como posibles fuentes de eventos e incidentes de seguridad dentro de la organización.

3.5 Operatividad de los portales o aplicativos web

A nivel de infraestructura tecnológica, los aplicativos se encuentran en una plataforma virtual en la nube, el proveedor es el encargado de la operatividad y seguridad informática, el riesgo del funcionamiento de los aplicativos está dado por la calidad del código de desarrollo.

Los portales o aplicativos webs que maneja la Universidad tienen como objetivo principal la visualización y accesibilidad de la información requerida por los estudiantes, docentes y personal administrativo, así como también ayudar con el proceso de aprendizaje de los alumnos. También se ofrece servicios adicionales como la matriculación de los estudiantes, compra de certificados, bienestar estudiantil, secretaria académica y secretaria general.

Los aplicativos web y herramientas informáticas que maneja la institución no se encuentran en un nivel óptimo de seguridad, por esta razón determinan un riesgo inherente como residual, y al no contar con procesos que permitan disminuir la susceptibilidad a los ataques, siempre existirá un riesgo alto de seguridad en los diferentes sistemas que tiene la institución.

3.6 Módulos críticos

A continuación, se detallan los módulos que se consideran críticos para la operatividad de la universidad:

Módulo de inicio de sesión

Este módulo tiene un riesgo alto, ya que, si el atacante obtiene las credenciales del estudiante, puede ingresar y visualizar toda la información del mismo, pero hay que tomar en cuenta que la Universidad ha invertido recursos sobre este módulo en criptografía de los parámetros importantes para el inicio de sesión, además, cuenta con el respaldo del ingreso al portal, a través del correo institucional con Google.

Ingrese mediante el uso de una cuenta de correo institucional



Figura 6: Inicio de sesión Portal Alumnos UISEK Fuente: Portal Alumnos UISEK

Módulo de hoja de vida e información del estudiante

Este módulo tiene un nivel de riesgo alto, debido a que se encarga de guardar la información del estudiante realizando un histórico para obtener estadísticas según las necesidades de la universidad, por último, si el atacante logra obtener toda la información del estudiante, puede utilizarlo para diferentes fines.



Figura 7: Módulo de hoja de vida UISEK Fuente: Portal Alumnos UISEK

Módulo de certificados

Este módulo tiene un nivel de riesgo bajo, ya que son solicitudes del estudiante hacia la

Universidad.

	Especie Valorada	
FECHA: SOLICITANTE: CÉDULA: CORREO: CORREO INSTITUCIONAL: SEMESTRE ACTUAL:		
SELECCIONE SU CARRERA: SELECCIONE SU © ESTADO:	Seleccione una opción	M
E1ij. 	a el tipo de solicitud que desea generar Seleccione una opción - V	

Figura 8: Módulo de certificados UISEK Fuente: Portal Alumnos UISEK

Módulo de Pagos

Este módulo permite realizar al estudiante los pagos de los servicios ofertados en el Portal Alumnos, tienda virtual de la universidad y en el proceso de pago de inscripciones, matrículas y créditos, por lo cual, tiene un nivel de riesgo alto, ya que es un punto en que el atacante puede obtener información sensible del estudiante y beneficiarse de manera económica.

Datos de Factura

Nombre:	Nombre
Tipo Identificación:	RUC ~
Identificación:	Identificación
Dirección:	Dirección
Teléfono:	Teléfono
Email:	Email

Formas de Pago

Tarjetas aceptada	5:					
VISA 🥌	Dieme Cable					
Marca Tarjeta	Seleccione una opción	~				
Banco Emisor	Seleccione una opción	~				
Tipo Crédito	Seleccione una opción	~				
Meses Diferido						
Confirme que los datos ingresados sean correctos, estos saldrán en su factura. Además acepta los términos y condiciones, políticas de privacidad.						
	Pagar					
Γ.						

Figura 9: Módulo de pagos UISEK Fuente: Portal Alumnos UISEK

Módulo de notas y asistencia

Este módulo es un nivel de riesgo medio, ya que el atacante podría modificar las notas de

los estudiantes, sin embargo, la Universidad puede detectar estos cambios y rectificarlos.

Nivel	TIPO	Código Asignatura	Nombre Asignatura	Paralelo	P1	PZ	N.Ex	NS	NES	Asis %	ASISTENCIA	Nota Final	Estado
3	MAT1	MCIBDIFP3SO	SEGURIDAD ORGANIZACIONAL Y PERSONAL							100	4/4 (100%)	7,8	APROBADO
3	MAT1	MCIBDIFP3SS	SEGURIDAD SOCIAL EN LA ERA DIGITAL							100	8/8 (100%)	9,4	APROBADO
3	MAT1	MCIBDIIA3SE	SEGURIDAD EN HARDWARE						~	100	7/7 (100%)	9,7	APROBADO
3	MAT1	MCIBTIIA3TA	TALLER INTEGRAL PARA LA IMPLEMENTACION DEL TRABAJO DE TITULACION							100	3/3 (100%)	9,1	APROBADO
<													>

Figura 10: Módulo de notas y asistencia UISEK Fuente: Portal Alumnos UISEK

3.7 Riesgos indirectos

Como cualquier entidad o empresa existe un riesgo importante de amenazas que pueden llegar a través de métodos o medios muy diversos, que pueden ser, desde negligencia del personal interno como de proveedores de servicios o ataques maliciosos cuidadosamente planificados con un objetivo específico, según PandaSecurity (2018) en una encuesta realizada por Crowd Research el 90% de las empresas consultadas se considera vulnerable a este tipo de problemas de seguridad de hecho, el 53% de las compañías asegura haber sufrido ataques internos en los últimos doce meses.

3.8 20 controles de la CIS

El presente análisis se realiza con el documento *CIS Critical Security Control v6.1 Assessment Tool*, proporcionado por el proyecto (AuditScripts, 2018), el cual brinda una estructura de calificación del 0 al 5 del estado de la seguridad informática de la empresa respecto a los 20 controles de las CIS, que se detallan a continuación:

()	AuditScri	ipts	5	Cri	tical S	Securi	ity Co	ntrol	s Init	ial As	sessn	nent	Tool	(v6.1o	:)			eno		/e
Maturity level Level One Level Two Level Three	Descriptio Policies Complete Controls 1-5 Imp All Controls Impl	n: e lement emente	Scor 0,3 ec 0,3 ed 0,1	re: 4 9 8		1,00 0,80 0,60					Matu	rity Le	vel Agg	regate	Scores	:				
Level Five	All Controls Add All Controls Repo Maturity Ratin *Rating is on a 0-	ng*: 5 scale	0,2 0,2 1,3	4		0,40 — 0,20 — 0,00 —	POLICIES	,34 COMPLET	E	CONTR IMPLEN	39 DLS 1-5 1ENTED	1	0,1 ALL CON IMPLEM	8 TROLS ENTED	ALL CO	0,23 NTROLS A	JTOMATEE	ALL CO	0,20 DNTROLS RE	PORTED
	100%					CS	C Imp	oleme	entat	ion Pe	ercen	tage	by Co	ontrol						
	90% 80% 70% 60% 50% 40% 20% 20% 25%	67%	39%	34%	33%	29%	22%	17%	33%	31%	43%	25%	8%	14%	14%	11%	10%	31%	4%	0%

Figura 11: Análisis de los 20 controles de las CIS. Elaborado por: Jorge Añazco

Con los resultados de la figura anterior, análisis de los 20 controles de las CIS v7, se puede concluir que las políticas de seguridad no están completas y existe fallas en su ejecución, que en general los controles de las CIS v7 no se han implementado de manera óptima y existe problemas de inventarios de hardware como de software, ningún control de la CIS v7 se ha implementado más del 70% y en otros controles es nula su implementación, no existen procesos completos ni automatizados de seguridad informática, lo cual se deriva por la falta de un programa de seguridad de la información, por último, con el puntaje obtenido de 1.34 se establece que el nivel de seguridad de la institución es baja y es necesario establecer acciones y procesos para mejorar la seguridad.

En las siguientes matrices, se detalla por cada control de la CIS v7 los problemas encontrados y su puntaje de cumplimiento:

Control	Descripción	Observación	Puntaje
1	Inventario y control de activos de hardware	Se puede observar falta de inventarios completos de los equipos de red y equipos tecnológicos, además, no existe un control de los equipos que se conectan y se desconectan de la red, lo que implica que no se puede identificar, registrar, responder y proteger a las acciones de estos equipos de manera inmediata y segura, se ha verificado que no existe ninguna implementación de certificados para que los equipos de la red de confianzas se puedan identificar.	25%
2	Inventario y control de activos de software	No existe ningún control de inventarios de software autorizado de manera óptima ya que no existe herramientas ni políticas (listas blancas, Active Directory) que estandaricen la utilización del software y actualizaciones de las mismas para evitar brechas de seguridad.	67%
3	Gestión continua de vulnerabilidades	No existen herramientas que ayuden a detectar o escanear posibles vulnerabilidades y evitar los riesgos que se genera, actualmente existe herramientas que solo ayudan en proteger a nivel de red posibles intrusiones. Y no están definidos procesos de calificación de riesgo para priorizar la corrección de vulnerabilidades descubiertas.	39%
4	Uso controlado de los privilegios administrativos	No existe procesos o herramientas que ayuden a controlar, rastrear, prevenir, corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes. Las aplicaciones web desarrolladas cuentan con un control de privilegios por medio de roles asignados a cada usuario, pero no se cuenta con un inventario general de cuentas administrativas que consten todos los accesos y cuentas de todos los sistemas de la universidad	34%
5	Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores	Se ha detectado que no todas las estaciones de trabajo y servidores cuentan con una configuración con buenas propiedades de seguridad, además si incluso existe una configuración solida de seguridad no hay una gestión para evitar la degradación de la seguridad a medida que se actualiza, se repare o exista algún cambio en el software. Por último, no existe respaldo de las configuraciones de todos los dispositivos y las mismas no son actualizadas frecuentemente.	33%

Tabla 3: Descripción análisis de los controles de las CIS v7 (1-5)

Elaborado por: Jorge Añazco

Control	Descripción	Observación	Puntaje
6	Mantenimiento, monitoreo y análisis de logs de auditoría	No existe un manejo y análisis total de los registros que generan todos los dispositivos informáticos por las actividades y eventos que genera la universidad, por esta razón no se puede detectar, comprender o recuperase de un ataque o fallo en los sistemas. Por último, no se tiene implementado un nivel de detalle de los registros para tener más información de los posibles eventos de seguridad que puedan existir.	29%
7	Protección de correo electrónico y navegador web	No existe configuraciones que ayuden asegurar y precautelar el uso de navegadores y clientes de correo electrónico, además no hay un control de soporte y que estén en la última versión que libera el proveedor. No hay control de los plugins o aplicaciones add-on instalados en los navegadores o cliente de correo electrónico y limitar solo lenguajes scripting autorizados en los navegadores.	22%
8	Defensas contra malware	No esta implementado un software antimalware gestionado centralmente para monitorear y defender continuamente cada una de las estaciones de trabajo y servidores. No existe la limitación para no ejecutar el contenido de los medios extraíbles. No existe información necesaria para realizar auditorías para detectar posibles ataques de los equipos de la institución.	17%
9	Configuración segura para dispositivos de red, tales como firewalls, routers y switches	No hay un control completo en la administración del uso operacional continuo de puertos, protocolos y servicios en dispositivos en red para poder rastrear, controlar, corregir y minimizar los posibles ataques.	33%
10	Funciones de recuperación de datos	No se han realizado pruebas que aseguren la integridad que los datos respaldados y de forma periódica mediante procesos automatizados.	31%
11	Protección perimetral	No hay herramientas que automaticen la verificación de configuraciones de equipos y detectar cambios, además que alerte cuando exista algún cambio. No existe maquinas dedicadas para las tareas administrativas o tareas que necesiten un acceso elevado.	43%
12	Defensa de borde	No existe equipos IDS/IPS para registrar, monitorear y alertar el flujo de paquetes en el límite de cada una de los bordes de la organización. No existe colectores NetFlow para registrar todos los datos de los equipos de borde de la red.	25%

Tabla 4: Descripción análisis de los controles de las CIS v7 (6-12)

Elaborado por: Jorge Añazco

Control	Descripción	Observación	Puntaje
		No hay cifrado de los discos duros internos, externos, medios extraíbles como flash, tarjetas	
13	Protección de datos	de memorias y equipos móviles y no existe configuraciones para que la información no sea	8%
		copiada en cualquier dispositivo de almacenamiento.	
		No se ha implementados procesos y herramientas utilizados para rastrear, controlar,	
14	Control de acceso basado en la nacesidad de saber	prevenir, corregir el acceso seguro a activos críticos como la información y recursos que	1/10/
14	Control de acceso basado en la necesidad de saber	genera la institución, además no hay una jerarquización a la necesidad de acceder a estos	14%
		activos críticos basado en una clasificación aprobada.	
		No hay autenticación inalámbrica con protocolos que requieran autenticación mutua de	
15	Control de acceso inalámbrico	múltiples factores, tampoco hay configuraciones que deshabiliten conexiones con equipos o	14%
		periféricos a través Bluetooth y NFC.	
		No hay una gestión activamente del ciclo de vida de las cuentas del sistema y de	
16	Monitoreo y control de cuentas	aplicaciones, tampoco hay un inventario de las cuentas y crear un punto de autenticación	11%
		centralizado.	
		No se ha realizado un análisis de brecha de habilidades por ende no se puede realizar	
		capacitaciones que ayuden a suplir la deficiencia de los empleados.	
17	Implementar un programa de concienciación y capacitación en seguridad	No se han realizado capacitaciones, talleres o cursos que actualicen, eduquen o informe	10%
		sobre temas de ciberseguridad al personal de la institución.	
		No se ha implementado prácticas seguras de codificación para el desarrollo interno y la	
18	Seguridad del software de aplicación	adquisición de nuevo software, no se ha definido procesos ni herramientas para receptar y	31%
		tratar reportes de seguridad (Errores, logs, bugs) del software adquirido por la institución.	
		No existe documentación de los procedimientos de respuesta a incidentes, tampoco existe	
19	Respuesta y gestión de incidentes	asignación de roles según el tipo de incidencia y por último, no hay un esquema de	4%
		priorización y puntuación de incidentes.	
		No se cuenta con personal, herramientas ni se ha contratado equipos externos para realizar	
20	Pruebas de penetración y ejercicios de equipo rojo	pruebas de penetración de servicio por ende no hay auditorias tanto internas como externas	0%
		que ayuden con las pruebas de penetración ni ejercicios de equipo rojo.	

Tabla 5: Descripción análisis de los controles de las CIS v7 (13-20)

Elaborado por: Jorge Añazco

En virtud de lo expuesto, en la calificación de los 20 controles de la CIS v7 y de acuerdo al gráfico de la figura 9, se puede identificar que la Universidad cuenta con un bajo nivel de seguridad informática, al no disponer de una estructura organizada ni estándares de calidad.

3.8.1 Posible escenario de mejora

Para mejorar la seguridad informática de la institución, se debería:

- Implementar un área administrativa que gestione transversalmente la seguridad de la información, mediante programas, políticas de seguridad según las necesidades de la institución, basándose en los controles de la CIS v7, ya que, en la actualidad no se realiza monitoreo, control, pruebas de calidad, pruebas de penetración de servicios, ni auditorias de seguridad informática.
- Desarrollar e implementar procesos de observación y monitorio de los sistemas como del comportamiento de los trabajadores dentro de las actividades de la universidad en tiempo real, realizar revisiones periódicas de los registros de los servidores, con el objetivo de comprobar algún comportamiento sospechoso, obtener datos específicos que permitan realizar análisis con el fin de detectar o prever de una posible amenaza interna.
- Planificar estrategias de prevención de pérdida y manipulación de datos, además de proteger información, ya sea encriptar o limitar su acceso según la criticidad de la misma, por último, desarrollar un control e identificación de acceso, así como restringir y registrar el uso del software como del hardware.

CAPÍTULO IV

PROPUESTA

De acuerdo a los objetivos planteados, a continuación, se detalla los pasos realizados para la instalación de la herramienta OSSIM AlienVault y la configuración de sus módulos.

Se define los tipos de scripts para el monitoreo y el proceso de implementación de los scripts en el Módulo de Disponibilidad.

4.1 Instalación/configuración de la herramienta OSSIM

4.1.1 Instalación

Herramientas

- Herramienta SIEM: OSSIM AlienVault versión 5.8.1
- Página Oficial: https://cybersecurity.att.com/products/ossim
- Link: https://dlcdn.alienvault.com/AlienVault_OSSIM_64bits.iso

Herramientas para ambiente de pruebas

- Herramienta de virtualización: VirtualBox 6.1.10 64bits
- Página Oficial: https://www.oracle.com/virtualization/virtualbox/
- Link: https://download.virtualbox.org/virtualbox/6.1.10/VirtualBox-6.1.10-138449-Win.exe

Para la instalación OSSIM AlienVault se debe tener conocimiento de la infraestructura de la organización donde se va a instalar es importante saber las configuraciones de las redes, subredes, los DNS, DHCP, puertas de enlaces, proxy y configuración de los equipos perimetrales para que la herramienta funcione correctamente, a continuación, la instalación:

La configuración de la máquina virtual será la siguiente:

• Sistema Operativo: Linux Debian 64Bits

Nombre:	OSSIM		
Tipo:	Linux	•	
Versión:	Debian (64-bit)	-	



• Memoria RAM: 2048MB



Figura 13:Configuración OSSIM AlienVault: Configuración memoria RAM Fuente: OSSIM AlienVault

• Tamaño de disco: 20GB

Ubicación del archivo y tamaño

máquina virtual, presionar clic derecho y seleccionar Configuración:

Escriba el nombre del archivo de unidad de disco duro virtual en el campo debajo o haga clic en el icono de carpeta para seleccionar una carpeta diferente donde crear el archivo.									
C:\Users\Sonic\VirtualBox VMs\OSSIM\OSSIM.vdi									
Seleccione el tamaño de disco duro virtual en megabytes. Este tamaño es el límite para el archivo de datos que una máquina virtual podrá almacenar en el disco duro.									
	20,76 GB								
400MP 200									
4,00 MB 2,00 TB									

Figura 14: Configuración OSSIM AlienVault: Tamaño de disco duro Fuente: OSSIM AlienVault

Agregar la imagen ISO para la instalación del OSSIM AlienVault, en el nombre de la

OSSIM (Instalacion)		• •
🜔 🕛 Apagada	😟 Configuración	Ctrl+S
	G Cl <u>o</u> nar	Ctrl+O
	😢 <u>M</u> over	
	R Export to OCI	
	😫 Eliminar	
	Agrupar	
	🔷 Iniciar	•
	0 Pausar	
	O <u>R</u> einiciar	
(Corrar	

Figura 15:Configuración OSSIM AlienVault: Configuración máquina virtual Fuente: OSSIM AlienVault

Después de ingresar a la opción de almacenamiento, en la parte de Controlador: IDE en la

opción de Vacío seleccionar la ISO de OSSIM AlienVault.

<u></u> (SSIM - Configuración				?	×	
	General	Almacenamiento					
	Sistema	Dispositivos de almacenamiento	Atributos				
	Pantalla	合 Controlador: IDE	Unidad óptica:	IDE secundario maestro	• •	0	
		💽 Vacío		CD/DVD vivo			Seleccione archivo de disco óptico virtual
	Almacenamiento	left Controlador: SATA	Información				AlienVault_OSSIM_64bits.iso
	Audio	OSSIM.vdi	Tipo:				CentOS-8-x86_64-1905-dvd1.iso
	Red		Ubicación:				kali-linux-2019.4-amd64.iso
	neu -		Conectado a:			G	Eliminar disco de la unidad virtual
	Puertos serie					_	
Ø	USB						
	Carpetas compartidas						
	Interfaz de usuario						
				Aceptar	Cancela	er 👘	

Figura 16: Configuración OSSIM AlienVault: Selección de la imagen OSSIM AlienVault Fuente: OSSIM AlienVault

Al iniciar la máquina virtual se muestra las opciones de instalación en este proyecto vamos a elegir la opción de *Install OSSIM AlienVault*.



Figura 17: Configuración OSSIM AlienVault: Pantalla de instalación OSSIM AlienVault Fuente: OSSIM AlienVault

Luego de Seleccionar la primera opción se desplegará la siguiente pantalla para seleccionar

el idioma que desee.



Figura 18: Configuración OSSIM AlienVault: Selección idioma. Fuente: OSSIM AlienVault

Se debe seleccionar la zona horaria, en este caso Ecuador - Guayaquil

	·]		
ALIEN VAULT OSSIN			
La ubicación seleccionada aquí se utilizar ayudarle a seleccionar la localización de vd. vive.	á para fijar su zor su sistema. Esta le	na horaria y también como ocalización será habitualm	ejemplo para iente el país donde
Esta es una lista reducida de ubicaciones ubicación no está en la lista. País, territorio o área:	basada en el idio	ma que ha seleccionado. I	Escoja «otro» si su
Colombia			<u>^</u>
Costa Rica			
Cuba			
Ecuador			
El Salvador			
España			
Estados Unidos			
Guatemala			-
Honduras			
México			
Nicaragua			
Panamá			~
Capturar la pantalla		Retroceder	Continuar
		D 🔾 📜 🗗 🄗 🗆 🖳	🔚 🔯 🚫 💽 CTRL DERECHA

Figura 19: Configuración OSSIM AlienVault: Selección país. Fuente: OSSIM AlienVault

ALIEN VAULT OSSIM		
Si la zona horaria deseada no está en la lista enton seleccione un país que utilice la zona horaria desea Seleccione una ubicación en su zona horaria:	nces vuelva atrás al paso «Escoja el ada (el país donde vive o está ubica	idioma» y do).
Guayaquil		
Capturar la pantalla	Retroceder	Continuar
	Q 💿 🐚 🗗 🔏 🗆 🖲) 🖶 💟 🔇 💽 CTRL DERECHA

Figura 20: Configuración OSSIM AlienVault: Selección zona horaria. Fuente: OSSIM AlienVault

Se debe elegir la distribución del teclado a utilizar.

ALIEN VAULT OSSIM Configure el teclado		
Mapa de teclado a usar: Kazajo Jemer Kirghizo Coreano Kurdo (variante F) Kurdo (variante Q) Laosiano Latinoamericano Letón Lituano Macedonio Malayalamo Nepalés Sami septentrional Noruego		
Capturar la pantalla	Retroceder	Continuar

Figura 21: Configuración OSSIM AlienVault: Distribución teclado. Fuente: OSSIM AlienVault

Luego el proceso de instalación cargará los componentes y comenzará la instalación.



Figura 22: Configuración OSSIM AlienVault: Instalación componentes. Fuente: OSSIM AlienVault

Inmediatamente se procede a configurar la red, para esta parte es necesario poner en modo puente/bridge la interface de red.

09	SSIM - Configuración		?	×
	General	Red		
	Sistema	Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4		
	Pantalla	Habilitar adaptador de red		
\bigcirc	Almacenamiento	Conectado a: Adaptador puente 🔻		
	Audio	Nombre: Intel(R) Ethernet Connection (2) I219-V		•
	Pad	Avanzadas		
	Red			
	Puertos serie			
	USB			
	Carpetas compartidas			
	Interfaz de usuario			
		Aceptar	Canc	elar

Figura 23: Configuración OSSIM AlienVault: Configuración de tarjeta de red (Virtual Box). Fuente: OSSIM AlienVault

La configuración de red en el ambiente de pruebas va a ser la siguiente:

- Capturar la pantalla

 Retroceder

 Capturar la pantalla
- IP: 192.168.0.161

- Figura 24: Configuración OSSIM AlienVault: Configuración IP (OSSIM AlienVault) Fuente: OSSIM AlienVault
- Máscara de red: 255.255.255.0

]			
ALIEN VAULT OSSIN	۱.			
La máscara de red se utiliza para determinar qué sistemas están incluidos en la red. Consulte al administrador de red si no conoce el valor. La máscara de red debería introducirse como cuatro números separados por puntos. <i>Máscara de red</i> :				
255. 255. 255. 0				
Capturar la pantalla		Retroceder	Continuar	
		0 o hi 🗗 🌶 🗆 🗉	🔚 💟 🚫 💽 CTRL DERECH/	

Figura 25: Configuración OSSIM AlienVault: Configuración mascara de red. Fuente: OSSIM AlienVault

• Gateway: 192.168.0.1

ALIEN VAULT OSSIM	
La pasarela es una dirección IP (cuatro núme pasarela, también concido como encaminar (por ejemplo, hacia internet) se envia a este no tener un encaminador; si es así lo puede pregunta, consulte al administrador de red. <i>Pasarela:</i>	neros separados por puntos) que indica el encaminador de ador por omisión. Todo el tráfico que se envia fuera de su LAN e encaminador. En algunas circunstancias anormales, puede e dejar en blanco. Si no sabe la respuesta correcta a esta l.
192.168.0.1	
Capturar la pantalla	Retroceder Continuar
	🞴 💿 📜 🖶 🌽 🗐 📳 🕲 🔇 💽 CTRL DERECH

Figura 26: Configuración OSSIM AlienVault: Configuración *Gateway*. **Fuente:** OSSIM AlienVault

• DNS: 192.168.0.1

ALIEN VAULT OSSIM Configurar la red	
Los servidores de nombres se utilizan para buscar los n introduzca la dirección IP (no el nombre de sistema) de l espacios. No utilice comas. Se consultarán los servidore utilizar ningún servidor de nombres deje este campo en Direcciones de servidores de nombres: 192.168.0.1	ombres de las máquinas de la red. Por favor, hasta tres servidores de nombres, separados por es en el orden en que se introduzcan. Si no quiere blanco.
Capturar la pantalla	Retroceder Continuar

Figura 27: Configuración OSSIM AlienVault: Configuración DNS. Fuente: OSSIM AlienVault

Luego se debe generar la contraseña del usuario root.

ALIEN VAULT OS	SIM
onfigurar usuarios y contraseñas	
vecesita dennir una contrasena pai sistema. Podría tener graves conse cualificación tuviera acceso a la cue elegir un la contraseña para el sup que se encuentre en el diccionario,	a el superusuario («root»), la cuenta de administracion del cuencias que un usuario malicioso o un usuario sin la debida nta del administrador del sistema, así que debe tener cuidado y srusuario que no sea fácii de adivinar. No debería ser una palabra o una palabra que pueda asociarse fácilmente con usted.
Ina huena centraceña debe center	er una mezcla de letras, números y signos de puntuación, y debe
cambiarse regularmente. .a contraseña del usuario «root» (a)lanco, entonces se deshabilitará li »ermisos para convertirse en usuar	dministrador) no debería estar en blanco. Si deja este valor en s cuenta de root creará una cuenta de usuario a la que se le darán io administrador utilizando la orden «sudo».
na bora contrasena debe conten a contraseña del usuario «root» (a olanco, entonces se deshabilitará l bermisos para convertirse en usuar fenga en cuenta que no podrá ver la Clave del superusuario:	dministrador) no debería estar en blanco. Si deja este valor en a cuenta de root creará una cuenta de usuario a la que se le darán io administrador utilizando la orden «sudo». a contraseña mientras la introduce.
Cambiarse regularmente. La contraseña del usuario «root» (a blanco, entonces se deshabilitará l permisos para convertirse en usuar fenga en cuenta que no podrá ver la Clave del superusuario:	idministrador) no debería estar en blanco. Si deja este valor en a cuenta de root creará una cuenta de usuario a la que se le darán io administrador utilizando la orden «sudo». a contraseña mientras la introduce.
ora buera contraseria debe conten cambiarse regularmente. La contraseña del usuario «root» (a blanco, entonces se deshabilitará l permisos para convertirse en usuar fenga en cuenta que no podrá ver l <i>Clave del superusuario:</i> Mostrar la contraseña en claro Por favor, introduzca la misma contr correctamente.	idministrador) no debería estar en blanco. Si deja este valor en a cuenta de root creará una cuenta de usuario a la que se le darán io administrador utilizando la orden «sudo». a contraseña mientras la introduce.
Cambiarse regularmente. La contraseña del usuario «root» (a blanco, entonces se deshabilitará l permisos para convertirse en usuar Tenga en cuenta que no podrá ver la <i>Clave del superusuario:</i> Mostrar la contraseña en claro Por favor, introduzca la misma contr correctamente. Vuelva a introducir la contraseña para s	idministrador) no debería estar en blanco. Si deja este valor en a cuenta de root creará una cuenta de usuario a la que se le darán io administrador utilizando la orden «sudo». a contraseña mientras la introduce. aseña de superusuario de nuevo para verificar que la introdujo u verificación:
Cambiarse regularmente. La contraseña del usuario «root» (a Dianco, entonces se deshabilitará l permisos para convertirse en usuar Tenga en cuenta que no podrá ver la Clave del superusuario: Mostrar la contraseña en claro Por favor, introduzca la misma contr correctamente. Vuelva a introducir la contraseña para s	idministrador) no debería estar en blanco. Si deja este valor en a cuenta de root creará una cuenta de usuario a la que se le darán io administrador utilizando la orden «sudo». a contraseña mientras la introduce. a seña de superusuario de nuevo para verificar que la introdujo u verificación:
Cambiarse regularmente. La contraseña del usuario «root» (a blanco, entonces se deshabilitará l. permisos para convertirse en usuar Tenga en cuenta que no podrá ver l. <i>Clave del superusuario:</i> Mostrar la contraseña en claro Por favor, introduzca la misma contr correctamente. Welva a introducir la contraseña para s	idministrador) no debería estar en blanco. Si deja este valor en a cuenta de root creará una cuenta de usuario a la que se le darár io administrador utilizando la orden «sudo». a contraseña mientras la introduce. aseña de superusuario de nuevo para verificar que la introdujo u verificación:
Cambiarse regularmente. La contraseña del usuario «root» (a blanco, entonces se deshabilitará l. permisos para convertirse en usuar Tenga en cuenta que no podrá ver la Clave del superusuario: Mostrar la contraseña en claro Por favor, introduzca la misma contr correctamente. Wuelva a introducir la contraseña para s Mostrar la contraseña en claro	idministrador) no debería estar en blanco. Si deja este valor en a cuenta de root creará una cuenta de usuario a la que se le darán io administrador utilizando la orden «sudo». a contraseña mientras la introduce.

Figura 28: Configuración OSSIM AlienVault: Configuración de usuarios Fuente: OSSIM AlienVault

Luego comenzará la instalación del sistema en el disco duro.



Figura 29: Configuración OSSIM AlienVault: Instalación Fuente: OSSIM AlienVault

Una vez que la instalación finalice, se reinicia el servidor para ingresar a la pantalla de inicio de la herramienta OSSIM AlienVault.



Figura 30: Configuración OSSIM AlienVault: Ingreso al sistema (Pantalla de inicio). Fuente: OSSIM AlienVault

Al ingresar el usuario root con su respectiva contraseña se despliega la siguiente pantalla:



Figura 31: Configuración OSSIM AlienVault: Levantamiento de servicios. Fuente: OSSIM AlienVault

Para validar si el servidor se encuentra con acceso local, ingresar en un navegador la IP y si se refleja un mensaje de sitio no seguro, ingresar a Configuración Avanzada y luego acceder a 192.168.0.163 (sitio no seguro)



Figura 32: Configuración OSSIM AlienVault: Entorno web. Fuente: OSSIM AlienVault

Una vez que se ha ingresado a las opciones del punto anterior, se puede visualizar la siguiente

página, para lo cual se debe detallar la información solicitada:

Welcome					
Congratulations on choosing Ali administrator user account.	ienVault as your Unified Security M	lanage	ment tool. Before using your AlienVault, you will need to ci		
If you need more information ab	oout AlienVault, please visit AlienV	/ault.co	om.		
Administrator Accour	nt Creation				
Create an account to access you	r AlienVault product.				
* Asterisks indicate required fields					
FULL NAME *	Jorge Danilo Añazco Bedon	Ð			
USERNAME *	admin	10			
PASSWORD *		10			
	strong				
CONFIRM PASSWORD *		Ð			
	strong				
E-MAIL *	jdanazco.mcib@uisek.edu.ec	0			
COMPANY NAME	Uisek	10			
LOCATION	Ecuador		→ View Map		
☑ Share anonymous usage stati	stics and system information with	Alien	/ault to help us make USM better. Learn More		
	START USING ALIENVAULT				

Figura 33: Configuración OSSIM AlienVault: Creación de cuenta. Fuente: OSSIM AlienVault

Luego de ingresar los datos, damos clic en Start Using AlienVault, lo que permite iniciar sesión.

ALIEN	VAULT	OSSIM 0.163	~
USERNAME	admin	10	
PASSWORD	Forgot Passv	vord?	
	LOGIN		

Figura 34: OSSIM AlienVault : Ingreso AlienVault. Fuente: OSSIM AlienVault

Al ingresar por primera vez por la página web, se debe configurar el servidor de Alienvault.



Welcome to the AlienVault OSSIM Getting Started Wizard

You are about to use this wizard to configure the critical security capabilities provided by AlienVault OSSIM. 1 Monitor Network Configure interfaces and monitor network traffic for threats 3 Collect Logs & Monitor Assets Monitor asset logs and alarm on suspicious activity 2 Discover Assets OSSIM will perform a discovery scan to detect assets 9 0 0 • 🛡 0 ß 7 Once done you'll be ready to use AlienVault OSSIM. Now, go forth! START Skip AlienVault Wizard

> Figura 35: OSSIM AlienVault : Pantalla de inicio. Fuente: OSSIM AlienVault

Para la configuración del servidor, primero la interface de red.

Get Started	Configure Ne	twork Interfaces			
NETWORK INTERFACES	The network inter interfaces you'll n or has the ability	rfaces in AlienVault OSSIM can be configure need to ensure that the networking is config to reach out to the desired network.	d to run Network Monitoring ured appropriately for each ir	or as Log Collecti Iterface so that A	on & Scanning. Once you've configured the lienVault OSSIM is either receiving data passiv
ASSET DISCOVERY					
DEPLOY HIDS	NIC	PURPOSE	IP ADDRESS	STATUS	Information Management: The Management interfac
LOG MANAGEMENT	eth0	Management 🔻	192.168.0.163	-	was configured on the OSSIM Console ar allows you to connect to the web UI. This interface cannot be changed from the we
JOIN OTX					 Network Monitoring: Passively listen for network traffic. Interface will be set to promiscuous mode. Requires a network tap or span. See Instructions on how to setup a network tap or span.
					 Log Collection & Scanning: Collect or receive logs from your assets, run an ass scan, or deploy the HIDS agent. Require routable access to your networks.
					 Not in Use: Use this option if you do no want to use one of the network interface
					· · · · · · · · · · · · · · · · · · ·

Figura 36: OSSIM AlienVault: Configuración interface de red. Fuente: OSSIM AlienVault

La siguiente pantalla, permite agregar los dispositivos de la red y catalogarlos, esto ayudará con un inventario de equipos en el sistema.

Let's Get Started	Scan & Add Assets							
1 NETWORK INTERFACES	In order to begin monitoring can scan your network using	vour environment we m network ranges, import	ust first find a CSV of ass	the assets in your net ets in your network, o	work. There are three r you can add assets r	(3) ways you can add a manually.	ssets to monito	r: you
2 ASSET DISCOVERY	Add Asset Manually							
3 DEPLOY HIDS	Hostname	IP		Select an Asset Type 🔻	+ ADD	SCAN NETWORKS	IMPORT FRO	om csv
4 LOG MANAGEMENT							Search	
	HOSTNAME		r IP			TYPE		
	alienvault		192.168.0	163		Linux X	¥	Ô
	Host-192-168-0-1		192.168.0	1		Network Device 🕷	w.	ŵ
	Host-192-168-0-161		192.168.0	161		Windows ×	¥	Ô
	SHOWING 1 TO 3 OF 3 ASSET	5						T LAST
SKIP ALIENVAULT WIZARD	BACK							NEXT

Figura 37: OSSIM AlienVault: Configuración de *asset*. Fuente: OSSIM AlienVault

En la pantalla que se presenta a continuación, se requiere el usuario y contraseña del administrador de los equipos, para desplegar agente HIDS (Sistema de detección de intrusos en un Host) para monitorear los equipos.

et's Get Started	Deploy HIDS to Servers	
1 NETWORK INTERFACES	For these devices we recommend deploying HIDS in order to perfor machines the HIDS agent will be installed locally, for Unix/Linux env	m file integrity monitoring, rootkit detection and to collect event logs. For windows ronments remote HIDS monitoring will be configured.
2 ASSET DISCOVERY	WINDOWS (1) UNIX / LINUX (3)	
	Enter the domain admin account to install the HIDS agent. The user an agent to the selected assets.	name and password you provide will not be permanently stored, it will be used to deploy
4 LOG MANAGEMENT	Username	Deploy to the following hosts:
5 JOIN OTX	12	🗁 🕒 No data found
	Password	
	Domain (Optional)	
		NEXT

Figura 38: OSSIM AlienVault: Desplegar HIDS Fuente: OSSIM AlienVault

En la siguiente pantalla se solicita las características del dispositivo de red para el manejo de los logs.

Welcome to AlienVault OSSIM				
Let's Get Started	Set up Log Management			
1 NETWORK INTERFACES	During the asset discovery scan we found 1 network devic "Enable" button to enable the data source plugin for each	e on your network. Confirm the vendor, device.	model, and version of the de	evice shown. Click the
2 ASSET DISCOVERY	ACCET	VENDOR	MODEL	VERSION
3 DEPLOY HIDS	ASSE I	VENDOR	MODEL	VERSION
4 LOG MANAGEMENT	Host-192-168-0-1 (192.168.0.1)	D-Link X Y	Unified Wireless X 🔻	- x v
5 JOIN OTX				CHARLE
				ENADLE
SKIP ALIENVAULT WIZARD	BACK			SKIP THIS STEP

Figura 39: OSSIM AlienVault: Manejo y configuración de los logs. Fuente: OSSIM AlienVault

A continuación, se ingresa el código de OTX que permite la integración del sistema

inteligente contra amenazas creado por la comunidad.



Figura 40: OSSIM AlienVault: Configuración OTX. Fuente: OSSIM AlienVault

4.1.2 Configuración e instalación del OSSIM AlienVault

Para realizar ciertas configuraciones del AlienVault se debe ingresar a través del servicio ssh con la IP del servidor, el usuario administrador en este caso root y su respectiva contraseña, al momento de ingresar correctamente se despliega la siguiente pantalla:



Figura 41: OSSIM AlienVault: Configuraciones de preferencias del sistema (AlienVault Setup). Fuente: OSSIM AlienVault

Se procede a configurar el sensor del equipo para que detecte las IPs y realice el monitoreo respectivo, para lo cual, se ingresa a *Configure Sensor* y después se agrega la red, en este caso es la 192.168.0.0/24, y en el caso que se requiera que la herramienta monitoree otras redes, simplemente se ingresa cada red separado por comas.

Network CIDRs
Enter Monitored Networks (CIDRs separated by ,)
i.e. 127.0.0.0/24,192.168.0.0/16
192.168.0.0/24_

Figura 42: OSSIM AlienVault : Configuración de los sensores. Fuente: OSSIM AlienVault

Para guardar los cambios realizados se debe ir al menú principal y seleccionar *Apply all Changes*

AlienVault Setup AlienVault Setup
O System Preferences Configure Sensor Maintenance & Troubleshooting Jailbreak System Support About this Installation Reboot Appliance Shutdown Appliance Apply all Changes
<pre>KAceptar> < Exit ></pre>

Figura 43: OSSIM AlienVault : Guardado de configuraciones. Fuente: OSSIM AlienVault

Para ingresar a la administración del servidor a través de consola se debe dirigir a la opción

Jailbreak System y seleccionar aceptar.

AlienVault Set	AlienVault Setup up							
	0 System Preferences 1 Configure Sensor 2 Maintenance & Troublesbooting							
4	Jailbreak System Support							
5	About this Installation Reboot Appliance Shutdown Appliance							
8	Apply all Changes							
L	_							
	< <mark>Aceptar></mark> < Exit >							

Figura 44: OSSIM AlienVault : Configuración Jailbreak System. Fuente: OSSIM AlienVault

Al ingresar a la consola se puede ingresar los comandos de cualquier servidor basado en

Debian.

🚰 192.168.0.163 - Pu	TTY						
alienvault:/etc	c/nagios3#	uname	-a				
Linux alienvau	lt 4.9.0-1	2-amd6	4 #1 9	SMP Del	bian	4.9.210-1	(2020-01-20) x86_64 GNU/Linux
alienvault:/etc	c/nagios3#	df -h					
Filesystem	Type	Size	Used	Avail	Use%	Mounted o	n
udev	devtmpfs	1.3G		1.3G	0%	/dev	
tmpfs	tmpfs	256M	1.4M	254M	1%	/run	
/dev/sdal	ext4	13G	5.4G	6.8G	45%		
tmpfs	tmpfs	5.0M		5.0M	0%	/run/lock	
tmpfs	tmpfs	1.1G	12K	1.1G	1%	/run/shm	
alienvault:/etc	c/nagios3#						

Figura 45: OSSIM AlienVault : Conexión por ssh. Fuente: OSSIM AlienVault

4.2 Gestión de activos

Se debe ingresar por la interfaz web, se dirige a Entorno y elegir Activos y Grupos

C A No es seguro 192.168.0.163/c	ossim/#dashboard/overview/overview							* 4
			e	IIENVENIDO ADMIN ALIEN	VAULT 192.16	8.0.163 🔀 cc	ONFIGURACIONES SOPORTE SALIR	
	CUADROS DE MANDO	ANÁLISIS	5	ENTORNO		E REPORTS		
	INFORMACIÓN GENERAL			ACTIVOS & GRUPOS			0	
	EXECUTIVE TICKETS SECURITY	TAXONOMY	VULNERABIL	VULNERABILIDADES			/ © ×	
	SECURITY EVENTS: TOP 5 ALARMS	(E) 2		CAPTURA DE TRÁFICO DISPONIBILIDAD	€?		TIVITY IN YOUR ENVIRONMENT	
	No data avallable yet.		95	5%		No	s recent OTX activity.	
				Authentication Availability Access				
	SIEM VS LOGGER EVENTS	@ ?	= 1	OP 10 HOSTS WITH MULTIPLE EVENT	s 🔳 ?	SIEM: EVEN	ITS BY SENSOR/DATA SOURCE	
		\sim					PAM_UNIX ANOMALIES	

Figura 46: Gestión de activos: Consola. Fuente: OSSIM AlienVault

En esta pantalla se despliega los dispositivos que ha detectado OSSIM, para agregar nuevos

se dirige a Añadir Activos y seleccionar Scan for new assets

CUADROS DE MANDO)	ANÁLISIS		ENTO	DRNO	REPORTS		CON	FIGURACIÓN	
ACTIVOS & GRUPOS										0
ACTIVOS GRUPOS DE A	CTIVOS	REDES GRUPOS	DE REDES SCHED	JLE SCAN						
Buscar	Act	ivos						AÑ	ADIR ACTIVOS	Ģ
Tiene alarmas								A&Nt	ilde;Adir Equip Importar CS	o V
Tiene eventos								Impo	rtar Desde SIE For New Asse	M
Vulnerabilidades									Activos	
									Limpiar todos lo	s filtros
	20	 ACTIVOS 								
Connected		NOMBRE EQUIPO	▲ IP	٥	TIPO DE DISPOSITIVO	SISTEMA OPERATIVO	VALOR ACTIVO	VULN SCAN SCHEDULED	♦ HIDS STATUS ♥	
O Disconnected Not Deployed		Host-192-168-0-180	192.168.0.180				2	No	Not Deployed	QI.
vailability Status	0	Host-192-168-0-161	192.168.0.161			Windows XP SP1+, 2000 SP3	2	No	Not Deployed	Ø
O Abajo O Unconfigured		Host-192-168-0-141	192.168.0.141				2	No	Not Deployed	Ø.
Aostrar activos añadidos	0	Host-192-168-0-114	192.168.0.114				2	No	Not Deployed	Q!
O Ultimo Dia O Última semana		Host-192-168-0-109	192.168.0.109			Linux 2.6	2	No	Not Deployed	Ø
O Rango de fechas		Host-192-168-0-1	192.168.0.1		Network Device	Linux 2.6	2	No	Not Deployed	Ø
Jltima actualización ⊖Último Día	•	alienvault	192.168.0.163			AlienVault OS	2	No	Connected	Ø
O Última semana	MOST	RANDO DE 1 A 7 DE 7 AC	TIVOS							

Figura 47: Gestión de activos: Escáner. Fuente: OSSIM AlienVault

En esta pantalla se elige los objetos de red que se desea añadir, en este caso se procede a revisar los dispositivos de la red 192.16.0.0/24, con una búsqueda rápida y con el sensor que viene en el OSSIM AlienVault se escoge las opciones de Resolución de DNS y autodetectar servicios para el escaneo.

CUADROS DE MANDO	ANÁLISIS	ENTORNO	REPORTS	CONFIGURACIÓN
ACTIVOS & GRUPOS			INFORMACIÓN GENERAL	0
ACTIVOS GRUPOS DE ACTIVOS	REDES GRUPOS DE REDES	SCHEDULE SCAN		
		SCAN FOR NEW ASSETS		
		SELECCIÓN DE OBJETIVOS		
	Po	r favor, seleccione los activos que quiera esc	canear	
	192.168.0.0/24 (Local_192_168.1 192.168.0.0/24 (Local_192_168.1 0 Local sensor Launch scan from Automático sensor Lanzar esc v SFLCFC SAST ASSOCIATIZET ESC	2.0.2.4) ESCIPA aquidacute: para → O Todo Ios activo ⊕ @ Activos ⊕ @ Activos	a buscar activos os uctivos edes	
	alienvault [192.168.0.16	3] OPCIONES AVANZADAS		
	Tipo de escaneo: Escaneo rá Plantilla de tiempo: Normal	Fast mode escaneará menos puert	tos que el escaneo por defecto	
	Habilitar resolución DNS			
		INICIAR ESCANEO		

Figura 48: Gestión de activos: Búsqueda rápida Fuente: OSSIM AlienVault Al iniciar el escaneo se puede demorar según el alcance y el número de dispositivos que se encuentran en la red, al momento de encontrarlos se despliega una lista de los equipos, a continuación, se debe guardar con el botón *Update Manager Assets*

RESULTADOS DEL ESCANEO										
EQUIPO	NOMBRE EQUIPO	FQDN 🕑	TIPOS DE DISPOSITIVOS	MAC 2	SO 🤉	SERVICIOS 🔋	FQDN AS HOSTNAME			
192.168.0.1	Host-192-168-0-1	dlinkrouter	General Purpose	10:62:EB:9A:03:38	💧 Linux 3.X	https, domain, http				
192.168.0.109	Host-192-168-0-109	-	Specialized	F8:D0:27:5A:69:81	💧 Linux 2.6.X	netbios-ssn, tcpwrapped, microsoft-ds, tcpwrapped				
192.168.0.114	Host-192-168-0-114			2C:AA:8E:6C:54:D2						
192.168.0.141	Host-192-168-0-141			1C:CC:D6:42:3B:25						
192.168.0.157	Host-192-168-0-157			E4:DB:6D:AB:49:45						
192.168.0.161	Host-192-168-0-161		General Purpose	70:8B:CD:7E:3A:D5	🎥 Windows 2008	msrpc, netbios-ssn, microsoft-ds				
192.168.0.163	alienvault	alienvault.alienvault	General Purpose		👌 Linux 3.X	ssh, mysql, https, http, otp				
192.168.0.180	Host-192-168-0-180		-	04:03:D6:DA:48:F8						
192.168.0.188	Host-192-168-0-188			2C:AA:8E:23:9A:A4						
192.168.0.195	Host-192-168-0-195		Phone, General Purpose	D8:5D:E2:21:23:23	? CyanogenMod 12.X	http				
192.168.0.197	Host-192-168-0-197			0C:FE:45:89:AE:35						
			IMPIAR RESULTADO DEL ES	CANEO UPDATE MA	ANAGED ASSETS					

Figura 49: Gestión de activos: Update Maneger Assets. Fuente: OSSIM AlienVault

Antes de guardar se procede a ingresar la información de la lista, por ejemplo, a qué grupo pertenece, el valor del activo, a qué sensor pertenece y la descripción.

Opcional nombre del grupo	Descripción
Grupo Servidores (Prueba)	Grupo de servidores practica <u>QSSIM</u>
Valor activo *	Activo externo *
5 🗸	🔿 si 💿 No
Sensores *	
✓ 192.168.0.163 (alienvault)	
	CANCELAR GUARDAR

Figura 50: Gestión de activos: Creación de grupos activos. Fuente: OSSIM AlienVault

Luego se regresa a Entorno y se elige Activos y Grupos, en la opción Grupos de Activos se visualiza las diferentes estadísticas del grupo que se acaba de crear, pero hay que mencionar

que se debe activar los módulos Nagios, Snort y OpenVas, para que se refleje las estadísticas de cada opción.

CTIVOS & GF	RUPOS						0
ACTIVOS	GRUPOS DE ACTIVO	OS REDES GRUPO	IS DE REDES SCHEDULE SCAN				
uscar		Grupos de activos					CREATE NEW GROUP
Tiene alarm	as						
Tiene evente	os] Grupos
Vulnerabilid	lades Critico						Limpiar todos los filtros
Valor activo							
	4 5	20 V GRUPOS					ACCIONES -
strar activo Último Día	s añadidos		 PROPIETARIO(S) 	ACTIVOS	ALARMAS	VULNERABILIDADES	EVENTOS
) Último mes Rango de fe	s echas	Grupo Servidores-Prueb	a	11			© 🖋 Ø
tima actualiz O Último Día O Última sem O Último mes O Rango de fi	zación nana s jechas	11		2К	0%	17	0
MÁS EU TROS		Activos	Vulnerabilidades Alarm	as Eventos	Disponibilidad	Servicios	Notas
into Thermos		SHOWING 1 TO 1 OF 1 GROU	JPS			< A	NTERIOR 1 SIGUIENTE >

Figura 51: Gestión de activos: Módulos. Fuente: OSSIM AlienVault

En la opción de Redes, se muestran las redes que se puede escanear con la herramienta.

ACTIVOS & GRUPOS						0
ACTIVOS GRUPOS DE ACT	IVOS REDES GRUPOS DE R	EDES SCHEDULE SCAN				
Buscar	Redes					AÑADIR RED 👻 📑
□ Tiene alarmas						
□ Tiene eventos						1
Uulnerabilidades						Redes
Info Medio Crítico					l	Limpiar todos los filtros
□ Valor activo						
0 1 2 3 4 5						
Mostrar activos añadidos	20 V REDES					ACCIONES +
⊖ Ultimo Día ⊖ Última semana	RED	▲ CIDR	PROPIETARIO(S)	SENSORES ALARMAS	VULNERABILIDADES	EVENTOS
⊖ Ultimo mes ○ Rango de fechas	Local_192_168_0_0_24	192.168.0.0/24		alienvault -		o 🖋 Q
Ultima actualización O Último Día O Última semana Ó Último mes O Rango de fechas	MOSTRANDO DE 1 A 1 DE 1 REDES				< ANTERI	OR 1 SIGUIENTE >
MÁS FILTROS						
	Fig	ura 52: Gestión	de activos: Rec	les		

Fuente: OSSIM AlienVault

Para visualizar las estadísticas de cada dispositivo se dirige a Entorno y se elige la opción de Activos, y en la lista que se despliega se debe ingresar en la opción lupa, que se encuentra en la parte derecha de cada dispositivo.

Host-192-168-0-161	192.168.0.161	General Purpose	Windows 2008	5	No	Not Deployed	<u>Q</u> !

Figura 53: Gestión de activos: Estadísticas. Fuente: OSSIM AlienVault

Al ingresar se despliega toda la información del dispositivo, desde los servicios hasta las vulnerabilidades que tiene, también se puede editar algunas características de cada dispositivo.

CUADROS DE MANDO	ANÁLISIS	ENTORNO	REPORTS	CONFIGURACIÓN
INFORMACIÓN GENERAL ESTADO DESPLIEGUE ABRIR INTERCAMBIO DE	REDES GRUPOS DE REDES	SCHEDULE SCAN		0
AMENAZA Host-192-168-0-161 192.168.0.161 [70:88:CD:7E:3A:D5] Windows 2008 Valor activo 0 1 2 3 4 5 Modelo Desconocido	i po de dispositivo Re neral Purpose Lov	des Sens al_192_168_0_0_24 (192.168 alienv	DTES Ault (192.168.0.163)	ACCIONES - ASSET LOCATION
Tipo activo Interno O Vulnerabilidades O Alarmas	5 Eventos Disponibil	dad 3 Servicios	os O Notas	Coogle Datos de mapas 62020 Términos de uto ENVIRONMENT STATUS HIDS Descubrimiento de activos automático Vuln Scan Scheduled
Descripción Grupo de servidores practica OSSIM VULNERABILIDADES ALARMAS	EVENTOS SOFTWARE SERVICIO	S PLUGINS PROPIEDADES NE	TFLOW GRUPOS	SUCCESTIONS Actualmente no hay sugerencias
10 VULNERABILIDADES	VULNERABILITIES	VULN ID SERVICE	♦ SEVERITY ♦	

Figura 54: Gestión de activos: Dashboard. Fuente: OSSIM AlienVault

Para editar la información del dispositivo, se ingresa a Acciones y luego Editar.



Fuente: OSSIM AlienVault

Al ingresar a la opción Editar se despliega la siguiente pantalla, donde se configura y

actualiza la información del dispositivo.

	Los campos	s marcados con (") son obligatorios
Nombre *		Icono Allowed format: Up to 400x400 PNC, JPC or CIF image
Host-192-16	i8-0-161	Choose icon
Dirección I	P*	Localización
192.168.0.1	61	Undetermined location
		D. C.
Valor activ 5 V Sensores *	o * Activo externo * O Si 🖲 No	Google Datos de mapas ©2020 Google, ORION-ME Términos de uso Latitud/Longitud
Valor activ 5 v Sensores * 2 192.168	o * Activo externo * O Si No 0.163 (alienvault) erativo	Google Datos de mapas 82020 Google, ORION-ME Términos de uad Latitud/Longitud
Valor activ 5 V Sensores * V 192.168 Sistema op Windows 20	o* Activo externo * O Si No 0.163 (alienvault) erativo 08	Google Datos de mapas ©2020 Google, ORION-ME Términos de uso Latitud/Longitud
Valor activ 5 V Sensores * V 192.168 Sistema op Windows 20 Descripció	o* Activo externo * O Si No 0.163 (alienvault) verativo 08	Google Datos de mapas @2020 Google, ORION-ME Términos de uso Latitud/Longitud
Valor activ 5 Sensores * V 192.168 Sistema op Windows 20 Descripció Grupo de se	o * Activo externo * Si No 0.163 (alienvault) rerativo 08 n rvidores practica OSSIM	Coogle Datos de mapas 82020 Google, ORION-ME Términos de uso Latitud/Longitud Modelo Tipos de dispositivos AGREGAR AGREGAR

Figura 56: Gestión de activos: Editar y actualizar. Fuente: OSSIM AlienVault
4.3 Gestión de disponibilidad

Para habilitar el monitoreo en la herramienta hay que ingresar al Módulo de Disponibilidad y dirigirse a Entorno y se elige opción de Activos, en la lista que se despliega, se ingresa en la opción de lupa que se encuentra en la parte derecha de la lista por cada dispositivo, al ingresar se visualiza la información del dispositivo y en Acciones se encuentra la opción para habilitar el monitoreo la opción es *Enable Availability Monitoring*, al hacer clic en esta opción se refleja el mensaje que ya está habilitado el monitoreo.



Figura 57: Gestión de disponibilidad: Activación. Fuente: OSSIM AlienVault

Para habilitar el monitoreo de los servicios se dirige en la parte inferior de la pantalla anterior

y se ingresa a Edit Services.

							EDIT SERVICES
10 V SERVICIOS							LOTT SERVICES
IP ADDRESS	PORT	 PROTOCOL 	NAME	٥	STATUS	٥	MONITORING
Host-192-168-0-161 (192.168.0.161)	135	tcp	msrpc		-		No
Host-192-168-0-161 (192.168.0.161)	139	tcp	netbios-ssn				No
Host-192-168-0-161 (192.168.0.161)	445	tcp	microsoft-ds				No

Figura 58: Gestión de disponibilidad: Editar servicios. Fuente: OSSIM AlienVault

Se despliega la lista de servicios que tiene el servidor, y en la columna Monitorizando, se tiene la opción para habilitar el monitoreo de servicios.

IT SERVICES		<i>a</i>				
dd New Service 192.168.0.161 Enter Port	Protocolo 👻	Enter Service			GUARDAR	
arch by service						SAD - D
DIRECCIÓN IP	PUERTO 🗘 I	PROTOCOLO \$	NOMBRE \$	ESTADO	MONITORIZANDO	ACCIONES
DIRECCIÓN IP	PUERTO \$	PROTOCOLO 🗘	NOMBRE \$	ESTADO	MONITORIZANDO	ACCIONES
DIRECCIÓN IP Host-192-168-0-161 (192-168.0.161) Host-192-168-0-161 (192-168.0.161)	PUERTO 0 1 135 139	tcp tcp	NOMBRE 🗢 msrpc netblos-ssn	ESTADO	MONITORIZANDO	ACCIONES

Figura 59: Gestión de disponibilidad: Servicios. Fuente: OSSIM AlienVault

Al habilitar el monitoreo de los servicios se actualiza la información de los paneles, como se muestra a continuación:



Figura 60: Gestión de disponibilidad: Paneles de información. Fuente: OSSIM AlienVault Para visualizar las estadísticas globales de monitoreo se dirige a Entorno y se elige la opción de disponibilidad.



Figura 61: Gestión de disponibilidad: Estadísticas globales. Fuente: OSSIM AlienVault

Al ingresar se despliega la información de todos los dispositivos que se encuentran en el monitoreo sus respectivos servicios.

ONITORIZANDO	INFORM	IES												
		D	ETALLE DEL INTERRU	SERVICIO DET PCIONES LA REI	ALLE EQUIPO D D COMENTARIO	ESCRIPCIÓN DE E	STADO MALI TO INFORMA	LA DE ESTADO ICIÓN DE PRO) MAPA DE E CESOS INFOI	TADO PE MACIÓN I	OBLEMAS DE FUNCIÓ	DE SERVICI	O PROBLEM LISTA DE F	MAS DE PROGRA
W CEDVICE STATIS			TCROURE			Host Status	Totals				ervice S	tatus Tota	ls	
W SERVICE STATUS W HOST STATUS D W STATUS SUMMA	RY FOR ALL	ALL HOST (HOST GROUPS	GROUPS		Up [Down Unreach 0 0	able Pendi 0	ng	Ok 9	Warning 0	j Unkr	own Cri	tical Pene	ding 0
						All Problems	All Types			A	ll Problen			
					Service (o Overview Fo	2 All Host	Groups			0	9	963	
Grupo	Servidores-P	rueba (Gri	upo Servido	res-Prueba)	Service (0 Overview For All Server	2 r All Host	Groups	Debi	an GNU/Li	0 nux Serve	rs (debian-s	ervers)	
Grupo	Servidores-P	rueba (Gri	ipo Servido Services	res-Prueba) Actions	Service C	0 Overview For All Server: Status	2 r All Host s (all) Services	Groups	Debi Host	an GNU/Li Statu	0 nux Serve	rs (debian-s	ervers)	
Grupo Host-192	Servidores-P lost -168-0-161	rueba (Gri Status UP	ipo Servido Services 3 OK	res-Prueba) Actions	Service C	0 Overview For All Server Status 8-0-161 UP	2 r All Host s (all) Services 3 OK	Groups	Debi Host localhost	an GNU/Li Statu	0 nux Serve s Servi	rs (deblan-s ces Acti	ervers) ons	
Grupo Host-192	Servidores-P tost !-168-0-161	rueba (Gri Status UP	upo Servido Services 3 OK	res-Prueba) Actions	Service C Host Host-192-168 localhost	OVERVIEW FOR All Server Status 8-0-161 UP OUP	2 r All Host s (all) Services 3 OK 6 OK	Groups Actions 역 을 몲 역 을 몲	Debi Host localhost (an GNU/Li Statu UP	0 nux Serve s Servi 6 C	rs (deblan-s ces Acti	ervers) ons	
Grupo Host-192	Servidores-P lost I-168-0-161 HTTP s	rueba (Gri Status UP servers (ht	upo Servido Services 3 OK tp-servers)	res-Prueba) Actions 《 🔒 品	Service C Host Host-192-168 localhost	0 Overview For All Server Status 4-0-161 UP 0 UP microsoft-ds (m	2 All Host (all) Services 3 OK 6 OK (crosoft-ds)	Actions	Debi Host localhost (an CNU/Li Statu UP	0 nux Serve s Servi 6 C	rs (debian-s ces Acti K	ervers) ons	
Grupo Host-192	Servidores-P tost I-168-0-161 HTTP s Statu	rueba (Gri Status UP ervers (ht s Servi	ipo Servido Services 3 OK tp-servers) ces Acti	res-Prueba) Actions	Service (Host Host-192-168 localhost	OVERVIEW FO	2 All Host (all) Services 3 OK 6 OK (crosoft-ds) Services	Actions 옥 을 몰 Actions	Debi Host localhost (an GNU/Li Statu UP	0 nux Serve s Servi o C nsrpc (ms Status	rs (debian-s ces Acti K Q	ervers) ons	
Crupo Host-192 Host-192 localhost	Servidores-P tost P-168-0-161 HTTP s Statu C UP	rueba (Gri Status UP ervers (ht s Servi ō C	ipo Servido Services 3 OK (p-servers) ces Acti K	res-Prueba) Actions Actions	Service C Host Host-192-168 localhost Host-192-168	OVERVIEW FOR All Server Status I-0-161 UP microsoft-ds (m Status Status Status	2 All Host (all) Services 3 OK (crosoft-ds) Services 3 OK	Actions	Debi Host localhost (Host-192-1	an GNU/Li Statu UP ;t 68-0-161	0 nux Serve s Servi 6 C status UP	rs (deblan-s ces Acti K Q I Services 3 OK	ervers) ons Actions	L
Grupo Host-192 Host-192 Iocalhost	Servidores-P lost -168-0-161 HTTP s Statu : O UP netbi	rueba (Gri Status UP ervers (ht s Servi 6 C os-ssn (nei	upo Servido Services 3 OK tp-servers) ces Acti K Q S blos-ssn)	res-Prueba) Actions 오 을 몰 ons	Service (Host Host-192-168 localhost Host-192-168	OVERVIEW FOR All Server Status 5-0-161 UP OUP microsoft-ds (m Status 5-0-161 UP SSH servers (ss	2 All Host s (all) Services 3 OK 6 OK Services 3 OK h-servers)	Actions	Debi Host localhost (Host-192-1	an CNU/Li Statu UP it 68-0-161	0 nux Serve s Servi 6 C nsrpc (ms Status UP	rpc)	ervers) ons 요. Actions	Ŀ

Figura 62: Gestión de disponibilidad: *Dashboard*. Fuente: OSSIM AlienVault

Los servicios que se encuentran disponibles están en verde, los que presenten algún problema cambiarán de color a rojo o a naranja, según el estado del servicio o del dispositivo.



Figura 63: Gestión de disponibilidad: Verificación de servicios. Fuente: OSSIM AlienVault

Una de las funcionalidades de este módulo es la creación de informes, ya sea por dispositivos o grupos de dispositivos, por servicio o grupo de servicios y por el estado, para esta función se ingresa a informes tendencias, se elige el dispositivo, el lapso de tiempo y las características del informe, cabe señalar que existe varios tipos de gráficos para la generación de informes, según las necesidades del administrador.



Figura 64: Gestión de disponibilidad: Informes. Elaborado por: Jorge Añazco

4.4 Gestión de notificaciones

Para configurar el envío de notificaciones de Nagios, se ingresa al servidor por ssh y como primer requisito se establece los contactos que se enviara las notificaciones, para editar los contactos se ingresa a /etc/nagios3/conf.d/contacts_nagios2.cfg.



Figura 65: Gestión de notificaciones: Configuración. Fuente: OSSIM AlienVault (Nagios)

Para aplicara los cambios se reinicia el servicio de Nagios.



Figura 66: Gestión de notificaciones: Configuración nagios. Elaborado por: Jorge Añazco

Según las necesidades del administrador se puede configurar el servicio de mail saliente ya que puede ser sendmail o Postfix, en la instalación por defecto de la herramienta OSSIM AlienVault se encuentra por defecto Postfix como servidor de correo, pero con el comando dpkg-reconfigure postfix o dpkg-reconfigure sendmail se puede establecer y configurar el servidor de correo.



Figura 67: Gestión de notificaciones: Configuración correo nombre del sistema (1). Fuente: OSSIM AlienVault



Figura 68: Gestión de notificaciones: Configuración correo remitente (2). Fuente: OSSIM AlienVault



Figura 69: Gestión de notificaciones: Configuración correo dominio (3). Fuente: OSSIM AlienVault



Figura 70: Gestión de notificaciones: Configuración correo redes (4). Fuente: OSSIM AlienVault



Figura 71: Gestión de notificaciones: Configuración correo protocolo de internet (5). Fuente: OSSIM AlienVault

Después de la configuración del servidor de correo, se realiza la prueba de envío del mail

con el comando mail.



Figura 72: Gestión de notificaciones: Envió de prueba de correo. Elaborado por: Jorge Añazco

Al realizar pruebas de disponibilidad del servicio, al momento que exista un problema el nagios notificará al mail.

	🛪 inglés 🗕 🗲 chino 🚽 Traducir mensaje
**	*** Nagios *****
N	otification Type: PROBLEM
Si Hi Ai St	ervice: PING ost: My Linux Server ddress: 64.46.64.254 tate: CRITICAL
D	ate/Time: Fri Dec 14 09:41:21 ECT 2012
A	dditional Info:
DI	ING CRITICAL - Packet loss = 1% RTA = 113 76 ms

Figura 73: Gestión de notificaciones: Correo de prueba. Elaborado por: Jorge Añazco

Para editar el contenido de las notificaciones vía mail, se puede hacer el cambio en el archivo /etc/nagios3/commands.cfg, se agrega más métodos de notificación por vía SMS y por whatsapp.



Figura 74: Gestión de notificaciones: Configuración correo reglas nagios. Elaborado por: Jorge Añazco

4.5 Gestión de vulnerabilidades

Para ingresar a la gestión de vulnerabilidades se dirige a Entorno y se selecciona Vulnerabilidades.

ACTIVOS & GRUPOS
VULNERABILIDADES
NETFLOW
CAPTURA DE TRÁFICO
DISPONIBILIDAD
DETECCIÓN

Figura 75: Gestión de vulnerabilidades: Ingreso. Fuente: OSSIM AlienVault

Al ingresar en el panel vulnerabilidades, se dirige a trabajos de escaneo para comenzar con

la programación del escaneo de vulnerabilidades.

CUADROS DE MANDO	ANÁLISIS	ENTORNO	REPORTS	CONFIGURACIÓN
VULNERABILIDADES		•		Ø
INFORMACIÓN GENERAL TRABA	JOS DE ESCANEO BASE DE DATOS DI	E AMENAZAS		
POR GRAVEDAD POR SERVICIOS	- TOP 10	TOP 10 EQUI	POS TOP 10 REDES	PERFILES CONFIGURACIONES
,	No hay resultados		No hay resultados	
Vulnerabilidades actuales NUEVO TRABAJO DE ESCANEO	DET. [No se encontraron resultac	ALLES DE LAS VULNERABILIDADES DEL EQU	IPO O servicio O Texto libre BUSCAR de vulnerabilidades ahora	
► REPORT HISTORY				

Figura 76: Gestión de vulnerabilidades: *Dashboard*. Fuente: OSSIM AlienVault

En esta pantalla hay que ingresar a nuevo trabajo de escaneo, para programar un escaneo de vulnerabilidades a un activo o dispositivo.

	BASE DE DATOS DE AMENAZAS	TRABAJOS DE ESCANEO	INFORMACIÓN GENERAL
PERFILES CONFIGURACIONES		IMPORTAR FICHERO NBE	NUEVO TRABAJO DE ESCANEO
	ESCANEOS EJECUTÁNDOSE		
	No hay trabajos ejecutándose		
	TRABAJOS PROGRAMADOS		
	No hay trabajos programados		
	TODOS LAS ESCANEOS		
	No hav trabains		

Figura 77: Gestión de vulnerabilidades: Escaneo de vulnerabilidades. Fuente: OSSIM AlienVault

En la pantalla *CREATE SCAN JOB*, se puede realizar varios tipos de escaneo, desde un escaneo exhaustivo, personalizado y con niveles profundidad hasta un escaneo rápido, también se puede dejar tareas programadas para que se ejecute en un periodo de tiempo, por último, se puede escanear a varios activos a la vez.

No Se Pri Sc Ex Ex Ex C	ombre del trabajo: elect Sensor: chedule Method: VANZADO xclude Ports: Only scan hosts that are live (greatly speeds up the only scan hosts that are live (greatly speeds up the Pre-Scan locally (do not re-scan from scanning nixor) No resolver nombres	CREATE SCAN JOB Win10-test alienvault[192.166.0.163] Default - Non destructive Full and Fast scan Immediatamente Escriba aquí para buscar activos Host-192-168-0-161 (192.166.0.161) Immediatamente
No Se Pri Sc EX EX EX EX	ombre del trabajo: elect Sensor: rofile: chedule Method: VANZADO veclude Ports: Only scan hosts that are ranning process) Only scan bosts that are ranning process) Pre-scan locally (do not rescan from scanning moor) No resolver nombres	Win10-test alienvault[192.166.0.103] Default - Non destructive Full and Fast scan Immediatamente Immediatamente Escriba aqui para buscar activos Host-192-168-0-101 (192.168.0.101) Immediatamente
		Image: Second
		GUARDAR CONFIGURACIÓN DE LOS RESULTADOS
192.168.0.161	Host-192-168-0-161	UDJETIVO PERMITIDO SENSORES SENSOR PERMITIDO ESCANED NIMAP CAR 192.168.0.163 [alienvault]

Figura 78: Gestión de vulnerabilidades: Programar un trabajo de escaneo. Fuente: OSSIM AlienVault

Para guardar el informe o reporte de escaneo se debe esperar hasta que termine el proceso para que aparezca la opción de guardado.

	NOMBRE DEL TRABAJO	PROPIETARIO	DURACIÓN DEL ESCANEO	PROGRESO	ACCIÓN
🔀 Win10-test		admin	RUN >5 mins	9496	•

Figura 79: Gestión de vulnerabilidades: Progreso de escaneo. Fuente: OSSIM AlienVault

Al momento de terminar el escaneo, se genera el reporte de vulnerabilidades, también se

visualiza un resumen del proceso de escaneo, como puede ser el tiempo de duración y las fechas.

ESTADO	NOMBRE DEL TRABAJO	TIEMPO DE LANZAMIENTO	TIEMPO INICIO ESCANEO	TIEMPO FIN ESCANEO	DURACIÓN DEL ESCANEO	SIGUIENTE ESCANEO	ACCIÓN
Completado	Win10-test	2020-07-02 02:15:56	2020-07-02 02:16:02	2020-07-02 02:26:26	10 mins		(18) 📷 🍪 🛋 📩 🔝

Figura 80: Gestión de vulnerabilidades: Escaneo completado. Fuente: OSSIM AlienVault

Al momento que se genera el reporte se exportar o guardar en formato de tipo web, pdf,

Excel, a continuación, se visualiza el reporte web que se genera:



Figura 81: Gestión de vulnerabilidades: Informe de escaneo. Fuente: OSSIM AlienVault

En el reporte indica un estado de las vulnerabilidades en un diagrama de pastel, cada tipo de vulnerabilidad es representado por un color, por ejemplo, las vulnerabilidades serias de color morado, las vulnerabilidades altas de color rojo, las vulnerabilidades medias de color amarillo, las vulnerabilidades bajas de color azul y las vulnerabilidades que solo son informativas o de advertencia de color verde, esta información también se puede visualizar en la opción de Información General, además de ver los escaneos anteriores de otros activos.

UNINACION GENERAL	SCANED BASE DE DATOS	DE AMENAZAS							
R GRAVEDAD POR SERVICIOS - TOP 10			TOP 10 EQUIPO	DS TOP	10 REDES			PERFI	LES CONFIGURACIO
	Medium [1] Low [1] Info [16]			Host	:-192-168-0-	161 [18]			
B.									
EFF.	D	ETALLES DE LAS VULNERA	BILIDADES DEL EQUIF	0					
terabilidades actuales	D	ETALLES DE LAS VULNERA	BILIDADES DEL EQUIF	PO Diservicio O	Texto libre	BUSC	AR		
erabilidades actuales TO TRABAJO DE ESCANEO EQUIPO - IP	DI	TALLES DE LAS VULNERA	BILIDADES DEL EQUIF	D D servicio O	Texto libre	BUSC	AR		
IN TRABAJO DE ESCANEO EQUIPO - IP All	DI	TALLES DE LAS VULNERA PROPIETARIO	BILIDADES DEL EQUIF	10 D Servicio (C) Intern 0	Texto libre	e BUSC	AR EGOV	960	

Figura 82: Gestión de vulnerabilidades: Representación de las vulnerabilidades. Fuente: OSSIM AlienVault

4.6 Gestión de riesgos

Para ingresar al módulo de gestión de riesgos, se dirige a la parte de Análisis, a la opción de Eventos SIEM.



Figura 83: Gestión de riesgos: Ingreso. Fuente: OSSIM AlienVault

Al ingresar se despliega una lista de los diferentes eventos de seguridad detectados por los diferentes módulos de OSSIM AlienVault, en esta pantalla se visualiza el riesgo, la descripción, el origen, el destino y el grado del riesgo detectado.

EVENTOS SIEM								0
SIEM TIEMPO-REAL								
Buscar Nombre del evento	✓ <a>R							¥
MOSTRAR EVENTOS ORÍGENES DE DA	TOS	GRUPOS DE AC	TIVOS		OTX IP REPUTATION		CLEAR FILT	
Last Hour				•	•	Last Hour 😠		
O Último Día DATA SOURCE GR	ROUPS	GRUPOS DE RE	DES		OTX PULSE			
🔿 Última semana	•			•	Pulse name			
O Último mes SENSORES		RIESGO						
O Rango de fechas	~			~	ONLY OTX PULSE ACTIVITY			
Userdata1 field	10					BÚSQUEDA	AVANZADA	
userdata1 V like V								
EVENTOS AGRUPADOS LÍNEA DE TIEMPO MOSTRAR 50 v ENTRIES MOSTRAR GRÁFICO DE TENDENCIAS Off Off						CHANGE VIEW +	ACCION	ES 🔹
DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS.						9.321 EVENTOS EN TOTA	EN BASE DE	DATOS
NOMBRE DEL EVENTO	▼ FECHA GMT-5:00	SENSOR	ОТХ	ORIGEN	DESTINO	ACTIVO S 🌩 D	RIESGO	
AlienVault HIDS: System running out of memory. Availab ility of the system is in risk.	2020-07-02 19:39:29	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)	Ø
AlienVault HIDS: Login session closed.	2020-07-02 19:37:59	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)	Q
AlienVault HIDS: Login session closed.	2020-07-02 19:37:59	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)	Ø.
🛷 🔲 sudo: Session closed	2020-07-02 19:37:58	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)	Ø
🛷 🔲 sudo: Session closed	2020- <mark>07-02 19:37:57</mark>	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)	Ø
🛷 🔲 SSHd: Session disconnected		- Vice - Inc.						
	2020-07-02 19:37:57	allenvauit	N/A	alienvault:5916	4 alienvault:22	5->2	LOW (0)	<u>Ó</u>

Figura 84: Gestión de riesgos: *Dashboard*. Fuente: OSSIM AlienVault

Para ver su funcionamiento se realiza una prueba para la detección de eventos de seguridad

simplemente tratando de ingresar al servidor con un usuario que no existe.

	國 192.168.0.163 - PuTTY
	2 login as: juan 2 juan@192.168.0.163's password: 2 Access denied 2 juan@192.168.0.163's password:
🛊 🗌 SSHd: Failed password	2020-07-02 19:45:52 alienvault N/A Host-192-168-0-161:54619 0.0.0.022 5->2 (MED:1))

Figura 85: Gestión de riesgos: Prueba de detección. Elaborado por: Jorge Añazco

Al dar clic en el evento se reflejará una pantalla con los detalles del evento de seguridad.

SSH:F. Bield password: 2050-07-02 16 45 52 CMT-5:00 Autemication:				
FECHA 20200-702 10 45 52 CMT-500 Audemication Audemication ALERVAULT SENSOR alemaski [192166.161] SUBCATECORIA Raided IP DISPOSITIVO 120166.161 [160] SUBCATECORIA Raided ID TIPO EVENTO 1 DORIGEN DE DATOS sh PROTOCOLO TCP DE RENTO DIALINFO Inv/ ORICEN FABILIDAD RESCO OTX INDICATORS ID TIPO EVENTO Exertition Science Sentitions Nomes 0 ID TIPO EVENTO TOP ID TIPO EVENTO ID TIPO EVENTO ID TIPO EVENTO TOP ID TIPO EVENTO ID TIPO EVENTO ID EVENTO DINICOP TOP ID TIPO EVENTO ID TIPO EVENTO ID TIPO EVENTO TOP ID TIPO EVENTO ID TIPO EVENTO ID TIPO EVENTO TOP ID TIPO EVENTO ID TIPO EVENTO ID TIPO EVENTO TOP ID TIPO EVENTO ID TIPO EVENTO ID TIPO EVENTO ID TIPO EVENTO ID TIPO EVENTO ID TIPO EVENTO ID TIPO EVENTO ID TIPO EVENTO ID TIPO EVENTO ID	SHd: Failed password			
ALIBANAULT SIBSOR alexaudt [192:168.013] Alexaudt [192:168.013] SUBCATECORIA neid 19 DEPOSITIVO 102:168.0163 [m0] NOMEE DE CRICIN DE DATOS sh3 10 THO LEVENTO 1 Contex De DATOS contex De DATOS contex De DATOS 10 THO LEVENTO 1 Contex De DATOS contex De DATOS contex De DATOS 10 THO LEVENTO 1 Contex De DATOS contex De DATOS contex De DATOS 10 THO DE DATOS Contex De DATOS contex De DATOS contex De DATOS contex De DATOS 10 THO DE DATOS Contex De DATOS contex De DATOS contex De DATOS contex De DATOS 10 THO DE DATOS 2 Contex De DATOS contex De DATOS contex De DATOS 10 THO DE DATOS 1000 THO DE DATOS DE DATOS contex De DATOS contex De DATOS 10 THO DE DATOS 2 Contex De DATOS contex De DATOS contex De DATOS 10 THO DE DATOS Localización: N/A Denders De DATOS Contex De NA Contex De NA 10 THO DE DATOS Secondarders Pruebas Contex De NA Contex De NA 10 THO DE DATOS Localización: N/A Contex De NA Contex De NA 10 THO DE DATOS Secondarders Pruebas Contex De NA Contex De NA 10 Han	FECHA	2020-07-02 19:45:52 CMT-5:00	CATEGORÍA	Authentication
IP DSPOSITIVO 192.168.0.163 [end] NOMERE DE DATOS snh ID TAPO EVENTO 1 DO DECENTO 0.03 ID EVENTO ÚNICO2 bottol 1.62060 000-07.86 lebote.200400 DO DE PRODUCTO snr ID TOPO EVENTO total 1.62060 000-07.86 lebote.200400 DO DE PRODUCTO snr ID TOPO EVENTO total 1.62060 000-07.86 lebote.200400 DO DE PRODUCTO snr ID TOPO EVENTO total 1.62060 000-07.86 lebote.200400 Total 1.62060 000 Snr ID TOPO EVENTO TOP NOMERE DE DATOS snr ID TOPO EVENTO TOP Snr Total 1.62060 000 ID TOPO EVENTO TOP TOP OTONOALI INFO NO ID TOPO EVENTO TOP TOP TOP TOP TOP ID TOPO EVENTO TOP TOP TOP TOP TOP TOP ID TOPO EVENTO TOP TOPO EVENTO TOPO TOPO INALI INFO TOPO TOPO INALI INFO TOPO TOPO INALI INFO TOPO TOPO INALI INFO TOPO TOPO INFORMALI INFO TOPO TOPO INFO	ALIENVAULT SENSOR	alienvault [192.168.0.163]	SUBCATECORÍA	Failed
101 F02 EVENTO 1 603 102 EVENTO ÚNICO2F 505 505 ROTOCOLO To* 100 EVENDO ÚNICO 100 EVENDO ÚNICO 3 2 100 EVENDO ÚNICO 0 ORCEN HOST 202 EVENDO ÍN // EVENDO ÚNICO 0 0 Nombre equipo: 10x1 102:168:0.161 [192:168:0.161 [1	IP DISPOSITIVO	192.168.0.163 [eth0]	NOMBRE DE ORIGEN DE DATOS	ssh
ID EVINTO ÚNICOS serviros apulgos 2,759 48bbb.2054200 PROTOCOLO TOP TOP TOP TOPOLO Serviros APULGADO SERVIROS APULGADOS	ID TIPO EVENTO		ID ORIGEN DE DATOS	4003
PROTOCOLO TCP ADDITIONAL INFO N/A PRIORIDAD PRALIUAD RESCO OTX INDICATORS 3 2 MEMORIA 0 ORIGEN Nontro sequipo: Host-192-168-0-161 [192,168.0.161 [192,168.0	ID EVENTO ÚNICO#	bcc611ea-b296-0800-27a9-8bbc8c204d20	TIPO DE PRODUCTO	Server
PROBLOAD PAILUDAD RESCO OTX INDICATORS 3 2 MECEN 0 0RGEN Hosts122/168/0161 [192.168.0161] 0 0 0RGEN Hosts122/168/0161 [192.168.0161] DESTIO 0 0RGEN Localización: N/A Dirección MAC: 708 CD/2E1A/DS Contexto: N/A Conpos de activos: N/A Dirección MAC: 1/2, 168,0,0,24 Username & Domain: N/A Username & Domain: N/A Username & Domain: N/A Username & Domain: N/A Username & Domain: N/A Logged Users: N/A Logged Users: N/A Username & Domain: N/A Contexto: N/A Logged Users: N/A Username & Domain: N/A Contexto: N/A Logged Users: N/A Username & Domain: N/A Contexto: N/A Logged Users: N/A Logged Users: N/A Contexto: N/A Logged Users: N/A Logged Users: N/A Contexto: N/A Logged Users: N/A Logged Users: N/A Contexto: N/A Logged Users: N/A 1 SERVICIO PUERTO PROTOCOLO SERVICIO PUERTO PROTOCOLO 5 SERVICIO PUERTO PROTOCOLO SERVICIO PUERTO PROTOCOLO NOMERE DE USUARIO USEDATAI USEDATAI USEDATAI USEDATAI	PROTOCOLO	тср	ADDITIONAL INFO	N/A
Nomese guipo: No Nuesta 192 (182,016) Nuesta 192 (182,016) DESTINO O ORCEN Hossi 192 (182,016) [192,163,0,16] DESTINO Contexts: N/A Derection MAC: 70,85 CD 7E3A D5 Contexts: N/A Contexts: N/A Contexts: N/A Dimma: struit/acide: N/A Contexts: N/A Contexts: N/A Contexts: N/A Discrection MAC: 70,85 CD 7E3A D5 Contexts: Crupo Sendores Privaba O Dimma: struit/acide: N/A Rodes: struit/a Contexts: N/A Discrection MAC: N/A Logged Users: N/A Contexts: N/A Username & Domain: N/A Logged Users: N/A Logged Users: N/A Valor activo: 5 OTIX IP Reputation: No SERVICIO< •	PRIORIDAD	ELABLIDAD.	815500	
ORCEN Hoss:192:168-0161 [192.168.0.161] DESTINO Contexto Contexto Nombre equipo: Hoss:192:168-0161 Localización: N/A Contexto: N/A Dirección MAC: 708 (CD/F2:A DS) Contexto: N/A Contexto: N/A Contexto: N/A Nombre equipo: N/A Dirección MAC: N/A Contexto: N/A Contexto: N/A Contexto: N/A Contexto: N/A Contexto: N/A Utername & Domain: N/A Logal Users: N/A Logal Users: N/A Contexto: N/A Contexto: N/A Contexto: N/A Contexto: N/A Contexto: N/A Contexto: N/A Utername & Domain: N/A Logal Users: N/A Logal Users: N/A Contexto: N/A Contexto: N/A Contexto: N/A Contexto: N/A Sternco PUERTO PROTOCOLO Sternco PUERTO PROTOCOLO Sternco PUERTO PROTOCOLO Sternco PUERTO PROTOCOLO NOMBER DE USUARIO USEDATAL USEDATAL USEDATAL USEDATAL	3	2	MED (1)	0
ORICEN Host-192-168-0.161 [192,163.0.161] DESTINO OESTINO Nombre equipo: Not-1-92-168-0.161 in Localización: N/A Dirección MAC: 708 CD: 723.AD 5 Contractor: N/A Contractor: N/A Contractor: N/A Pietro: 54619 Chupos de activos: Crupo Sendores-Prueba Direcand MAC: 708 CD: 723.AD 5 Crupos de activos: N/A Pietro: 54619 Chupos de activos: N/A Contractor: N/A Pietro: 54619 Chupos de activos: N/A Contractor: N/A Pietro: 54619 Chupos de activos: N/A Contractor: N/A Valor activo: 5 OTX.IP Reputation: No Contractor: N/A Valor activo: 5 Pietro: 2 OTX.IP Reputation: No SERVICIO Puetro: 2 OTX.IP Reputation: No SERVICIO Puetro: 2 OTX.IP Reputation: No SERVICIO Puetro: 2 OTX.IP Reputation: No				
Nomber & gupo: Hort-192:163-0-161 Localización: N/A Localización: N/A Dirección MAC: 70-86 CD-7E3A-D F Contexto: N/A Contexto: N/A Puerto: 5419 Contexto: N/A Contexto: N/A Utima atcalización: N/A Refers: N/A Contexto: N/A Utima atcalización: N/A Refers: N/A Contexto: N/A Utima atcalización: N/A Refers: N/A Contexto: N/A Valor activo: 5 OTX: IP Reputation: No OTX: IP Reputation: No SERVCIO PUENTO © PROTOCOLO © SERVCIO PUENTO © PROTOCOLO SERVCIO Nomere DE USUARIO USERDATAL USERDATAL	ORIGEN	Host-192-168-0-161 [192.168.0.161]	DESTINO	
SERVICIO PUERTO © PRIOTOCOLO © SERVICIO PUERTO © PRIOTOCOLO No services available <	Nombre equipo: host-192-188-0-181 Dirección MAC: 508:CD:F2:3A:D5 Pierto: 54619 Última actualización: N/A Username & Domain: N/A Valor activo: 5	Localización: N/A Contexto: N/A Grupos de activos: Crupo Servidores-Prueba Redes: Local, 192,168,0,0,24 Logad Users: N/A OTX IP Reputation: No	Nombre equipo: N/A Dirección MAC: N/A Puerto: 22 Última actualización: N/A Username & Domain: N/A Valor activo: 2	Localización: N/A Contexto: N/A Crupos de activos: N/A Redes: N/A Logged Users: N/A OTX IP Reputation: No
No services available No services available USERDATA1 USERDATA2	SERVICIO A PUERTO	♦ PROTOCOLO ♦	SERVICIO	PUERTO \$ PROTOCOLO
NOMERE DE USUARIO USERDATA1 USERDATA2	No servic	es available		No services available
NUMBRE DE USUARIO USERUATAT USERUATAZ				
invalid user alienvault	Iuan	invalid user		alienvault
RAWLOG		RAW LOG		
RAINLOG		RAW LOG		

Figura 86: Gestión de riesgos: Evento de seguridad. Fuente: OSSIM AlienVault

En la pantalla principal de los Eventos SIEM, también existe la opción de filtrar los eventos

según las necesidades del administrador, también pueden ser agrupados por el tipo de evento.

EV	ENTOS AGRUPADOS LÍNEA DE TIEMPO					
GRUPC	IS DE EVENTOS POR Nombre del ever					ACCIONES -
DISPLA	YING 1 TO 19 OF 19 EVENTS.					9.492 EVENTOS EN TOTAL EN BASE DE DATOS
	NOMBRE DEL EVENTO		ORG. ÚNICO #	DESTINO ÚNICO #	ÚLTIMO EVENTO	GRÁFICO
	sudo: Session opened	62	1	1	2020-07-02 19H	8n2 Jul 19n2
	sudo: Session closed	60	1	1	2020-07-02 19H	1 (101
	SSHd: Session disconnected	57	1	1	2020-07-02 19H	8n2 Jul 19n2
	AlienVault HIDS: Login session closed.	51	1	1	2020-07-02 19H	Re ² Iul 1000
	AlienVault HIDS: Login session opened.	35	1	1	2020-07-02 19H	n - j
	AllenVault HIDS: System running out of memory. Availability of the system is in risk.	10	1	1	2020-07-02 19H	0 m m_p0
	SSHd: Connection closed	6	1	1	2020-07-02 19H	0 10 2 3 1 19 12 3 1 19 12 3 1 19 12 3 1 19 12 3 1 19 12 3 1 19 12 3 1 19 12 3 1 19 12 3 1 19 12 3 1 19 12 3 1
	AlienVault HIDS: Attempt to login using a non-existent user	2	2	1	2020-07-02 19H	
	SSHd: Invalid user	1	1	1	2020-07-02 19H	
	AllenVault HIDS: Integrity checksum changed.	1	1	1	2020-07-02 19H	onz.jui 1982)
D order=0	AlienVault HIDS: User login failed. ccur_d#null_aux_div	1	1	1	2020-07-02 19H	enc.pli 1962)

Figura 87: Gestión de riesgos: Filtrar eventos. Fuente: OSSIM AlienVault

En la parte de la Línea de tiempo se observa de manera más exacta los eventos de seguridad y cuándo se detectaron.

EVENTOS AGRUPADOS LÍNEA DE TIEMPO RESOLUCIÓN LÍNEA DE TIEMPO: O SEGUNDOS IMINUTOS O HORAS	O días eventos para dibujar: 50 v
18br	primer evento último evento
19 19 19 19 19 19 19 19 19 19 19 19 10 11 11 12 13 14 15 16 17 18 19	SSHd. Session disconnected sudo: Session copend sudo: Session copend AllenVaul HIDS: Login session copend. SSHd. Session disconnected sudo: Session copend. SSHd. Session disconnected sudo: Session copend. AllenVaul HIDS: Login session copend. AllenVaul HIDS: Login session copend. AllenVaul HIDS: Login session copend. AllenVaul HIDS: Login session copend. AllenVaul HIDS: Softer session copend. SSHd. Session disconnected sudo: Session copened sudo: Session copened sudo: Session copened sudo: Session copened sudo: Session copened sudo: Session copened sudo: Session connected sudo: Session connect
Filtro: Resaltar:	< >>
<pre></pre>	
	© COPYRIGHT 2020 ALIENVAULT, INC. LEGAL

Figura 88: Gestión de riesgos: Línea de tiempo. Fuente: OSSIM AlienVault

4.7 Definición, desarrollo e implementación de scripts en el Módulo de Disponibilidad

Uno de los objetivos principales de este proyecto es la implementación de scripts personalizados para el monitoreo, pero como un paso previo se definió tipos scripts según la obtención de datos, ya que con esta definición se podrá homologar procedimientos para la obtención de los datos ya que este aspecto se le puede considerar el más complejo y genera malestar en el desarrollo.

4.7.1 Tipos de script según su funcionamiento

Un script de programación es un conjunto de intrusiones u órdenes con un objetivo específico que generalmente es ejecutado por otras entidades ya sea de software o hardware.

Un script es un texto plano que está definido por el lenguaje de programación, por ende, tiene extensión un ambiente donde se pueda ejecutar una entrada y una salida, ya que esta estructura es necesaria para que el sistema Nagios funcione correctamente.



Figura 89: Funcionamiento de un script Elaborado por: Jorge Añazco

Como muestra la imagen anterior un script necesita una entrada de datos, para realizar el análisis o procesamiento de datos y mostrar una salida y por ultimo necesita ejecutarse en un ambiente también conocido como framework que define el tipo de estructura y lenguaje de programación la cual debe estar construido el script.

4.7.2 Scripts de monitoreo por servicio

Este tipo de script tiene como principal funcionalidad hacer peticiones nativas de los diferentes servicios que existen, por ejemplo, el ping del protocolo ICMP para verificar si un servicio o equipo está activo en una red, peticiones DNS para detectar si el servicio de DNS se encuentra activo o hacer una petición Telnet para ver si un puerto se encuentra activo.



Figura 90: Scripts de monitoreo por servicio Elaborado por: Jorge Añazco

Básicamente para la obtención de datos para este tipo de script es la ejecución de comandos para ver los estados de los protocolos, por ejemplo, se ejecuta el comando nslookup definiendo un dominio como también la dirección del servidor DNS según la respuesta o salida del comando se puede validar si el servidor se encuentra activo.

4.7.3 Scripts de monitoreo en servidor (obtención de estados)

Este tipo de script ejecuta comandos nativos del sistema operativo o de un servicio de manera local, para obtener información según las necesidades del monitoreo, de acuerdo a los siguientes parámetros:

- Tamaños de logs, carpetas o archivos.
- Modificación y estados de servicios y de archivos.
- Obtener información de consumo y estado de los procesos que se ejecuta en el sistema operativo.

- Verificación de números sesiones activas en el servidor.
- Verificación de usuarios autenticados.

Nagios tiene dos clientes para entornos Linux y Windows, lo que realizan estos clientes es ejecutar los scripts de manera local y la salida o el resultado del script es enviado al Nagios para su interpretación, el cliente para entornos Windows se llama NSClient++ y para entornos Linux el cliente se llama NRPE, básicamente con este cliente es un servicio que ejecuta scripts remotos de manera local.



Figura 91: Scripts de monitoreo en servidor (obtención de estados) Elaborado por: Jorge Añazco

4.7.4 Scripts de monitoreo por análisis de datos

Este tipo de script como principal objetivo es la obtención de información de un banco de datos, ya sea de Bases de datos (SQL, Mysql, Postgresql, MongoDB etc.), archivos tipo banco de datos (CSV, XLSX, XLS, XML) o información de los registros de los sistemas o servicios, luego de tener la información lo procesa y manda un resultado.

Hay que tomar en cuenta que este tipo de script son los que generalmente consume más recursos del sistema, ya que, según el volumen de los datos obtenidos de procesamiento puede consumir recursos afectando al funcionamiento de la estabilidad del sistema.



Figura 92: Scripts de monitoreo por análisis de datos Elaborado por: Jorge Añazco

4.7.5 Scripts de monitoreo por interacción

Este tipo de scripts como una de sus principales funcionalidades es interactuar y enviar sentencias o comandos en los diferentes CLI (Command Line Interface) que existe por marca o dispositivo, para esta funcionalidad se utilizó el paquete/módulo Expect, el cual se encuentra en los ambientes Linux (Debian, Red Hat) y se puede implementar en lenguaje SHELL, este paquete ayuda a realizar desde la conexión y mandar las sentencias o comandos para obtener la información necesaria para el monitoreo.

Scripts de monitoreo por interacción



Figura 93: Scripts de monitoreo por interacción Elaborado por: Jorge Añazco

La herramienta que se utiliza para realizar las sesiones es el paquete Expect que es necesario instalar en el servidor OSSIM AlienVault con el siguiente comando:

• apt-get install expect

Por último un ejemplo de cómo se realiza una sesión con esta herramienta, básicamente en este comando hay que definir un proceso de inicio de sesión con el usuario y contraseña como la IP del dispositivo y el proceso de integración para la obtención de los datos, a continuación, se detalla los comando que tiene la herramienta.

- spawn: Iniciar un script o un programa.
- expect: Esperar la salida de un programa.
- <u>end</u>: Enviar una respuesta a tu programa.
- Interact: Permitirte interactuar con tu programa.

En el siguiente grafico de detalla un ejemplo de inicio de sesión y obtención de datos de un sistema de enfriamiento en un *Data Center* para la obtención de la temperatura promedio:

1	HOST="172.16.254.160"													
2	USER="DCPrueba"													
3	PASS="Adminprueba"													
4	PASS_ROOT="temporalPass"													
5	LOOP=2													
6	VAR=\$ (expect -c "													
7	match_max 100000													
8	<pre>spawn ssh -o StrictHostKeyChecking=no \$USER@\$HOS</pre>	Т												
9	<pre>expect \"Authenticated with partial success.\"</pre>													
10	<pre>expect \"*?assword:*\"</pre>													
11	send \"\$PASS\r\"													
12	expect \">\"													
13	send \"1\r\"													
14	<pre>expect \"* Device Manager *\"</pre>													
15	expect \">\"													
16	send $\"1\r$													
17	<pre>expect \"* Environment *\"</pre>													
18	expect \">\"													
19	send \"\033\r\"													
20	<pre>expect \"* Device Manager *\"</pre>													
21	expect \">\"													
22	send \"\033\r\"													
23	<pre>expect \"* Control Console *\"</pre>													
24	expect \">\"													
25	send \"4\r\"													
26	match_max 100000													
27	expect eof													
28	")													
20														

Figura 94: Ejemplo del comando expect. Elaborado por: Jorge Añazco

4.7.6 Scripts de monitoreo por consumo de microservicios

Este tipo de scripts como uno de sus principales objetivos es consumir un API o microservicios y una de las ventajas es que la manera en que se consulta los datos y la respuesta de los mismos es de manera uniforme a través de una petición HTTP/GET y requiere menos recursos del servidor ya que son autónomos a tal grado que el procesamiento de los datos se puede delegar al API o microservicios y solo consultar el dato específico para el análisis del monitoreo.

Hay que tomar en cuenta que la respuesta es en formato JSON y hay que procesar este tipo de datos, para este proyecto se utilizó programación en lenguaje Python para enviar y procesar los datos.

Scripts de monitoreo por consumo de microservicios



Figura 95: Scripts de monitoreo por consumo de microservicios Elaborado por: Jorge Añazco

4.8 Creación de scripts para el módulo de Nagios

Para el desarrollo de scripts para el módulo de Nagios se debe tomar en cuenta el tipo de lenguaje en el que se van a desarrollar, en este caso se utiliza SHELL con otras herramientas y lenguajes que ofrece el sistema operativo del OSSIM AlienVaulr como, por ejemplo, el lenguaje Ruby para tratamiento de datos y el módulo Expect que sirve para automatizar sesiones interactivas.

4.8.1 Características de un script para funcionar con Nagios

Los scripts de Nagios cuentan con la siguiente estructura:

Creación del script: El script se puede crear con el comando touch con extensión .sh además de tener permisos de ejecución.

```
alienvault:/nagios/scripts/Script_Prueba# touch nagios_scripts_HolaMundo_v2.sh
alienvault:/nagios/scripts/Script_Prueba# chmod +x nagios_scripts_HolaMundo_v2.sh
```

Figura 96: Características de un script: Creación Elaborado por: Jorge Añazco

Ruta del script: Ubicación del script dentro del servidor, para este ejemplo:

```
1 /nagios/scripts/Script Prueba/nagios scripts HolaMundo vl.sh
```

Figura 97: Características de un script: Ubicación. Elaborado por: Jorge Añazco

Cuerpo del script: es el contenido del documento dónde se encuentra los algoritmos y se

define lo que hace el script:



Figura 98: Características de un script: Cuerpo/código. Elaborado por: Jorge Añazco

Dónde:

Los mensajes que serán mostrados en el Nagios serán las líneas que imprime el comando

echo

Host 🕈	Status 🔦	Last Check 🕈	Duration **	Status Information
Host-192-168-0-161	UP	2021-03-28 19:31:18	269d 18h 34m 39s	PING OK - Packet loss = 0%, RTA = 0.98 ms
localhost 🛛 🔿 🍳	UP	2021-03-28 19:33:38	270d 21h 56m 24s	PING OK - Packet loss = 0%, RTA = 0.13 ms

Elaborado por: Jorge Añazco

Y el código exit, define el estado de la notificación para generar alarmas según el código

Código	Estado	Color
exit 0	OK	
exit 1	WARNING	
exit 2	CRITICAL	
exit 3	UNKNOWN	
Ela	borado por: Jorge	e Añazco

Tabla 6: Características de un script: Estados Nagios.

Depuración/Debug

Como ayuda al momento de crear y visualizar paso a paso la ejecución del script (depurar) se puede brindar seguimiento con los siguientes comandos:

\$bash -x nombredelscript.sh

alienvault:/nagios/scripts/Script Prueba# bash -x nagios scripts HolaMundo vl.sh ARCHIVO_PRUEBA=nagios/scripts/Script_Prueba/nagios_scripts_HolaMundo_vl.sh echo 'OK - El archivo existe' - El archivo existe exit 0

Figura 100: Depuración/Debug: Comando bash. Elaborado por: Jorge Añazco

Esto permite dar seguimiento y control de línea por línea de lo que ejecuta el script y facilita

la detección de errores de programación.

Por último, existe una manera de mostrar el valor de la ejecución que son los valores de los

exit:

\$echo \$?



Figura 101: Depuración/Debug: Comando echo \$?. Elaborado por: Jorge Añazco

Este comando captura el valor del último script ejecutado.

4.8.2 Agregar un nuevo comando-script a Nagios para monitoreo

Una vez creado el script, el siguiente paso es la configuración del Nagios para acceder al mismo:

Agregar un nuevo archivo de configuración donde se define y configura el nuevo comando, en este caso se crea una nueva carpeta en la ruta /etc/nagios3 llamada comandosnuevos la cual contendrá el archivo comandos_nuevos.cfg.

\$cd /etc/nagios3 && mkdir comandosnuevos && touch comandos_nuevos.cfg



Figura 102: Agregar un nuevo comando Nagios: Creación nuevo archivo de configuración. Elaborado por: Jorge Añazco

Se ingresa al archivo comandos_nuevos.cfg e ingresar la configuración del nuevo comando

para el Nagios:



Figura 103: Agregar un nuevo comando Nagios: Estructura de creación de un nuevo comando. Elaborado por: Jorge Añazco

Donde:

Tabla 7: Agregar un nuevo comando Nagios: Descripción de comandos.

Comando	Descripción							
command_name	Nombre del comando							
command_line	Ruta del script							
Elaborado por: Jorge Añazco								

Luego se ingresa en la configuración de Nagios (/etc/nagios3/nagios.cfg), e indicar la ruta

del nuevo archivo de configuración:

#Definitions for monitoring with custom scripts
cfg dir=/etc/nagios3/comandosnuevos

Figura 104: Agregar un nuevo comando Nagios: Agregar nuevo archivo/directorio de configuración. Elaborado por: Jorge Añazco

En este caso se utilizó cfg_dir, para indicar que ingrese en la configuración del Nagios todos los archivos del directorio /etc/nagios3/comandosnuevos, pero también se puede indicar un solo archivo para la configuración con el siguiente comando: cfg_file=/etc/nagios3/comandosnuevos/comandos_nuevos.cfg.

Luego de configurar el nuevo comando en el Nagios, hay que ingresarlo a la plantilla del host para el monitoreo, en este caso se utiliza el localhost como ejemplo. Se ingresa al archivo /etc/nagios3/conf.d /localhost_nagios2.cfg y se crea un nuevo servicio de monitoreo:



Figura 105: Agregar un nuevo comando Nagios: Agregar comandos al host. Elaborado por: Jorge Añazco

Donde:

Tabla 8: Agregar un nuevo comando Nagios: Comandos para agregar servicios al host.

Comando	Descripción							
use	Se indica la plantilla que se va utilizar por defecto							
host_name El nombre de host a cuál se le va ingresar el serv								
service_description Descripción del servicio								
check_command Nombre del comando que se va utilizar								
	Elaborado por: Jorge Añazco							

Para finalizar, compilamos los archivos de configuración de Nagios y visualizar si existe o

no algún error con el siguiente comando:

\$nagios3 -v /etc/nagios3/nagios.cfg

Y con esto se valida si existe algún error

Total	Warnings:	0
Total	Errors:	0

Figura 106: Agregar un nuevo comando Nagios: Errores de compilación Nagios. Elaborado por: Jorge Añazco

Por último, reiniciamos el servicio de Nagios:

al	ie	nv	aı	ult	::,	/e	t	c/	'n	a	gi	os	3/0	:0	nf	.d	# s	se:	rvi	.ce	nā	۱g:	io	s 3	r	es	ta	rt	5		
[•]		.]	I	Res	t	ar	t	ir	ıg	1	na	gi	os	3 1	mo	ni	toi	ci.	ng	da	emc	n	:	naç	gi	.os	3				
20	21	-0	3-	-29) (00	:	28	3:	1'	7	[6] ı	ıp	da	ti	ng	10	og	fi	le	11	nd	ex							
20	21	-0	3-	-29) (00	:	28	3:	1	7	[6] เ	ıp	da	ti	ng	1	og	fi	le	i.	nd	ex							
	0 k																														

Figura 107: Agregar un nuevo comando Nagios: Reinicio del servicio de Nagios. Elaborado por: Jorge Añazco

De esta manera se refleja el nuevo servicio en el panel de disponibilidad del AlienVault:

Host ★★ Service ★★	Status 🛧	Last Check 🕈 🕈	Duration **	Attempt 🛧	Status Information
localhost (Current Load	ок	2021-03-29 00:28:36	0d 1h 1m 10s	1/4	OK - load average: 1.42, 1.16, 1.19
Current Users	ОК	2021-03-29 00:29:36	271d 2h 50m 17s	1/4	USERS OK - 1 users currently logged in
Disk Space	OK	2021-03-29 00:26:06	271d 2h 49m 27s	1/4	DISK OK
HTTP	ОК	2021-03-29 00:27:06	271d 2h 48m 37s	1/4	HTTP OK: HTTP/1.1 302 Found - 454 bytes in 0.009 second response time
Prueba-Script	OK	2021-03-29 00:29:17	0d 1h 1m 40s	1/4	OK - El archivo existe
SSH	ОК	2021-03-29 00:29:06	271d 2h 47m 47s	1/4	SSH OK - OpenSSH_7.4p1 Debian-10+deb9u7 (protocol 2.0)
Total Processes	ОК	2021-03-29 00:25:06	271d 2h 46m 57s	1/4	PROCS OK: 127 processes

Figura 108: Agregar un nuevo comando Nagios: Nuevo servicio. Elaborado por: Jorge Añazco

4.9 Notificaciones y alertas a través de Telegram

Para las notificaciones y alertas a través de Telegram se necesita una herramienta llamada telegram-cli que es un software para sistemas Linux ya sea basados en Red Hat (Centos, Fedora, etc.) o Debian (Ubuntu, Kubuntu, Raspbian, etc.) que permite utilizar un terminal para el envío de mensajes a través de la plataforma Telegram.

La ventaja principal de usar telegram-cli en el terminal es que se puede unir con otras aplicaciones con scripts y automatizar envió de notificaciones directamente a los usuario y grupos como a cualquier tipo de dispositivos ya sean de escritorio o móviles.

4.9.1 Instalación telegram-cli en CentOS 8

Para la instalación se necesita el paquete telegram-cli que se puede conseguir en este enlace:

https://github.com/vysheng/tg o se puede ejecutar el siguiente comando en el terminal git clone

--recursive https://github.com/vysheng/tg.git

<pre>[root@localhost telegram_git]# git clonerecursive https://github.com/vysheng/tg.git</pre>
Clonando en 'tg'
remote: Enumerating objects: 4511, done.
remote: Total 4511 (delta 0), reused 0 (delta 0), pack-reused 4511
Recibiendo objetos: 100% (4511/4511), 2.99 MiB 1.91 MiB/s, listo.
Resolviendo deltas: 100% (3041/3041), listo.
Submódulo 'tgl' (https://github.com/vysheng/tgl.git) registrado para ruta 'tgl'
Clonando en '/home/janazco/telegram git/tg/tgl'
remote: Enumerating objects: 1555, done.
remote: Total 1555 (delta 0), reused 0 (delta 0), pack-reused 1555
Recibiendo objetos: 100% (1555/1555), 1.03 MiB 2.00 MiB/s, listo.
Resolviendo deltas: 100% (1137/1137), listo.
Ruta de submódulo 'tgl': check out realizado a 'ffb04caca7lde0cddf28cd33a4575922900a59ed'
Submódulo 'tl-parser' (https://github.com/vysheng/tl-parser) registrado para ruta 'tgl/tl-parser'
Clonando en '/home/janazco/telegram git/tg/tgl/tl-parser'
remote: Enumerating objects: 87, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 87 (delta 1), reused 1 (delta 1), pack-reused 83
Ruta de submódulo 'tgl/tl-parser': check out realizado a '36bf1902ff3476c75d0b1f42b34a9le944123b3c'

Figura 109: Descargar telegram-cli. Elaborado por: Jorge Añazco

Antes de continuar con la instalación se debe instalar los siguientes paquetes

- dnf install python3
- dnf install gcc gcc-c++
- dnf install libevent-devel
- dnf install openssl-devel
- dnf install readline-devel
- dnf install jansson-devel
- dnf install libgcrypt-devel
- dnf install jansson-devel

- dnf install lua-devel
- dnf install readline-devel
- dnf install libconfig-devel
- dnf install libevent-devel

Si la instalación es en Centos 8 el paquete lua-devel no se encuentra en el repositorio por defecto y se realizó la instalación manual descargando el paquete del siguiente enlace: https://centos.pkgs.org/8/centos-powertools-x86_64/lua-devel-5.3.4-11.el8.x86_64.rpm.htm

Y para instalar con el comando:

\$ rpm-ivh lua-devel-5.3.4-11.el8.x86_64.rpm

Por último y para servidores con el sistema operativo Centos 8 en el proyecto de telegramcli hay que modificar el archivo /tg/tgl/mtproto-utils.c t comentar las líneas 101 y 115 para que al momento de instalar no se presente un problema de configuración por el sistema operativo.

assert (0); // As long as nobody ever uses this code, assume it is broken.

Figura 110: Prerrequisito para la instalación de telegram-cli en Centos 8 Elaborado por: Jorge Añazco

Y para instalar se ejecuta los siguientes comandos en la ubicacion /tg

\$./configure --disable-openssl CFLAGS="-w"
\$ make

Luego de la instalación y para ejecutar directamente el telegram-cli como comando del sistema se realiza una copia del ejecutable en una carpeta para luego crear la referencia dentro /usr/bin.

\$ mkdir /opt/telegram-cli

&& cp bin/telegram-cli tg-server.pub /opt/telegram-cli/

&& ln -s /opt/telegram-cli/telegram-cli /usr/bin/

Para configurar el número celular que va a utilizar telegram-cli se introduce el comando:

\$ telegram-cli -k tg.pub

Luego se ingresa número celular para enviar un código de autenticación y este código lo recibirá en la aplicación de Telegram del dispositivo, se ingresa y presiona enter y ya está configurado telegram-cli.

```
$ telegram-cli -k tg.pub
Telegram-cli version 1.4.1, Copyright (C) 2013-2015 Vitaly Valtman
Telegram-cli comes with ABSOLUTELY NO WARRANTY; for details type `show_license'
This is free software, and you are welcome to redistribute it
under certain conditions; type `show_license' for details.
Telegram-cli uses libtgl version 2.1.0
Telegram-cli includes software developed by the OpenSSL Project
for use in the OpenSSL Toolkit. (http://www.openssl.org/)
I: config dir=[/home/pi/.telegram-cli]
phone number: +59396666666
code ('CALL' for phone code): 58964
```

Figura 111: Instalación telegram-cli Elaborado por: Jorge Añazco

Para ingresar a la consola del telegram-cli es con el comando telegram-cli -W -k server.pub



4.9.2 Script de comunicación para envió de alerta y notificaciones por telegram-cli

Para este proyecto se realizó un script para la comunicación entre la herramienta OSSIM AlienVault y telegram-cli que se encuentra en servidores diferentes para este se utilizó la herramienta Expect para su funcionamiento.

Primero se define el comando para enviar mensajes sin interactuar con el cliente del telegram-cli que es el siguiente:

(sleep 3;echo "msg \$destination \"\$message\""; echo "safe_quit") | telegram-cli -k tg-server.pub -W

Figura 112: Comando local para el envío un mensaje en telegram-cli Elaborado por: Jorge Añazco

Donde:

\$destination: Es el contacto a enviar el mensaje.

\$message: Es el contenido del mensaje

Ya definido el comando se puede automatizar un script de conexión y ejecución con la ayuda

de la herramienta Expect.



Figura 113: Comando remoto para el envío un mensaje en telegram-cli Elaborado por: Jorge Añazco

4.9.3 Script Telegram

- **Objetivo:** Script para enviar noticiones o alertas por el aplicativo Telegram.
- Entrada:

Entrada 1: Ejecución local para él envió de mensaje por Telegram

SendMessageTelegram.sh -c \$destination -m \$message

Entrada 2: Ejecución remota para él envió de mensaje por Telegram

SendMessageTelegram.sh -r -c \$destination -m \$message

- Salida del script: El envío de mensaje.
- Código: Ver Anexo 1.
- Flujo:



Figura 114: Flujo script SendMessageTelegram.sh Elaborado por: Jorge Añazco

4.9.4 Configuración Nagios para el envío de notificaciones o alertas por Telegram

Primero en el archivo commands.cfg se define la llamada del script SendMessageTelegram y se parametriza los argumentos de la entrada del script con las variables locales del Nagios, esta configuración es para las notificaciones de los servicios como de los dispositivos.

# 'not	ify-host-by-telegram' command definition
⊒define	command {
	command name notify-host-by-telegram
	command line /home/telegram/ScriptComunicacionTelegram.sh -r -c \$ CONTACTTELEGRAM\$ -m
	"***** Nagios ***** Notification Type: \$NOTIFICATIONTYPE\$ Host: \$HOSTNAME\$ State: \$HOSTSTATE\$
	Address: SHOSTADDRESSS Info: SHOSTOUTPUTS Date/Time: SLONGDATETIMES"
L	A ALTERS , ANDERDARDED A THEO, ANDEROTOTA DAVE, ALTER , ADARDATITATING
# 'not	ild-selaice-ph-telediam, command delivition
define	command {
	command_name notify-service-by-telegram
	command line /home/telegram/ScriptComunicacionTelegram.sh -r -c \$ CONTACTTELEGRAM\$ -m
	"***** Nagios ***** Notification Type: \$NOTIFICATIONTYPE\$ Service: \$SERVICEDESC\$ Host: \$HOSTALIAS\$
	Address: \$HOSTADDRESS\$ State: \$SERVICESTATE\$ Date/Time: \$LONGDATETIME\$ Additional Info: \$SERVICEOUTPUT\$"
	,

Figura 115: Configuración del comando para el envío de mensajes por Telegram Elaborado por: Jorge Añazco

Se crea una nueva plantilla de notificación por contactos donde definimos la llamada de los

nuevos comandos para notificar por Telegram

name	operaciones-contac	t-telegram ; The name of this contact template		
service_notification_period	24x7	; service notifications can be sent anytime		
host_notification_period	24x7	; host notifications can be sent anytime		
service_notification_options	w,u,c,r,f,s	; send notifications for all service states, flapping events, and scheduled downtime events		
host_notification_options	d,u,r,f,s	; send notifications for all host states, flapping events, and scheduled downtime events		
service notification commands	notify-service-by-telegram ; send service notifications via email			
host notification commands	notify-host-by-tel	egram ; send host notifications via email		
register	0	; DONT REGISTER THIS DEFINITION - ITS NOT A REAL CONTACT, JUST A TEMPLATE!		
}				



Se configura el usuario y se inicializa una nueva variable _telegram para definir el nombre de usuario del contacto de Telegram.



Figura 117: Configuración del contacto para el envío de mensajes por Telegram Elaborado por: Jorge Añazco

Por último, se realiza el envío de la notificación de prueba



Figura 118: Ejemplo de envío de notificación por Telegram. Elaborado por: Jorge Añazco

4.10 Scripts desarrollados

Actualmente se ha desarrollado 5 scripts para el monitoreo de Nagios, los cuales se detallan a continuación:

4.10.1 Script para la obtención de la temperatura del sistema de enfriamiento de un

Data Center

- **Objetivo:** Obtener los valores de temperatura a través de consultas directas en el sistema de enfriamiento, según la temperatura se analiza y se alerta.
- Tipo de script: Scripts de monitoreo por interacción.
- Alerta: Se emite cuando la temperatura es superior a 28° y la humedad es menor al 25%, para evitar posibles daños a los equipos que se encuentran en el data center, si por alguna razón existe un problema con el sistema de refrigeración.
- **Salida del script:** Temperatura = "\$TEMP" Humedad = "\$HUMEDAD"
- Código: Ver Anexo 2.
- Flujo:



Figura 119: Flujo script para la obtención de la temperatura del sistema de enfriamiento de un Data Center Elaborado por: Jorge Añazco

4.10.2 Script para la obtención de un archivo .csv donde se detalla número de *snapshots* de un hipervisor, para el análisis y él envió de los estados.

- **Objetivo:** Obtener un archivo .csv a través del servicio ftp donde se detalla número de *snapshots* que se tiene en las máquinas virtuales de un hipervisor, para luego analizarlo y alertar según los estados.
- **Tipo de script:** Scripts de monitoreo por análisis de datos (archivo .csv).
- Alerta: Cuando existe algún *snapshots* en el servidor, ya que para mantenerlo activo consume recursos y puede generar problemas con la máquina virtual.

• Salida del script: EXISTEN SNAPSHOTS EN "\$NOMBRE_SERVIDOR" --

Numero de Snapshots = "\$NUMERO_SNAPSHOTS"

- Código: Ver Anexo 3.
- Flujo:



Figura 120: Flujo script para la obtención de un archivo .csv donde se detalla número de snapshots que tiene en las máquinas virtuales de un hipervisor, para luego analizarlo y mandar los estados. Elaborado por: Jorge Añazco

4.10.3 Script que analiza el log de acceso del servicio de apache

- **Objetivo:** Analizar el log de acceso del servicio de apache.
- **Tipo de script:** Scripts de monitoreo por análisis de datos (archivo .log).
- Alerta: Se calcula la media del número de peticiones http que ingresan por día

y por hora, con este valor se puede determinar si hay un ataque en proceso a la

página web del log monitoreado.
• Salida del script:

Salida 1

Número de Peticiones son: "\$PETICIONES" MAX-NORMAL = "\$MAX" MAX-CRITICAL = "\$MAX_CRI"

Salida 2

Tamaño del LOG es: "\$SIZE_MATH\$TYPE" MAX-NORMAL = "\$i"M MAX-CRITICAL = "\$j"M Revisar los LOGS anteriores existe un log que pesa más de 1 GB

- Código: Ver Anexo 4.
- Flujo:



Figura 121: Flujo script que analiza e llog de acceso del servicio de apache Elaborado por: Jorge Añazco

4.10.4 Script que analiza los tamaños de los directorios y logs de la base de datos

Postgresql

- **Objetivo:** Obtener el tamaño de los log, espacio en disco y el tamaño del directorio de la base de datos Postgresql.
- **Tipo de script:** Scripts de monitoreo en servidor (obtención de estados).
- Alerta: Según el tamaño de los logs se calcula la media de tamaños de los directorios para alertar, esto ayuda a evitar caídas del servicio por falta de almacenamiento y además se podría detectar ataques a la base de datos.
- Salida del script:

Salida 1

Tamaño del LOG es: "\$SIZE_MATH\$TYPE" MAX-NORMAL = "\$i"M MAX-CRITICAL = "\$j"M

Salida 2:

"Tamaño del DIR LOG es: " \$SIZE_MATH\$TYPE"

Salida 3:

El porcentaje es: "\$SIZE_MATH\$TYPE" TAMAÑO = "\$TAMANO" OCUPADO = "\$UTILIZADO" DISPONIBLE = "\$DISPONIBLE"

- Código: Ver Anexo 4.
- Flujo:



Figura 122: Script que analiza los tamaños de los directorios y logs de la base de datos Postgresql Elaborado por: Jorge Añazco

4.10.5 Script que analiza el número de tickets de la mesa de servicio

- **Objetivo:** Obtener el número de tickets nuevos, asignados abiertos, asignados cerrados y tickets en seguimiento de la mesa de servicios.
- **Tipo de script:** Scripts de monitoreo por análisis de datos (consultas a la base de datos).
- Alerta: Se establece una franja de recepción de tickets abiertos con un mínimo de 20 y máximo de 25 sobre un tema particular de los establecidos en la base de datos del catálogo de servicios de la mesa de ayuda relacionados con el tema de seguridad, para alertar de un posible problema o mal funcionamiento de los sistemas de la universidad.

- Salida del script: Número de tickets nuevos son: "\$TICKETNUEVO" El número de tickets abiertos son "\$TICKETABIERTO" El número de tickets cerrados son "\$TICKETCERRADO" El número de tickets en seguimiento son "\$TICKETSEGUIMIENTO"
- Código: Ver Anexo 6.
- Flujo:



Figura 123: Script que analiza el número de tickets de la mesa de servicio Elaborado por: Jorge Añazco

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- De acuerdo al análisis, se puede concluir que, el estado actual de la infraestructura tecnológica de la Universidad Internacional SEK no se encuentra de manera óptima ni recomendable; refleja que la institución no cuenta con una estructura, cultura, estándar, esquema, metodología o un sistema para implementar procesos de seguridad de la información, que contribuya con el monitoreo y control de los diferentes sistemas que maneja la Universidad. En el caso de la adquisición o desarrollos de nuevos sistemas, se requiere estandarizar inventarios y actualizarlos, creación de más ambientes para el desarrollo de software, metodologías, definir procesos de seguimiento y control ya sea de software y hardware, control de calidad sobre el código, por último, se puede mejorar el reglamento interno sobre seguridad de la información, e invertir en personal con experiencia en infraestructura informática para mejorar la seguridad de la información de la Universidad.
- La herramienta OSSIM AlienVault tiene una interfaz amigable y fácil de configurar al permitir acceso vía web a su consola, tiene como valor agregado a su fortaleza técnica que contiene también varios reportes orientados a la administración y toma de decisiones. Es importante reconocer que la curva de

aprendizaje es rápida y didáctica ya que cuenta con muchos tutoriales y ayudas en Internet.

- La implementación de la <u>herramienta</u> y sus costos depende del tamaño de la organización y el alcance que debe tener la herramienta, ya que, entre más complejo, se pueden elevar los costos y necesitar más personal como equipos, y gracias a sus módulos autónomos de Gestión de Archivos, Gestión de Disponibilidad, Gestión de Notificaciones, Gestión de Vulnerabilidades y Gestión de Riesgos, se puede monitorear en diferentes niveles la disponibilidad de los activos como de los servicios, además, de alertar al momento de encontrar alguna anomalía, así como también, se puede generar varios tipos de reportes según las necesidades de la Universidad.
- Se ha logrado establecer cinco tipos de scripts y definir métodos como procesos para la obtención de información, uno de los malestares que es parte del monitoreo es como obtener la información para procesarla y dar un resultado válido para la herramienta OSSIM AlienVault, con estas definiciones se pueden iniciar de manera clara los scripts, implementar una estructura más limpia y se optimiza el tiempo de desarrollo.
- El desarrollo de scripts para las necesidades de monitoreo requiere de una planificación previa para cumplir con el objetivo. Para este proyecto se realizaron cinco desarrollos donde se analizó los mejores métodos de obtención de datos y algoritmos de procesamiento de datos y se estableció periodos de ejecución para no afectar el rendimiento del servidor, se utilizó diferentes herramientas como tecnologías para cumplir el objetivo del desarrollo y se estandarizó procesos para que se pueda reutilizar códigos que ayuden a bajar

tiempo de desarrollos y optimizar funcionalidades. Una de las ventajas encontradas del desarrollo personalizado es que, se puede expandir y controlar el núcleo de la seguridad informática ya que con esto se puede implementar nuevos recursos que ayuden a minimizar los posibles riesgos.

5.2 Recomendaciones

- Dado los resultados del análisis de los 20 controles de la CIS v7 es recomendable ir ajustando, modificando y crear políticas de seguridad e ir estableciendo fases para el cumplimento de los controles de CIS, en las primeras fases como principal objetivo sería definir procesos de inventario de los diferentes activos de la organización, ya que, con esto se podrá dimensionar y definir alcances para el progresivo cumplimiento de los controles además se tendría una perspectiva de la situación real de la organización.
- Con la instalación de la herramienta OSSIM AlienVault se debe considerar la creación de lineamientos para la implementación de metodologías, estándares de calidad y procesos para comenzar a utilizar todos los módulos que ofrece la herramienta, además con esta herramienta se puede centralizar algunos requisitos que piden los controles de la CIS y así estandarizar el flujo de la seguridad de la información de la entidad.
- Se recomienda para futuros desarrollos utilizar herramientas adicionales para cumplir con las necesidades o los objetivos del monitoreo, ya que el lenguaje Shell ofrece la opción de incluir otros lenguajes de programación dentro del código, cómo por ejemplo, estos pueden ser PHP, Ruby, Perl y Python, por último, se puede adaptar nuevas tecnologías para complementar la obtención de datos y su análisis.

BIBLIOGRAFÍA

- AT&T. (13 de septiembre de 2021). *AlienVault OSSIM*. Obtenido de AT&T Cybersecurity: https://cybersecurity.att.com/products/ossim
- AuditScripts. (2018). *Critical Security Controls*. Obtenido de The CIS Critical Security Controls: https://www.auditscripts.com/free-resources/critical-security-controls/
- Balarezo, A., & Poveda, D. (2015). PROPUESTA DE MEJORAMIENTO DE LA HERRAMIENTA OSSIM SIEM. (*Trabajo de titulación*). UNIVERSIDAD POLITÉCNICA SALESIANA, Quito.
- Bravo, Á., Villafuerte, Á., & Patiño, J. (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. *Artículos de Tesis de Grado FIEC*.
- CIS Controls. (2018). CIS Controls Spanish Translation V7. CIS Controls. Obtenido de https://learn.cisecurity.org/CIS-Controls-v7.1
- EcuRed. (15 de junio de 2016). *https://www.ecured.cu/*. Obtenido de http://www.nagios.org/ Nagios: https://www.ecured.cu/Nagios
- El Comercio. (12 de enero de 2021). *Ecuador, una de las naciones más atacadas por los 'hackers'*. Obtenido de El Comercio: https://www.elcomercio.com/tendencias/ecuadornaciones-atacadas-hackers-tecnologia.html
- El Comercio. (23 de julio de 2021). Virus RansomEXX es el responsable del ciberataque aCNT.ObtenidodeElComercio:

https://www.elcomercio.com/actualidad/negocios/virus-ransomeware-cnt-ministeriotelecomunicaciones.html

- Espinoza, D. (2015). ESTUDIO DE LA HERRAMIENTA DE SEGURIDAD OPEN. (*TESIS DE GRADO*). UNIVERSIDAD DE GUAYAQUIL, GUAYAQUIL.
- Gagne, G., Bear, P., & Silberschatz, A. (2006). *Fundamento de Sistemas Operativos*. Madrid: McGraw-Hill.
- Gómez, Á. (2011). Enciclopedia de la Seguridad Informática 2ª EDICIÓN ACTUALIZADA. Alfaomega Ra-Ma.
- González, R. (2011). *Python para todos*. Recuperado de: https://launchpadlibrarian.net/18980633/Python%20para%20todos.pdf.
- helpsystem. (2019 de Diciembre de 2020). https://www.hostdime.com.pe/. Obtenido de https://www.helpsystems.com/es/blog/que-es-un-siem
- Kaspersky. (2021). *Kaspersky cybermap*. Obtenido de CIBERAMENAZA MAPA EN TIEMPO REAL: https://cybermap.kaspersky.com/es

Labrador, R. M. (2003). PROGRAMACIÓN AVANZADA EN SHELL.

Marchionni, A. (2011). Administrador de Servidores. Buenos Aires: USERS.

- Membrey, P., Verhoeven, T., & Angenendt, R. (2009). *The Definitive Guide to CentOS*. New York: Apress.
- Ministerio de Telecomunicaciones y de la Sociedad de la Información. (15 de abril de 2019). *Ministerio de Telecomunicaciones y de la Sociedad de la Información*. Obtenido de Más de 40 millones de ataques al Ecuador neutralizados desde el retiro del asilo a Julian

Assange: https://www.telecomunicaciones.gob.ec/mas-de-40-millones-de-ataques-alecuador-neutralizados-desde-el-retiro-del-asilo-a-julian-assange/

- Noguera, B. (19 de marzo de 2011). ¿Qué son los Scripts? Obtenido de Culturación: https://culturacion.com/que-son-los-scripts/
- Scott, G., & LaQuey, T. (Febrero de 1993). *IETF Tools (RFC1392)*. Obtenido de https://tools.ietf.org/html/rfc1392
- Universida Internacional SEK. (2021). *Direccionamiento Estratégico*. Obtenido de Uisek Ecuador: https://www.uisek.edu.ec/es/uisek/direccionamiento-estrategico
- Universidad Internacional Sek. (2021). *Historia*. Obtenido de Universidad Internacional Sek : https://www.uisek.edu.ec/es/uisek/nosotros/historia

Universidad Internacional Sek. (2021). Uisek Ecuador. Obtenido de https://www.uisek.edu.ec

ANEXOS

```
1
2
    #!/bin/bash
3
    #12/05/2021
4
    #AUTOR: JORGE AÑAZCO
5
    #VERSION: 0.7
6
    #In the there will be only chaos :^ }
7
8
    FUNCTIONS SEND TELEGRAM LOCAL() {
           (sleep 3;echo "msg $destination \"$message\""; echo "safe quit") |
9
           telegram-cli -k tg-server.pub -W
10
    }
11
12
13
    FUNCTIONS SEND TELEGRAM REMOTO() {
14
15
           echo "Destino: $destination | −r | Mensaje: $message" >>
           /home/telegram/logtelegram.txt
16
17
           HOST="192.168.0.148"
18
           USER="root"
19
           PASS="Adminlocal2k11"
20
           VAR=$(expect -c "
21
                  spawn ssh -o StrictHostKeyChecking=no $USER@$HOST
                  match max 100000
22
                  expect \"*?assword:*\"
23
                  send -- \"$PASS\r\"
24
                  expect \"*$\"
25
26
                  send -- \"cd /home/janazco/script telegram\r\"
                  expect \"*$\"
27
28
                  send -- {./SendMessageTelegram.sh -c $destination -m \"$message\"}
                  send -- \''\r''
29
30
                  expect eof
31
           ")
    echo "========="
32
    echo "$VAR"
33
34
    }
35
36
37
38
    #Entrada del comando validicion y funcionamiento
39
    **********
    if [ "$1" == "" ]
40
41
           then
           echo " \"ALERTA\" ERROR EN EL COMANDO NO SE PUEDE PROCESAR"
42
43
           exit 3
44
    fi
    ******
45
    while [ "$1" != "" ]; do
46
47
       case $1 in
48
    #-----
    -----#
49
          -c | --contact )
50
                                                             shift
51
                                                             destination=$1
52
                                                             shift
                                                             if [ "$1" == "" ]
53
54
                                                                    then
55
                                                                           echo
    " \"ALERTA\" ERROR EN EL COMANDO NO SE PUEDE PROCESAR"
56
                                                                            exit 3
                                                             elif [ "$1" == "-m" ]
57
58
                                                                    then
59
                                                                            shift
60
    message=$1
61
    FUNCTIONS_SEND_TELEGRAM_LOCAL
62
                                                             else
63
                                                                            echo
    " \"ALERTA\" ERROR EN EL COMANDO NO SE PUEDE PROCESAR"
64
                                                                            exit 3
```

ц	I 1 ;;	
## -r remote)	shift if ["\$1" == "- c" then	
destination=\$1	else	
\"ALERTA\" ERROR EN EL COMANDO NO SE PUEDE PROCESAR"	echo " exit 3 fi	
shift	if ["\$1" == ""] then	
" \"ALERTA\" ERROR EN EL COMANDO NO SE PUEDE PROCESAR"	e: elif ["\$1" == "-1 then s!	
message =\$1 FUNCTIONS_SEND_TELEGRAM_REMOTO		
" \"ALERTA\" ERROR EN EL COMANDO NO SE PUEDE PROCESAR"	else e fi ;;	
"# -h help) {Remoto} -c {contanto} -m {mensaje} -h HELP"	<pre>echo "remote {Remoto}contact {contact -m {mensaje} help {HELP}" echo " [Ejemplo para env. mensaje de manera local] ./ScriptComunicac legram.sh -c TELEGRAM_CONTACT MENSAJE"</pre>	
	<pre>\$ echo " [Ejemplo para envia mensaje desde otro servidor] ./ScriptComunicacio legram.sh -r -c TELEGRAM_CONTACT -m MENSAJE" echo " Requisitos local {Telegram-cli} Requisitos remotos {Expect package}" exit 3 ;;</pre>	
#		

ENCONTRADO"

104		
105		
106	esac	
107	shift	
108	done	
109		
110		

echo "Para mas ayuda
--help|-h"
exit 3
;;

103

```
#!/bin/bash
 1
     #12/04/2021
 2
 3
     #AUTOR: JORGE AÑAZCO
 4
     #VERSION: 1
 5
     #In the there will be only chaos :^}
 6
 7
    FECHA=$ (date +%Y-%m-%d--%H:%M)
 8
9
    HOST="172.16.254.160"
10
    USER="DCPrueba"
11
    PASS="Adminprueba"
     PASS ROOT="temporalPass"
12
13
14
         VAR=$(expect -c "
15
             match max 100000
16
             spawn ssh -o StrictHostKeyChecking=no $USER@$HOST
             expect \"Authenticated with partial success.\"
17
18
             expect \"*?assword:*\"
19
             send -- \"$PASS\r\"
20
             expect \">\"
21
             send -- \[1\r\]
22
             expect \"* Device Manager *\"
23
             expect \">\"
24
             send -- \"1\r"
25
             expect \"* Environment *\"
             expect ">"
26
27
             send -- \"\033\r\"
28
             expect \"* Device Manager *\"
29
             expect \">\"
30
             send -- \"\033\r\"
             expect \"* Control Console *\"
31
32
             expect \">\"
33
             send -- \"4\r
34
             match max 100000
35
             expect eof
         ")
36
37
38
     TEMP=$(echo "$VAR" | grep "LP1: SensorH/T" | perl -pi -e "s[!][ ]g" |cut -d " " -f
     13,14 | cut -d "," -f 1)
39
     HUMEDAD=$ (echo "$VAR" | grep "LP1: SensorH/T" | perl -pi -e "s[!][]g" |cut -d " " -f
     13,14 | cut -d "," -f 2)
40
     echo "Temperatura = "$TEMP" Humedad = "$HUMEDAD
41
42
     TEMP=$( echo $TEMP | perl -pi -e "s[C][]g" )
    HUMEDAD=$( echo $HUMEDAD | perl -pi -e "s[%][]g" )
43
44
45
     if [ $TEMP -gt 28 ]
46
                              then
47
                              exit 2
48
                     elif [ $TEMP -le 25 -a $HUMEDAD -ge 25
                                                               1
49
                             then
50
                              exit 0
51
                     elif [ $TEMP -gt 25 -a $TEMP -le 28 ]
52
                              then
53
                              exit 1
54
                     elif [ $HUMEDAD -1t 25 ]
55
                              then
56
                              exit 2
57
                     fi
58
     exit 4
59
```

```
1
    #!/bin/bash
    #12/02/2021
2
3
    #AUTOR: JORGE AÑAZCO
4
    #VERSION: 1.1
5
    #In the there will be only chaos :^}
6
7
    #Declaración de Variables
8
    ARCHIVO SETUP="/home/nagios/Setup/config-server.info"
9
    ARCHIVO ESCRITURA="/home/nagios/Setup/serverwrite.info"
10
    ARCHIVO LOG="/home/nagios/logs/resumendiario.log"
11
    FECHA=$ (date +%Y-%m-%d)
12
    #Numero de host que se encuntran cofigurados
13
14
15
    typeset -i NUMERO HOSTS=$ (wc -1 $ARCHIVO SETUP | cut -d " " -f 1)
16
17
    #CABECERA DEL MAIL
    18
19
    echo "INICIO SCRIPT COPIA A TRAVES DE FTP" >> $ARCHIVO LOG
20
    echo "Fecha = "$FECHA >> $ARCHIVO LOG
21
    echo "-----" >> $ARCHIVO LOG
22
23
    ******
24
    #Comienzo del Script copiado de los archivos $ARCHIVO ESCRITURA permite el ingreso a
    las carpetas para obtener los archivos
25
26
    for ((a=4; a <= $NUMERO HOSTS; a++))</pre>
27
        do
28
        INFO HOST=$ (awk NR==$a $ARCHIVO ESCRITURA)
29
        #VALIDACION DE ARCHIVO
30
        cd /home/nagios/InfoVSphere/RVTools Diario "$INFO HOST"
31
32
        rm vSnapshot.csv
33
34
                   if [ $? = 0 ]
35
                          then
                          echo "ARCHIVO ANTIGUO ELIMINADO " >> $ARCHIVO LOG
36
37
                          else
38
                          echo "NO SE ENCONTRO EL ARCHIVO " >> $ARCHIVO LOG
39
                   fi
40
41
    #COPIA DEL ARCHIVO A TRAVEZ DE UN SERVICIO FTP
42
43
                   ftp -inv 172.16.0.33 <<< FTP
44
                          user admin Adminlocal2k11
45
                          cd RVTools Diario "$INFO HOST"
46
                          lcd /home/nagios/InfoVSphere/RVTools Diario "$INFO HOST"
47
                          get vSnapshot.csv
48
                          bye
49
    FTP
50
51
    #VALIDACION COPIA DEL ARCHIVO POR SERVICIO FTP
52
53
                   if [ -f
                   /home/nagios/InfoVSphere/RVTools Diario "$INFO HOST"/vSnapshot.csv ]
54
                          then
55
                          echo "SE REALIZO LA COPIA CORRECTAMENTE" >> $ARCHIVO LOG
56
                          else
57
                          echo "NO SE PUDO REALIZAR LA COPIA" >> $ARCHIVO LOG
58
                   fi
59
60
               61
62
    done
63
64
65
    exit
66
67
```

```
1
     #!/bin/bash
     #12/03/2021
 2
 3
     #AUTOR: JORGE AÑAZCO
 4
     #VERSION: 1
 5
     #In the there will be only chaos :^}
 6
 7
    FECHA=$ (date +%Y-%m-%d)
8
    MES=$(date +%m)
9
    YEAR=$ (date +%Y)
10
    SUM=0
11
    PROM=0
12
    MAX=0
13
14
     FUNCTIONS REPORT SIZE LOGS () {
15
     for (( a = 10; a > 0 ; a-- ))
16
17
         do
18
             FECHA SIZE=$ (date --date="-$a day" +"%Y-%m-%d")
19
             SIZE+=($( cat $ARCHIVO SIZEDIR | grep "$FECHA SIZE" | awk '{print $2}' ))
20
         done
21
22
     SIZE+=($( cat $ARCHIVO INFO | grep "$LOG INFO" | awk '{print $6}' ))
23
24
25
     for ((a=0; a< ${#SIZE[*]} - 1; a++))</pre>
26
         do
27
             typeset -i NUM CHARACTER=$ ( echo $ {SIZE[$a]} | wc -m )
28
             let d=(NUM CHARACTER - 2)
29
             SIZE MATH=$( echo ${SIZE[$a]} | cut -c 1-"$d" )
30
             let b=(NUM CHARACTER - 1)
             TYPE=$( echo ${SIZE[$a]} | cut -c "$b" )
31
32
33
             if [ $TYPE == 'K' ]
34
                 then
                     SIZE MATH=` echo "$SIZE MATH / 1000" | bc -1`
35
36
                 fi
37
                 if
                      [ $TYPE == 'G' ]
38
                          then
39
                              SIZE MATH=`echo "$SIZE MATH * 1000" | bc -1`
40
                              BAND=1
41
                          fi
42
                 SUM=`echo "$SUM + $SIZE MATH" | bc`
43
44
                 done
45
46
     PROM=`echo " $SUM / ( ${#SIZE[*]} - 1 )" | bc -1`
47
     MAX=`echo " $PROM * 2 " | bc -1`
48
     MAX CRI=`echo " $PROM * 3 " | bc -1`
49
50
     k=`echo "${#SIZE[*]} - 1 " | bc -1`
51
52
     NUM CHARACTER=$( echo ${SIZE[$k]} | wc -m )
53
     let d=(NUM CHARACTER - 2)
54
     SIZE MATH=$( echo ${SIZE[$k]} | cut -c 1-"$d" )
55
     let b=(NUM CHARACTER - 1)
56
     TYPE=$( echo ${SIZE[$k]} | cut -c "$b" )
57
58
     i=$( echo $MAX | cut -c 1-5 )
59
     j=$( echo $MAX CRI | cut -c 1-5 )
60
61
62
     if [ "$BAND" == "1" ]
63
             then
                     echo "Tamano del LOG es: "$SIZE MATH$TYPE" MAX-NORMAL = "$i"M
64
                     MAX-CRITICAL = "$j"M Revisar los LOGS anteriores existe un log que
                     pesa mas de 1 GB"
65
             else
             echo "Tamano del LOG es: "$SIZE MATH$TYPE" MAX-NORMAL = "$i"M MAX-CRITICAL =
66
             "$j"M"
```

```
67
      fi
 68
 69
 70
      if
          [ $TYPE == 'K']
 71
               then
 72
                       exit 0
 73
               else
 74
          [ $TYPE == 'G' ]
      if
 75
               then
 76
                   exit 2
 77
               else
 78
                       if [ $( echo "$SIZE MATH > $MAX SIZE INFO " | bc ) -eq 1 ]
 79
                                then
                   exit 2
 80
 81
                       elif [ $( echo "$SIZE MATH <= $MAX " | bc ) -eq 1 ]</pre>
 82
                                then
 83
                   exit 0
 84
                       elif [ $( echo "$SIZE MATH > $MAX && $SIZE MATH < $MAX CRI " | bc ) -eq
                       1]
 85
                                then
 86
                                exit 1
 87
                       elif [ $( echo "$SIZE MATH >= $MAX CRI " | bc ) -eq 1 ]
 88
                                then
 89
                                exit 2
 90
                       fi
 91
      fi
 92
      fi
 93
 94
      }
 95
 96
      FUNCTIONS REPORT APACHE ACCESS () {
 97
      for (( a = 0; a <= 10 ; a++ ))</pre>
 98
 99
                                do
100
                   FECHA INFO=$ (date --date="-$a day" +"%Y-%m-%d")
101
                   SIZE+=($( cat $ARCHIVO SIZEDIR | grep "$FECHA INFO" | awk '{print $2}' ))
102
      done
103
104
      SIZE+=($( cat $ARCHIVO INFO | grep "Numero de Consultas Totales son:" | awk '{print
      $7}'))
105
106
107
      for ((a=0; a< ${#SIZE[*]} - 1; a++))</pre>
108
                                do
109
                                let SUM=(SUM + SIZE[$a])
110
                                done
111
      x=${#SIZE[*]}
112
      let z=( x - 1 )
      let PROM=( SUM / z )
113
114
      let MAX=( PROM * 2 )
115
      let MAX CRI=( PROM * 3 )
116
117
      k=`echo "${#SIZE[*]} - 1 " | bc -1`
118
119
      echo "Numero de Peticiones son: "${SIZE[$k]}" MAX-NORMAL = "$MAX" MAX-CRITICAL =
      "$MAX CRI
120
121
              if [ ${SIZE[$k]} -gt $MAX SIZE INFO ]
122
                                then
123
                                exit 2
124
                       elif [
                               ${SIZE[$k]} -le $MAX ]
125
                                then
126
                                exit 0
127
                       elif [ ${SIZE[$k]} -gt $MAX -a ${SIZE[$k]} -lt $MAX CRI ]
128
                                then
129
                                exit 1
130
                       elif [ ${SIZE[$k]} -ge $MAX_CRI
                                                           1
131
                                then
132
                                exit 2
```

133 fi 134 135 136 } 137 while ["\$1" != ""]; do 138 139 case \$1 in 140 -t | --LOGSSIZE) shift 141 ARCHIVO INFO=\$1 142 shift 143 ARCHIVO SIZEDIR=\$1 144 shift LOG INFO=\$1 145 146 shift 147 MAX SIZE INFO=\$1 148 FUNCTIONS REPORT SIZE LOGS 149 ;; 150 -k | --BDDSIZE) shift 151 ARCHIVO INFO=\$1 152 shift 153 ARCHIVO SIZEDIR=\$1 154 shift 155 LOG INFO=\$1 156 shift MAX_SIZE_INFO=\$1 157 158 FUNCTIONS REPORT APACHE ACCESS 159 ;; 160 -h | --help) echo "-c {REPORTE COMPLETO} -l {ULTIMA HORA} -h HELP" 161 **echo** "--complete|-c --lasthour|-l --help|-h" 162 exit 163 ;; *) 164 echo "COMANDO NO ENCONTRADO" echo "Para mas ayuda --help|-h" 165 166 exit 167 ;; 168 esac 169 shift 170 171 done 172 173 exit 174

```
1
     #!/bin/bash
     #12/05/2021
 2
 3
     #AUTOR: JORGE AÑAZCO
 4
     #VERSION: 1
 5
     #In the there will be only chaos :^}
 6
 7
    FECHA=$ (date +%Y-%m-%d)
8
    MES=$(date +%m)
9
    YEAR=$ (date +%Y)
10
    SUM=0
11
    PROM=0
12
    MAX=0
13
14
     FUNCTIONS REPORT SIZE LOGS () {
     ARCHIVO SIZE LOG="/SIZEDIRPERDAYLOG.txt"
15
16
     LOG FINAL=$ (echo "$ARCHIVO INFO" | cut -d "/" -f 1,2,3,4,5,6)
17
     LOG="$LOG FINAL$ARCHIVO SIZE LOG"
18
19
     for (( a = 10; a > 0 ; a-- ))
20
                              do
21
                              FECHA=$ (date --date="-$a day" +"%Y-%m-%d")
22
                              SIZE+=($ ( cat $LOG | grep "$LOG INFO""$FECHA" | awk '{print
                              $1}'))
23
     done
24
     FECHA=$ (date --date="-$a day" +"%Y-%m-%d")
25
     SIZE+=($( cat $ARCHIVO INFO | grep "$LOG INFO$FECHA" | awk '{print $1}' ))
26
27
     for ((a=0; a< ${#SIZE[*]} - 1; a++))</pre>
28
                              do
29
                 typeset -i NUM CHARACTER=$( echo ${SIZE[$a]} | wc -m )
30
                 let d=(NUM CHARACTER - 2)
31
                 SIZE MATH=$( echo ${SIZE[$a]} | cut -c 1-"$d" )
32
                 let b=(NUM CHARACTER - 1)
33
                 TYPE=$( echo ${SIZE[$a]} | cut -c "$b" )
34
35
                 if [ $TYPE == 'K' ]
36
                          then
37
                                  SIZE MATH=`echo "$SIZE MATH / 1024" | bc -1`
38
                          fi
39
                 if [ $TYPE == 'G' ]
40
                          then
41
                              SIZE MATH=`echo "$SIZE MATH * 1024" | bc -1`
42
                          BAND=1
43
                          fi
44
                 SUM=`echo "$SUM + $SIZE MATH" | bc`
45
                 PROM=`echo "$SUM / ( ${#SIZE[*]} - 1 )" | bc -1`
46
47
                 done
48
49
    MAX=`echo "$PROM * 2 " | bc -1`
50
    MAX CRI=`echo "$PROM * 3 " | bc -1`
51
52
     k=`echo "${#SIZE[*]} - 1 " | bc -1`
53
     NUM CHARACTER=$ ( echo $ {SIZE [$k] } | wc -m )
54
     let d=(NUM CHARACTER - 2)
55
     SIZE MATH=$( echo ${SIZE[$k]} | cut -c 1-"$d" )
56
     let b=(NUM CHARACTER - 1)
57
     TYPE=$( echo ${SIZE[$k]} | cut -c "$b" )
58
59
     i= (echo $MAX | cut -c 1-5 )
60
     j=$( echo $MAX CRI | cut -c 1-5 )
61
62
63
     if [ "$BAND" == "1" ]
64
             then
65
                     echo "Tamano del LOG es: "$SIZE MATH$TYPE" MAX-NORMAL = "$i"M
                     MAX-CRITICAL = "$j"M Revisar los LOGS anteriores existe un log que
                     pesa mas de 1 GB"
66
             else
```

```
67
              echo "Tamano del LOG es: "$SIZE MATH$TYPE" MAX-NORMAL = "$i"M MAX-CRITICAL =
               "$j"M"
 68
      fi
 69
 70
 71
      if
          [ $TYPE == 'K' ]
 72
               then
 73
                       exit 0
 74
               else
 75
      if
          [ $TYPE == 'G' ]
 76
               then
 77
                   exit 2
 78
               else
 79
                       if [ $( echo "$SIZE MATH > $MAX SIZE INFO " | bc ) -eq 1 ]
 80
                                then
                   exit 2
 81
 82
                       elif [ $( echo "$SIZE MATH <= $MAX " | bc ) -eq 1 ]</pre>
 83
                               then
 84
                   exit 0
                       elif [ $( echo "$SIZE_MATH > $MAX && $SIZE_MATH < $MAX_CRI " | bc ) -eq
 85
                       1]
 86
                                then
 87
                               exit 1
 88
                       elif [ $( echo "$SIZE MATH >= $MAX CRI " | bc ) -eq 1 ]
 89
                               then
                               exit 2
 90
 91
                       fi
 92
      fi
 93
      fi
 94
 95
      }
 96
 97
 98
      FUNCTIONS REPORT SIZE DIR () {
 99
100
      SIZE=$( cat $ARCHIVO INFO | grep "$DIR LOG" | grep -v "postgresql" | awk '{print $1}' )
101
      typeset -i NUM CHARACTER=$ ( echo $SIZE | wc -m )
102
      let d=(NUM CHARACTER - 2)
103
      SIZE MATH=$ ( echo $SIZE | cut -c 1-"$d" )
104
      let b=(NUM CHARACTER - 1)
105
      TYPE=$( echo $SIZE | cut -c "$b" )
106
      echo "Tamano del LOG es: " $SIZE MATH$TYPE
107
108
      SIZE DIR=$(cat $ARCHIVO SIZEDIR | grep "$FECHA" | awk '{print $2}')
109
110
      typeset -i NUM CHARACTER=$ ( echo $SIZE DIR | wc -m )
111
      let d=(NUM CHARACTER - 2)
112
      SIZE MATH DIR=$ ( echo $SIZE DIR | cut -c 1-"$d" )
113
      let b=(NUM CHARACTER - 1)
114
      TYPE DIR=$( echo $SIZE DIR | cut -c "$b" )
115
116
117
      if [ $TYPE == 'K' ]
118
          then
119
          SIZE MATH=`echo "$SIZE MATH / 1024" | bc -1`
120
          fi
121
      if [ $TYPE == 'G' ]
122
          then
123
          SIZE MATH=`echo "$SIZE MATH * 1024" | bc -1`
124
          fi
125
126
      if [ $TYPE DIR == 'K' ]
127
               then
128
               SIZE MATH DIR=`echo "$SIZE MATH DIR / 1024" | bc -1`
129
              fi
          [ $TYPE DIR == 'G' ]
130
      if
131
              then
132
               SIZE MATH DIR=`echo "$SIZE MATH DIR * 1024" | bc -1`
133
               fi
```

```
134
135
      DIR PORCENTAJE=`echo "$SIZE MATH DIR * 0.1 " | bc -1`
136
137
      SUM1=`echo "$SIZE MATH DIR + $DIR PORCENTAJE " | bc -1`
138
      SUM2=`echo "$SIZE MATH DIR + ( $DIR PORCENTAJE * 2 ) " | bc -1`
139
140
       if [ $( echo "$SIZE MATH <= $SUM1 " | bc ) -eq 1 ]</pre>
141
                               then
142
                               exit 0
143
                       elif [ $( echo "$SIZE MATH > $SUM1 && $SIZE MATH < $SUM2 " | bc ) -eq 1 ]
144
                               then
145
                               exit 1
                       elif [ $( echo " $SIZE MATH > $SUM2 " | bc ) -eq 1 ]
146
147
                               then
148
                               exit 2
149
                       fi
150
151
152
      }
153
154
      FUNCTIONS REPORT SIZE BDD () {
155
      SIZE=$( cat $ARCHIVO INFO | grep "$DIRECTORIO" | awk '{print $5}' )
156
      TAMANO=$ ( cat $ARCHIVO INFO | grep "$DIRECTORIO" | awk '{print $2}' )
157
      UTILIZADO=$( cat $ARCHIVO INFO | grep "$DIRECTORIO" | awk '{print $3}' )
      DISPONIBLE=$( cat $ARCHIVO INFO | grep "$DIRECTORIO" | awk '{print $4}' )
158
159
      typeset -i NUM CHARACTER=$ ( echo $SIZE | wc -m )
160
161
      let d=(NUM CHARACTER - 2)
162
      SIZE MATH=$( echo $SIZE | cut -c 1-"$d" )
163
      let b=(NUM CHARACTER - 1)
164
      TYPE=$( echo $SIZE | cut -c "$b" )
165
      echo "El porcentaje es: " $SIZE MATH$TYPE "TAMANO = "$TAMANO" OCUPADO = "$UTILIZADO"
      DISPONIBLE = "$DISPONIBLE
166
167
       if [ $SIZE MATH -le 80 ]
168
                               then
169
                               exit 0
170
                       elif [ $SIZE MATH -gt 80 -a $SIZE MATH -lt 90 ]
171
                               then
172
                               exit 1
173
                       elif [ $SIZE MATH -ge 90 ]
174
                               then
175
                               exit 2
176
                       fi
177
178
179
      }
180
181
      while [ "$1" != "" ]; do
182
         case $1 in
183
             -t | --LOGSSIZE )
                                     shift
184
                                     ARCHIVO INFO=$1
185
                                     shift
186
                                     ARCHIVO SIZEDIR=$1
187
                                     shift
188
                                     LOG INFO=$1"-"
189
                                     shift
190
                                                                  MAX SIZE INFO=$1
191
                                     FUNCTIONS REPORT SIZE LOGS
192
                                     ;;
193
             -1 | --DIRSIZE )
                                     shift
194
                                     ARCHIVO INFO=$1
195
                                         shift
196
                                                                  ARCHIVO SIZEDIR=$1
197
                                     shift
198
                                     DIR LOG=$1
199
                                     FUNCTIONS_REPORT_SIZE_DIR
200
                                     ;;
             -k | --BDDSIZE )
201
                                     shift
```

202			ARCHIVO_INFO=\$1
203			shift
204			DIRECTORIO <mark>=\$1</mark>
205			FUNCTIONS REPORT SIZE BDD
206			;;
207		-h help)	echo "-c {REPORTE COMPLETO} -l {ULTIMA HORA} -h HELP"
208			echo "complete -clasthour -lhelp -h"
209			exit
210			;;
211		*)	echo "COMANDO NO ENCONTRADO"
212			echo "Para mas ayudahelp -h"
213			exit
214			;;
215	esac		
216		shift	
217			
218	done		
219			
220	exit		
221			

```
#!/bin/bash
1
2
   #10/06/2021
3
   #AUTOR: JORGE AÑAZCO
   #VERSION: 1
4
5
   #In the there will be only chaos :^}
6
7
   FUNCTIONS OPTION IP () {
      INFO HOST=$(echo $IP ADDRESS | perl -pi -e "s[\.][""]g")
8
9
      ARCHIVO VSPHERE=$ ( echo "/home/nagios/InfoVSphere/RVTools Diario IP/vSnapshot.csv" |
      perl -pi -e "s[IP]["$INFO HOST"]g" )
      if [ -f $ARCHIVO VSPHERE ]
10
11
          then
             typeset -i NUMERO LINEAS=$ (wc -1 $ARCHIVO VSPHERE | cut -d " " -f 1)
12
13
             if [ $NUMERO LINEAS = 1 ]
14
                 then
15
                              echo -e "No exite SnapShot en el Servidor"
16
                 exit 0
17
             else
18
                 let NUMERO SNAPSHOTS=(NUMERO LINEAS-1)
19
                 echo "\"EXISTEN SNAPSHOTS EN ESTE SERVIDOR\" | Numero de Snapshots =
                 "$NUMERO SNAPSHOTS
20
                 if [[ $NUMERO SNAPSHOTS > 1 && $NUMERO SNAPSHOTS < 7 ]]
21
                    # Se valida si el numero de snapshots son mayores a 1 y menores a 7
2.2
                    then
23
                       exit 1
24
                       # Si el numero de snapshots son entre 1 y 7 solo se da una
                       advertencia
25
                    else
                       exit 2
26
27
                       # Si el numero de snapshots son mayores a 7 se alerta
28
                 fi
29
30
          fi
31
      else
32
                 echo "\"ALERTA NO SE PUDO ENCONTRAR EL ARCHIVO .CSV FAVOR REVISAR\""
33
          exit 3
34
      fi
35
    }
36
37
    *****
38
   if [ "$1" == "" ]
39
40
       then
41
       echo "\"ALERTA\" ERROR EN EL COMANDO NO SE PUEDE PROCESAR"
42
       exit 3
43
   fi
44
   45
   while [ "$1" != "" ]; do
46
      case $1 in
47
    #_____
    -----#
48
          -p | --ipaddress )
                             shift
49
                IP ADDRESS=$1
50
                 FUNCTIONS OPTION IP
51
                ;;
    #-----
                   _____
52
                                                        _____
    -----#
53
          -h | --help )
                              echo "-p {IP ADDRESS} | -h HELP"
54
                              echo "--ipaddress|-p --help|-h"
55
                              exit 3
56
                             ;;
57
    #-----
      _____#
58
           * )
                             echo "COMANDO NO ENCONTRADO"
59
                 echo "Para mas ayuda --help|-h"
60
                 exit 3
61
                 ;;
```

62	esac		
63	shift		
64	done		
65			
66			
67	exit		
68			