

UNIVERSIDAD NACIONAL DEL SANTA FACULTAD DE INGENIERÍA

Escuela Profesional de Ingeniería de Sistemas e Informática



**"IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE
SEGURIDAD (COS) PARA MEJORAR LA SEGURIDAD EN LA RED
INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DEL SANTA"**

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE
SISTEMAS E INFORMÁTICA**

TESISTAS:

- Bach. Jimmy Gustavo Sánchez Revollo
- Bach. Sixto Moisés Ferrer Dulce

ASESOR:

Dr. GUILLERMO EDWARD GIL ALBARRAN

NUEVO CHIMBOTE – PERÚ

2021



UNIVERSIDAD NACIONAL DEL SANTA
FACULTAD DE INGENIERÍA
Escuela Profesional de Ingeniería de Sistemas e Informática

CONFORMIDAD DEL ASESOR

El presente trabajo de Tesis titulado:

"IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (COS) PARA MEJORAR LA SEGURIDAD EN LA RED INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DEL SANTA" elaborado por los bachilleres,

- **Bach. Jimmy Gustavo Sánchez Revollo**
- **Bach. Sixto Moisés Ferrer Dulce**

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

Revisado y aprobado por:

Dr. GUILLERMO EDWARD GIL ALBARRAN
Asesor



UNIVERSIDAD NACIONAL DEL SANTA
FACULTAD DE INGENIERÍA
Escuela Profesional de Ingeniería de Sistemas e Informática

JURADO EVALUADOR

El presente trabajo de Tesis titulado:

**"IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE
SEGURIDAD (COS) PARA MEJORAR LA SEGURIDAD EN LA
RED INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DEL
SANTA" elaborado por los bachilleres,**

- **Bach. Jimmy Gustavo Sánchez Revolledo**
- **Bach. Sixto Moisés Ferrer Dulce**

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO
DE SISTEMAS E INFORMÁTICA**

Ms. Camilo Ernesto Suarez Rebaza
PRESIDENTE

Dr. Guillermo Edward Gil Albarrán
SECRETARIO

Ms. Carlos Alfredo Gil Narvaez
INTEGRANTE

ACTA DE INSTALACIÓN PARA SUSTENTACIÓN DE TESIS

A los 26 días del mes de noviembre del año dos mil veintiuno, siendo las 11:00 am., cumpliendo con la Resolución N° 306-2020-CU-R-UNS (12.06.21) y la Directiva 003-2020-UNS-VRAC, sobre la "ADECUACIÓN DE LOS PROCEDIMIENTOS DE OBTENCIÓN DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES POR PARTE DE LOS ESTUDIANTES DE PREGRADO DE LA UNS, SE REALICE EN FORMA VIRTUAL; el Jurado Evaluador designado mediante Resolución N° 176 - 2021-UNS- CFI de fecha 08.06.2021, integrado por los docentes **Ms. Camilo Ernesto Suarez Rebaza (Presidente)**, **Dr. Dr. Guillermo Edward Gil Albarrán (Secretario)**, **Ms. Kene Abustamante Reyna Rojas (Integrante)**, **Ms. Carlos Alfredo Gil Narváez (Accesitario)**. Asimismo se indica que el Ms. Kene Abustamante Reyna Rojas, no se hizo presente a la sustentación por motivos de encontrarse con licencia por enfermedad; por lo tanto, a través del aplicativo virtual Zoom, se instaló el Jurado Evaluador quedando conformado de la siguiente manera: **MS. CAMILO ERNESTO SUAREZ REBAZA (Presidente)**, **DR. GUILLERMO EDWARD GIL ALBARRÁN (Integrante)**, **MS. CARLOS ALFREDO GIL NARVAEZ (Accesitario)**, y en atención a la Resolución Decanal N° 665-2021-UNS-FI de Declaración de Expedito de fecha 24.11.2021, se da inicio a la sustentación del Informe Final de Tesis, cuyo título es: "**IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (COS) PARA MEJORAR LA SEGURIDAD EN LA RED INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DEL SANTA**", perteneciente al Bachiller: **JIMMY GUSTAVO SÁNCHEZ REVOLLEDO, código N° 200514051**, tiene como **ASESOR** al Dr. **Guillermo Edward Gil Albarrán**, según T/Resolución Decanal N° 582-2018-UNS-FI, de fecha 24.09.2018.

Siendo las 12:00 pm. del mismo día, se da por iniciado el Acto de sustentación, para lo cual en señal de conformidad firma el Jurado en pleno la presente Acta.

Nuevo Chimbote, 26 de noviembre de 2021



MS. CAMILO ERNESTO SUAREZ REBAZA
PRESIDENTE



DR. GUILLERMO EDWARD GIL ALBARRÁN
SECRETARIO



MS. CARLOS ALFREDO GIL NARVAEZ
INTEGRANTE

ACTA DE EVALUACIÓN PARA SUSTENTACIÓN DE TESIS

A los 26 días del mes de noviembre del año dos mil veintiuno, siendo las 11:00 am., cumpliendo con la Resolución N° 306-2020-CU-R-UNS (12.06.21) y la Directiva 003-2020-UNS-VRAC, sobre la "ADECUACIÓN DE LOS PROCEDIMIENTOS DE OBTENCIÓN DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES POR PARTE DE LOS ESTUDIANTES DE PREGRADO DE LA UNS, SE REALICE EN FORMA VIRTUAL; el Jurado Evaluador designado mediante Resolución N° 176 - 2021-UNS- CFI de fecha 08.06.2021, integrado por los docentes **Ms. Camilo Ernesto Suarez Rebaza (Presidente)**, **Dr. Dr. Guillermo Edward Gil Albarrán (Secretario)**, **Ms. Kene Abustamante Reyna Rojas (Integrante)**, **Ms. Carlos Alfredo Gil Narváez (Accesitario)**. Asimismo se indica que el Ms. Kene Abustamante Reyna Rojas, no se hizo presente a la sustentación por motivos de encontrarse con licencia por enfermedad; por lo tanto, a través del aplicativo virtual Zoom, se instaló el Jurado Evaluador quedando conformado de la siguiente manera: **MS. CAMILO ERNESTO SUAREZ REBAZA (Presidente)**, **DR. GUILLERMO EDWARD GIL ALBARRÁN (Integrante)**, **MS. CARLOS ALFREDO GIL NARVAEZ (Accesitario)**, y en atención a la Resolución Decanal N° 665-2021-UNS-FI de Declaración de Expedito de fecha 24.11.2021, se da inicio a la sustentación del Informe Final de Tesis, cuyo título es: "**IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (COS) PARA MEJORAR LA SEGURIDAD EN LA RED INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DEL SANTA**", perteneciente al Bachiller: **JIMMY GUSTAVO SÁNCHEZ REVOLLEDO**, código N° 200514051, tiene como **ASESOR** al **Dr. Guillermo Edward Gil Albarrán**, según T/Resolución Decanal N° 582-2018-UNS-FI, de fecha 24.09.2018.

Terminada la sustentación, la tesista respondió a las preguntas formuladas por los miembros del Jurado Evaluador.

El Jurado después de deliberar sobre aspectos relacionados con el trabajo, contenido y sustentación del mismo y con las sugerencias pertinentes y en concordancia con el artículo 73° y 103° del Reglamento General de Grados y Títulos, vigente de la Universidad Nacional del Santa; considera la siguiente nota final de Evaluación:

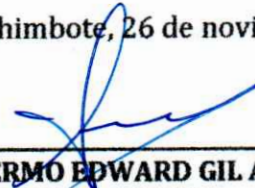
BACHILLER	PROMEDIO VIGESIMAL	PONDERACION
JIMMY GUSTAVO SÁNCHEZ REVOLLEDO	16	BUENO

Siendo la 12: 00 m. se dio por terminado el Acto de Sustentación y en señal de conformidad, firma el Jurado la presente Acta.

Nuevo Chimbote, 26 de noviembre de 2021



MS. CAMILO ERNESTO SUAREZ REBAZA
PRESIDENTE



DR. GUILLERMO EDWARD GIL ALBARRÁN
SECRETARIO



MS. CARLOS ALFREDO GIL NARVAEZ
INTEGRANTE

ACTA DE INSTALACIÓN PARA SUSTENTACIÓN DE TESIS

A los 26 días del mes de noviembre del año dos mil veintiuno, siendo las 11:00 am., cumpliendo con la Resolución N° 306-2020-CU-R-UNS (12.06.21) y la Directiva 003-2020-UNS-VRAC, sobre la "ADECUACIÓN DE LOS PROCEDIMIENTOS DE OBTENCIÓN DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES POR PARTE DE LOS ESTUDIANTES DE PREGRADO DE LA UNS, SE REALICE EN FORMA VIRTUAL; el Jurado Evaluador designado mediante Resolución N° 176 - 2021-UNS- CFI de fecha 08.06.2021, integrado por los docentes **Ms. Camilo Ernesto Suarez Rebaza (Presidente), Dr. Dr. Guillermo Edward Gil Albarrán (Secretario), Ms. Kene Abustamante Reyna Rojas (Integrante), Ms. Carlos Alfredo Gil Narváez (Accesitario)**. Asimismo se indica que el Ms. Kene Abustamante Reyna Rojas, no se hizo presente a la sustentación por motivos de encontrarse con licencia por enfermedad; por lo tanto, a través del aplicativo virtual Zoom, se instaló el Jurado Evaluador quedando conformado de la siguiente manera: **MS. CAMILO ERNESTO SUAREZ REBAZA (Presidente), DR. GUILLERMO EDWARD GIL ALBARRÁN (Integrante), MS. CARLOS ALFREDO GIL NARVAEZ (Accesitario)**, y en atención a la Resolución Decanal N° 665-2021-UNS-FI de Declaración de Expedito de fecha 24.11.2021, se da inicio a la sustentación del Informe Final de Tesis, cuyo título es: "**IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (COS) PARA MEJORAR LA SEGURIDAD EN LA RED INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DEL SANTA**", perteneciente al Bachiller: **SIXTO MOISES FERRER DULCE, código N° 200514010**, tiene como **ASESOR** al Dr. **Guillermo Edward Gil Albarrán**, según T/Resolución Decanal N° 582-2018-UNS-FI, de fecha 24.09.2018.

Siendo las 12:00 pm. del mismo día, se da por iniciado el Acto de sustentación, para lo cual en señal de conformidad firma el Jurado en pleno la presente Acta.

Nuevo Chimbote, 26 de noviembre de 2021



MS. CAMILO ERNESTO SUAREZ REBAZA
PRESIDENTE



DR. GUILLERMO EDWARD GIL ALBARRÁN
SECRETARIO



MS. CARLOS ALFREDO GIL NARVAEZ
INTEGRANTE

ACTA DE EVALUACIÓN PARA SUSTENTACIÓN DE TESIS

A los 26 días del mes de noviembre del año dos mil veintiuno, siendo las 11:00 am., cumpliendo con la Resolución N° 306-2020-CU-R-UNS (12.06.21) y la Directiva 003-2020-UNS-VRAC, sobre la "ADECUACIÓN DE LOS PROCEDIMIENTOS DE OBTENCIÓN DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES POR PARTE DE LOS ESTUDIANTES DE PREGRADO DE LA UNS, SE REALICE EN FORMA VIRTUAL; el Jurado Evaluador designado mediante Resolución N° 176 - 2021-UNS- CFI de fecha 08.06.2021, integrado por los docentes **Ms. Camilo Ernesto Suarez Rebaza (Presidente), Dr. Dr. Guillermo Edward Gil Albarrán (Secretario), Ms. Kene Abustamante Reyna Rojas (Integrante), Ms. Carlos Alfredo Gil Narváez (Accesitario)**. Asimismo se indica que el Ms. Kene Abustamante Reyna Rojas, no se hizo presente a la sustentación por motivos de encontrarse con licencia por enfermedad; por lo tanto, a través del aplicativo virtual Zoom, se instaló el Jurado Evaluador quedando conformado de la siguiente manera: **MS. CAMILO ERNESTO SUAREZ REBAZA (Presidente), DR. GUILLERMO EDWARD GIL ALBARRÁN (Integrante), MS. CARLOS ALFREDO GIL NARVAEZ (Accesitario)**, y en atención a la Resolución Decanal N° 665-2021-UNS-FI de Declaración de Expedito de fecha 24.11.2021, se da inicio a la sustentación del Informe Final de Tesis, cuyo título es: "**IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (COS) PARA MEJORAR LA SEGURIDAD EN LA RED INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DEL SANTA**", perteneciente al Bachiller: **SIXTO MOISES FERRER DULCE, código N° 200514010**, tiene como **ASESOR** al **Dr. Guillermo Edward Gil Albarrán**, según T/Resolución Decanal N° 582-2018-UNS-FI, de fecha 24.09.2018.

Terminada la sustentación, la tesista respondió a las preguntas formuladas por los miembros del Jurado Evaluador.

El Jurado después de deliberar sobre aspectos relacionados con el trabajo, contenido y sustentación del mismo y con las sugerencias pertinentes y en concordancia con el artículo 73° y 103° del Reglamento General de Grados y Títulos, vigente de la Universidad Nacional del Santa; considera la siguiente nota final de Evaluación:

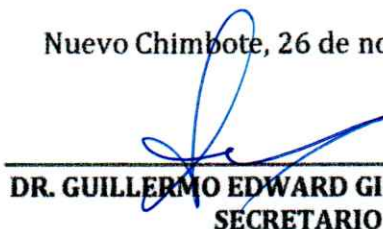
BACHILLER	PROMEDIO VIGESIMAL	PONDERACION
SIXTO MOISES FERRER DULCE	16	Bueno

Siendo la 12: 00 m. se dio por terminado el Acto de Sustentación y en señal de conformidad, firma el Jurado la presente Acta.

Nuevo Chimbote, 26 de noviembre de 2021



MS. CAMILO ERNESTO SUAREZ REBAZA
PRESIDENTE



DR. GUILLERMO EDWARD GIL ALBARRÁN
SECRETARIO



MS. CARLOS ALFREDO GIL NARVAEZ
INTEGRANTE

DEDICATORIA

A nuestros padres, por habernos apoyado incondicionalmente en nuestros proyectos profesionales.

A los docentes de la E.A.P. de Ingeniería de Sistemas e Informática, quienes nos inculcaron todos los conocimientos necesarios para desarrollarnos profesionalmente.

AGRADECIMIENTO

A nuestros jefes y compañeros de trabajo que colaboraron con nosotros en el proyecto de tesis con información diversa.

RESUMEN

La Universidad Nacional del Santa, institución académica de educación superior, donde a través de sus redes informáticas internas se traslada toda la información administrativa y académica, originada desde las diferentes oficinas, así como desde los equipos de estudiantes, docentes y administrativos, existiendo en forma permanente la amenaza de factores externos e internos, pues cada equipo enlazado a la red es una potencial puerta de ingreso y riesgo.

Por esto, se propone la implementación de una Centro de Operaciones de Seguridad (COS) para mejorar la seguridad en la Red Informática de la Universidad Nacional del Santa.

ABSTRACT

The Universidad Nacional del Santa, an academic institution of higher education, where through its internal computer networks all administrative and academic information is transferred, originated from the different offices, as well as from the student, teacher and administrative teams, existing in a way The threat of external and internal factors is permanent, since each equipment linked to the network is a potential entry and risk door.

Therefore, the implementation of a Security Operations Center (COS) is proposed to improve security in the Computer Network of the National University of Santa.

PRESENTACIÓN

SEÑORES MIEMBROS DEL JURADO EVALUADOR

UNIVERSIDAD NACIONAL DEL SANTA

De nuestra mayor consideración:

Siguiendo con el Reglamento de Grados y Títulos y de conformidad a la Ley Universitaria N° 30220, para optar el Título de INGENIERO DE SISTEMAS E INFORMÁTICA en la Escuela Profesional de Ingeniería de Sistemas e Informática, ponemos a disposición la presente tesis titulada **“IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (COS) PARA MEJORAR LA SEGURIDAD EN LA RED INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DEL SANTA”**.

Esperando que la presente cubra las expectativas y características solicitadas por las leyes universitarias vigentes de la Universidad, ponemos a su disposición señores Miembros del Jurado este informe para su revisión y Evaluación.

Atentamente,

Los Autores

INTRODUCCIÓN

La Universidad Nacional del Santa cada día maneja mayor información, tanto académica como administrativa, información que fluye como bits a través de la red informática, siendo necesario contar con un lugar centralizado desde donde se controle la seguridad de transmisión.

Un Centro de Operaciones de Seguridad permite gestionar las tecnologías relacionadas a las redes informáticas de una manera segura, para mantener la integridad, autenticidad y disponibilidad de la información.

El informe está dividido en capítulos estructurados de la siguiente manera:

CAPITULO I - LA INSTITUCIÓN. - En este capítulo se realiza una descripción de la Universidad Nacional del Santa.

CAPITULO II - PLAN DE INVESTIGACIÓN. - En este capítulo se determina el problema, los antecedentes del mismo, se enuncia hipótesis, el diseño de la investigación, los objetivos generales y específicos.

CAPITULO III - MARCO TEÓRICO. - En este capítulo se abarca los conceptos básicos involucrados en el desarrollo de la Tesis.

CAPITULO IV - MATERIALES Y MÉTODOS. - En este capítulo se detallan los materiales y métodos utilizados en la tesis.

CAPITULO V - RESULTADOS. - En este capítulo se muestra los resultados de la tesis.

CAPITULO VI - DISCUSIÓN. - Se realiza la contrastación de la Hipótesis.

CONCLUSIONES. - En esta parte se mencionan las conclusiones obtenidas del desarrollo del estudio.

RECOMENDACIONES. -En esta parte se dan las recomendaciones propuestas del estudio.

ÍNDICE

RESUMEN	V
ABSTRACT	VI
PRESENTACIÓN	VII
INTRODUCCIÓN	VIII
CAPÍTULO I.....	1
LA INSTITUCIÓN	
1.1. ANTECEDENTES DE LA INSTITUCIÓN	1
1.2. IDENTIFICACIÓN DE LA INSTITUCIÓN	4
1.2.1. DENOMINACIÓN	4
1.2.2. DOMICILIO LEGAL	4
1.2.3. UBICACIÓN TERRITORIAL	5
1.3. FUNCIONES DE LA UNS	6
1.4. FINES DE LA UNS	6
1.5. MISIÓN Y VISIÓN.....	7
1.6. ESTRUCTURA ORGÁNICA	7
1.7. OBJETIVOS.....	9
CAPÍTULO II	10
PLAN DE INVESTIGACIÓN	
2.1. EL PROBLEMA	10
2.1.1. REALIDAD PROBLEMÁTICA.....	10
2.1.2. ANÁLISIS DEL PROBLEMA	11
2.1.3. FORMULACIÓN DEL PROBLEMA.....	12
2.1.4. ANTECEDENTES	12

2.1.5.	JUSTIFICACIÓN DEL PROYECTO	17
2.2.	OBJETIVOS.....	18
2.2.1.	OBJETIVO GENERAL	18
2.2.2.	OBJETIVOS ESPECÍFICOS	18
2.3.	HIPÓTESIS	19
2.4.	VARIABLES	19
2.4.1.	VARIABLE INDEPENDIENTE.....	19
2.4.2.	VARIABLE DEPENDIENTE.....	19
CAPITULO III.....		21
MARCO TEÓRICO		
3.1.	SEGURIDAD INFORMÁTICA.....	21
3.1.1.	OBJETIVOS	22
3.1.2.	AMENAZAS	23
3.2.	CENTRO DE OPERACIONES DE SEGURIDAD	24
3.1.3.	OBJETIVO.....	26
3.1.4.	PROBLEMAS QUE RESUELVE	27
3.1.5.	CARACTERÍSTICAS	27
3.1.6.	VENTAJAS.....	28
3.1.7.	SERVICIOS DE VALOR AGREGADO DEL COS.....	29
3.3.	FUNDAMENTOS DE LA CIBERSEGURIDAD.....	33
CAPÍTULO IV		37
MATERIALES Y MÉTODOS		
4.1.	DISEÑO DE INVESTIGACIÓN	37
4.2.	METODOLOGÍA A SEGUIR	37
4.3.	COBERTURA DEL ESTUDIO.....	38

4.3.1. POBLACIÓN	38
4.3.2. MUESTRA	38
4.4. FUENTES TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS.....	38
CAPITULO V.....	39
RESULTADOS	
5.1. ESTADO DEL ARTE DE LA SEGURIDAD INFORMÁTICA Y CENTRO DE OPERACIONES DE SEGURIDAD	39
5.1.1. ACTUALIDAD DE LA SEGURIDAD INFORMÁTICA.....	39
5.1.2. ACTUALIDAD DE LOS CENTROS DE OPERACIONES DE SEGURIDAD	44
5.2. ANÁLISIS DE LA RED INFORMÁTICA DE LA UNS.....	51
5.2.1. INFRAESTRUCTURA INFORMÁTICA ACTUAL.....	53
5.3. EVALUACIÓN DE LA SEGURIDAD EN LA RED INFORMÁTICA DE LA UNS	63
5.4. ANÁLISIS Y DISEÑO DE LA PROPUESTA DEL CENTRO DE OPERACIONES DE SEGURIDAD	66
5.5. IMPLEMENTACIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD.....	71
5.6. LOGROS DEL CENTRO DE OPERACIONES DE SEGURIDAD.....	135
CAPITULO VI.....	137
DISCUSIÓN	
6.1. CONTRASTACIÓN DE LA HIPÓTESIS	137
6.2. EVALUACIÓN DE INDICADORES	138
6.3. CONCLUSIÓN.....	140
CONCLUSIONES.....	141
RECOMENDACIONES.....	142
BIBLIOGRAFÍA.....	143

A) BIBLIOGRAFÍA BÁSICA	143
B) BIBLIOGRAFÍA ESPECIALIZADA	143
ANEXOS.....	145
METODOLOGIA OSSIM	147
CASO FRECUENTE COS EN LA UNS	160

ÍNDICE DE FIGURAS

FIGURA 1. UBICACIÓN GEOGRÁFICA EN DISTRITO DE NUEVO CHIMBOTE.....	5
FIGURA 2. UBICACIÓN GEOGRÁFICA EN LA PROVINCIA DEL SANTA.....	5
FIGURA 3. ORGANIGRAMA DE LA UNS.....	8
FIGURA 4. PROPUESTA DE UN CENTRO DE OPERACIONES DE SEGURIDAD.....	25
FIGURA 5. PRINCIPAL OBJETIVO DEL CENTRO DE OPERACIONES DE SEGURIDAD.....	26
FIGURA 6. ESQUEMA DE LOS SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD.....	31
FIGURA 7. MODELO DE COS DE LA EMPRESA INGENIA.....	33
FIGURA 8. PILARES DE LA SEGURIDAD.....	34
FIGURA 9. FÓRMULA PARA MEDIR EL RIESGO.....	35
FIGURA 10. MAPA DE INFECCIÓN DEL QSNATCH.....	43
FIGURA 11. LOGO DE SYMANTEC.....	44
FIGURA 12. LOGO DE MCAFEE CORPORATION.....	44
FIGURA 13. CISCO CORPORATION.....	45
FIGURA 14. LOGO DE TREND MICRO.....	45
FIGURA 15. CENTRO DE OPERACIONES DE TELEFÓNICA.....	47
FIGURA 16. CENTRO DE OPERACIONES, IBM.....	48
FIGURA 17. CENTRO DE OPERACIONES SAN FERNANDO.....	49
FIGURA 18. SICUR, SALÓN INTERNACIONAL DE SEGURIDAD.....	50
FIGURA 19. EDIFICIO DE RECTORADO.....	52
FIGURA 20. VISTA DEL CAMPUS 1 DESDE EDIFICIO DE EDUCACIÓN.....	52
FIGURA 21. LÍNEA DE VISTA DEL EDIFICIO DE RECTORADO.....	53
FIGURA 22. UBICACIÓN DE LA UNS EN NUEVO CHIMBOTE.....	54
FIGURA 23. ARQUITECTURA DE RED INFORMÁTICA UNS.....	55
FIGURA 24. PLANO DE LA RED INFORMÁTICA EN EL CAMPUS 1 UNS.....	56
FIGURA 25. DISEÑO LÓGICO DE DISTRIBUCIÓN DE EQUIPOS EN EDIFICIOS.....	58
FIGURA 26. FIBRA ÓPTICA VIAJA SUBTERRÁNEA POR LA AVENIDA PRINCIPAL DEL CAMPUS UNIVERSITARIO.....	59
FIGURA 27. SERVICIO DE VIDEOCONFERENCIA LOCAL.....	61
FIGURA 28. SERVICIO DE TRABAJO EN GRUPO.....	62
FIGURA 29. MÓDULOS DE SISTEMAS DE INFORMACIÓN DE LA UNS.....	67
FIGURA 30. PAGINA WEB DE LA UNIVERSIDAD NACIONAL DEL SANTA.....	68
FIGURA 31. SELECCIONANDO EL MODO DE INSTALACIÓN DE OSSIM.....	71
FIGURA 32. SELECCIONANDO EL IDIOMA DE INSTALACIÓN DE OSSIM.....	72
FIGURA 33. SELECCIONANDO LA UBICACIÓN DE OSSIM.....	73
FIGURA 34. CONFIGURANDO EL TECLADO PARA OSSIM.....	74

<i>FIGURA 35. SE INICIA LA CARGA DE LOS COMPONENTES DE INSTALACIÓN OSSIM</i>	75
<i>FIGURA 36. CONFIGURACIÓN DE LA DIRECCIÓN IP</i>	76
<i>FIGURA 37. CONFIGURACIÓN DE LA MÁSCARA DE LA DIRECCIÓN IP</i>	77
<i>FIGURA 38. CONFIGURACIÓN DE LA IP DE LA PUERTA DE ENLACE</i>	78
<i>FIGURA 39. CONFIGURACIÓN DEL SERVIDOR DE NOMBRES</i>	79
<i>FIGURA 40. INICIO DE INSTALACIÓN DEL SISTEMA BASE</i>	80
<i>FIGURA 41. AVANCE DE INSTALACIÓN DEL SISTEMA BASE</i>	80
<i>FIGURA 42. CULMINACIÓN DE INSTALACIÓN DE OSSIM</i>	81
<i>FIGURA 43. INICIO DE OSSIM</i>	81
<i>FIGURA 44. LOGUEAR A OSSIM DESDE LA WEB 192.168.1.222</i>	82
<i>FIGURA 45. CONFIGURANDO EL TIPO DE MONITOREO DE OSSIM</i>	82
<i>FIGURA 46. PANTALLA PRINCIPAL SUPERIOR DE OSSIM</i>	83
<i>FIGURA 47. PANTALLA PRINCIPAL INFERIOR DE OSSIM</i>	83
<i>FIGURA 48. ACCESO A OSSIM DESDE MÁQUINA VIRTUAL LINUX CENTOS</i>	84
<i>FIGURA 49. MENÚ PRINCIPAL DE CONFIGURACIÓN DE OSSIM</i>	84
<i>FIGURA 50. SUBMENÚ PREFERENCIAS DEL SISTEMA</i>	85
<i>FIGURA 51. SUBMENÚ CONFIGURE SENSOR</i>	86
<i>FIGURA 52. CONFIGURANDO LA RED DE MONITOREO</i>	86
<i>FIGURA 53. CONFIGURANDO LA DIRECCIÓN IP DEL SERVIDOR OSSIM</i>	86
<i>FIGURA 54. CONFIGURANDO PLUGINS DE ORIGEN DE DATOS</i>	87
<i>FIGURA 55. ACTUALIZANDO LA CONFIGURACIÓN</i>	87
<i>FIGURA 56. INGRESANDO A MODO CONSOLA DE COMANDOS</i>	88
<i>FIGURA 57. CONFIRMACIÓN PARA INGRESO A MODO DE COMANDOS</i>	88
<i>FIGURA 58. VISUALIZANDO LOS PROCESOS EJECUTÁNDOSE EN EL SERVIDOR OSSIM</i>	89
<i>FIGURA 59. VISUALIZANDO LAS PARTICIONES DEL DISCO DURO DEL SERVIDOR OSSIM</i>	89
<i>FIGURA 60. VISUALIZANDO LAS PARTICIONES DEL DISCO DURO DEL SERVIDOR OSSIM</i>	90
<i>FIGURA 61. CONFIGURAR LA BÚSQUEDA DE NUEVOS ACTIVOS EN LA RED INFORMÁTICA</i>	91
<i>FIGURA 62. BÚSQUEDA DE HOSTS EN LA RE INFORMÁTICA</i>	92
<i>FIGURA 63. RESULTADOS DE BÚSQUEDA DE HOSTS</i>	93
<i>FIGURA 64. CONFIGURANDO GRUPO DE ACTIVOS DE LA RED INFORMÁTICA</i>	94
<i>FIGURA 65. GRUPO UNSRED RECIÉN CREADO</i>	95
<i>FIGURA 66. REDES CONFIGURADAS</i>	96
<i>FIGURA 67. VISUALIZANDO DETALLE DE ESTACIÓN DE TRABAJO WINDOWS</i>	97
<i>FIGURA 68. VISUALIZANDO DETALLES DE LA ESTACIÓN DE TRABAJO LINUX</i>	97
<i>FIGURA 69. VISUALIZANDO INFORMACIÓN DETALLADA DEL SERVIDOR WEB</i>	98
<i>FIGURA 70. EDICIÓN DE DETALLES DE UN ACTIVO</i>	99
<i>FIGURA 71. CONFIGURANDO LA DISPONIBILIDAD DEL SERVIDOR WEB</i>	100
<i>FIGURA 72. DISPONIBILIDAD CONFIGURADA PARA EL SERVIDOR WEB</i>	101

<i>FIGURA 73. RESULTADOS DE MONITOREO DEL SERVIDOR WEB</i>	<i>102</i>
<i>FIGURA 74. EDICIÓN DE SERVICIOS DEL SERVIDOR WEB</i>	<i>103</i>
<i>FIGURA 75. LOS SERVICIOS DEL SERVIDOR WEB CONFIGURADOS PARA MONITOREO</i>	<i>104</i>
<i>FIGURA 76. SERVICIOS MONITOREADOS EN LA RED UNS.....</i>	<i>105</i>
<i>FIGURA 77. VISUALIZANDO DETALLES DEL HOSTS SERVIDOR WEB.....</i>	<i>106</i>
<i>FIGURA 78. VISUALIZANDO EL STATUS DEL SERVIDOR WEB</i>	<i>107</i>
<i>FIGURA 79. VISUALIZANDO LOS SERVICIOS CON ERROR CRÍTICOS.....</i>	<i>108</i>
<i>FIGURA 80. ENCONTRANDO SOPORTE A ERROR CRITICO ENCONTRADO POR EL SERVIDOR OSSIM ..</i>	<i>109</i>
<i>FIGURA 81. VISUALIZANDO ALERTAS CUANDO SUCEDE UN PROBLEMA EN EL SERVIDOR WEB</i>	<i>110</i>
<i>FIGURA 82. MOSTRANDO EL DETALLE DEL STATUS DE LOS SERVICIOS EN TODOS LOS SERVIDORES.</i>	<i>111</i>
<i>FIGURA 83. VISUALIZANDO EL STATUS DE LOS HOSTS DENTRO DE LA RED INFORMÁTICA.....</i>	<i>112</i>
<i>FIGURA 84. CONFIGURANDO EL TIPO DE REPORTE A GENERAR EN EL SERVIDOR OSSIM.....</i>	<i>113</i>
<i>FIGURA 85. SELECCIONANDO EL SERVIDOR DEL CUAL SE HARÁ EL REPORTE.....</i>	<i>113</i>
<i>FIGURA 86. CONFIGURAR LAS OPCIONES DEL REPORTE.....</i>	<i>114</i>
<i>FIGURA 87. VISUALIZANDO EL REPORTE EN UN LAPSO DE TIEMPO.....</i>	<i>114</i>
<i>FIGURA 88. VISUALIZANDO UN HISTOGRAMA DE EVENTOS.....</i>	<i>115</i>
<i>FIGURA 89. MAPA DE RIESGOS A NIVEL MUNDIAL CONFIGURADO POR DEFECTO EN OSSIM.....</i>	<i>116</i>
<i>FIGURA 90. CONFIGURACIÓN DE MAPA REAL DE ACUERDO A LA INSTITUCIÓN</i>	<i>117</i>
<i>FIGURA 91. CARGANDO EL MAPA DE NUEVO CHIMBOTE</i>	<i>118</i>
<i>FIGURA 92. SERVIDORES UBICADOS EN LAS INSTALACIONES DE LA UNS DE ACUERDO AL MAPA DE RIESGOS.....</i>	<i>119</i>
<i>FIGURA 93. CONFIGURANDO LOS PARÁMETROS PARA MOSTRAR EVENTOS SIEM.....</i>	<i>120</i>
<i>FIGURA 94. VISUALIZANDO LOS EVENTOS DE LA RED INFORMÁTICA.....</i>	<i>121</i>
<i>FIGURA 95. VISUALIZANDO LOS EVENTOS EN TIEMPO REAL.....</i>	<i>122</i>
<i>FIGURA 96. TRATANDO DE ACCEDER AL SISTEMA OSSIM</i>	<i>123</i>
<i>FIGURA 97. SE MUESTRA EL EVENTO DONDE NOTIFICA DE INTENTO DE ACCESO CON USUARIO INEXISTENTE.....</i>	<i>124</i>
<i>FIGURA 98. INFORMACIÓN DETALLADA DEL EVENTO</i>	<i>125</i>
<i>FIGURA 99. INFORMACIÓN DETALLADA DEL EVENTO MOSTRADO EN MODO LOG.....</i>	<i>126</i>
<i>FIGURA 100. VISUALIZANDO LOS EVENTOS AGRUPADOS.....</i>	<i>127</i>
<i>FIGURA 101. CONFIGURANDO EL FILTRO DE LOS EVENTOS</i>	<i>128</i>
<i>FIGURA 102. VISUALIZANDO LOS EVENTOS FILTRADOS POR EL HOST 192.168.1.250.....</i>	<i>129</i>
<i>FIGURA 103. INGRESANDO A VISUALIZAR AMENAZAS A NIVEL MUNDIAL</i>	<i>130</i>
<i>FIGURA 104. INGRESANDO LA CUENTA OTX</i>	<i>131</i>
<i>FIGURA 105. VISUALIZANDO LAS AMENAZAS A NIVEL MUNDIAL REGISTRADAS.....</i>	<i>132</i>
<i>FIGURA 106. CONFIGURANDO LAS ALARMAS.....</i>	<i>133</i>
<i>FIGURA 107. ASIGNANDO UN TICKET A UNA ALERTA</i>	<i>134</i>
<i>FIGURA 108. LISTADO DE TICKETS GENERADOS EN LAS ALERTAS</i>	<i>135</i>

CAPÍTULO I

LA INSTITUCIÓN

1.1. ANTECEDENTES DE LA INSTITUCIÓN

La Universidad Nacional del Santa, creada por Ley N° 24035 del 20 de diciembre de 1984, es persona jurídica de derecho público. Se rige fundamentalmente por la Constitución Política del Perú, la Ley Universitaria N° 30220, el Estatuto y sus Reglamentos.

La Universidad Nacional del Santa es una comunidad académica orientada a la investigación, docencia, extensión cultural y proyección social que brinda una formación humanista, científica y tecnológica con clara conciencia de nuestro país como realidad multicultural. Adopta el concepto de educación como derecho fundamental y servicio público esencial. Está integrada por docentes, estudiantes y graduados.

La Universidad Nacional del Santa ha sido concebida, desde su creación, como universidad para el desarrollo, con clara conciencia de su compromiso con el bienestar y la justicia social, su respeto por la ciencia y la cultura, y la necesidad de su aporte al progreso del país y de la región, reconociendo los valores imprescriptibles de la libertad y la dignidad humana, los cimientos de la cultura nacional que hacen de la identidad del pueblo peruano, y la integración armónica de los sectores sociales que la componen.

La Universidad Nacional del Santa tiene su sede en el distrito de Nuevo Chimbote, provincia del Santa, departamento de Ancash; para el cumplimiento de sus fines dispone de unidades académico-administrativas.

La Universidad Nacional del Santa se identifica para todos los actos oficiales como UNIVERSIDAD NACIONAL DEL SANTA, cuya sigla es UNS y su logo es la figura del Punkurí, dentro de una franja ovalada con las palabras UNIVERSIDAD NACIONAL DEL SANTA CHIMBOTE-PERÚ.

El 20 de diciembre de cada año se declara “Día de la Universidad Nacional del Santa”, en conmemoración a la promulgación de la Ley N° 24035, ley de creación de la Universidad.

La UNS contaba desde 1986 con las escuelas profesionales de Ingeniería en Energía e Ingeniería Agroindustrial; en el año 1990 se inició la escuela profesional de Enfermería, y en año 1991 iniciaron las escuelas profesionales de Educación Inicial, Primaria y Secundaria, Comunicación Social, Biología en Acuicultura, Ingeniería Civil e Ingeniería de Sistemas e Informática.

Posteriormente, se crean cinco nuevas carreras: Ingeniería Mecánica, Ingeniería Agrónoma, Derecho y Ciencias Políticas y Biotecnología, en el año 2009; y en el año 2012 se crea la escuela profesional de Medicina Humana. Asimismo, se dio inicio a la construcción de la imponente infraestructura del Centro Cultural de la UNS y se construyó e inauguró el Instituto de Investigación Tecnológica Agroindustrial, el cual cuenta con una moderna infraestructura, así como con modernos equipos destinados a trabajos de investigación para el sector agroindustrial y afines.

Con el objetivo de seguir extendiendo su labor y contribución a la comunidad, en octubre de 2014 se puso en funcionamiento el Consultorio Jurídico Gratuito, el cual brinda el servicio de asesoría jurídica a todos los ciudadanos que la requieran.

En noviembre de 2014, se inauguró el imponente Centro Cultural de la UNS, el cual cuenta con un moderno auditorio, debidamente equipado y ambientes apropiados para el desarrollo de las diferentes actividades culturales y artísticas. Con la entrada en vigencia de la nueva Ley Universitaria N° 30220, asumen, en noviembre de 2015, las autoridades interinas, como rector el doctor Sixto Díaz Tello, acompañado de la doctora Lía Salazar Soto, como vicerrectora académica y el del doctor Fernando Merino Moya, como vicerrector de investigación. En julio de 2016, este mismo equipo de profesionales asume de manera definitiva la conducción de la UNS, para el período 2016 – 2021.

Durante esta nueva gestión, se han implementado, significativamente, los laboratorios con modernos y sofisticados equipos de las diversas escuelas profesionales. Incluso, se ha inaugurado el moderno laboratorio de Genética y Fisiología, de la Facultad de Ciencias, el cual es considerado uno de los mejores del país, por su moderna infraestructura y equipamiento.

Asimismo, la UNS ha logrado un importante incremento presupuestal que ha permitido mejorar la calidad de los servicios que brinda la UNS, se ha implementado la Planta Piloto Agroindustrial y se ha renovado el mobiliario de la Institución Educativa Experimental.

De igual manera, se ha recuperado los espacios invadidos (por más de 13 años) en el campus II y por ende se ha construido un amplio cerco para evitar futuras invasiones; así también se ha recuperado los terrenos invadidos en el Fundo Santa Rosa, en donde se han iniciado trabajos a cargo de la escuela de Ingeniería Agrónoma.

Actualmente, tras un largo proceso iniciado el 07 de agosto de 2017, la UNS ha logrado el licenciamiento institucional mediante Resolución N° 028-2019-

SUNEDU/CD, de fecha 11 de marzo de 2019, por una vigencia de 6 años, reconociendo la legalidad de todos sus programas educativos superiores, como los grados de bachilleres, licenciaturas, maestrías, doctorados y segundas especialidades.

A par de todo este desarrollo de la universidad, se nota que la tecnología de información y comunicación no ha ido creciendo en la misma magnitud, contando algunos edificios con red informática, en los puntos principales como autoridades, secretarías, y laboratorios de tecnologías; pero no llegan en forma eficiente a las aulas, ambientes de docentes, etc.

Asimismo, la red informática solo brinda acceso a la red de la universidad o acceso a internet, pero los paquetes viajan en forma transparente, sin ningún tipo de control o verificación, ante posibles ataques o fallas de seguridad, lo que hace riesgoso para los usuarios conectarse a la red, pudiendo permitir el acceso de virus, escaneos, copias, etc; lo que dependiente del tipo de información que se maneje y envíe, puede significar problemas para el usuario.

La integración de la red informática con los nuevos edificios, debe considerar una estrategia de seguridad, para controlar los paquetes que circulan, así como los usuarios que acceden.

1.2. IDENTIFICACIÓN DE LA INSTITUCIÓN

1.2.1. Denominación

UNIVERSIDAD NACIONAL DEL SANTA.

1.2.2. Domicilio Legal

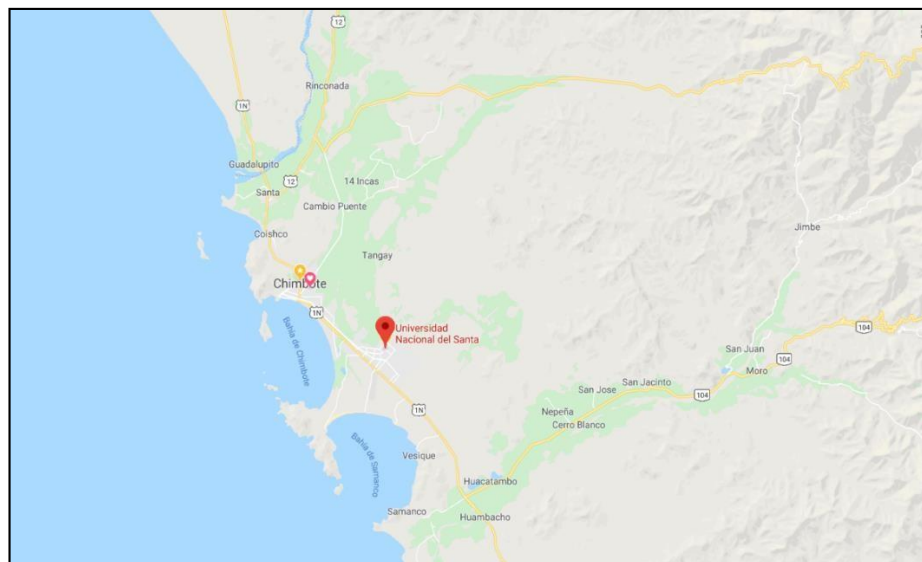
Av. Pacifico N° 508 – Nuevo Chimbote.

1.2.3. Ubicación Territorial:

La UNS se encuentra ubicada en el distrito de Nuevo Chumbote, teniendo 3 instalaciones: Edificio de Rectorado, Campus I y Campus II (recién en implementación).



*Figura 1. Ubicación Geográfica en Distrito de Nuevo Chumbote
Fuente: Google Map*



*Figura 2. Ubicación Geográfica en la Provincia del Santa
Fuente: Google Maps*

1.3. FUNCIONES DE LA UNS

Son funciones de la Universidad Nacional del Santa:

- Formación profesional.
- Investigación.
- Extensión cultural y proyección social.
- Educación continua.
- Contribución al desarrollo humano.
- Las demás que señala la Constitución Política del Perú, la Ley Universitaria N° 30220, su Estatuto y normas conexas.

1.4. FINES DE LA UNS

Son fines de la Universidad Nacional del Santa:

- Preservar, acrecentar y transmitir de modo permanente y con sentido crítico, la herencia científica, tecnológica, cultural y artística de la humanidad, y con preferente afirmación de la identidad regional y nacional.
- Formar profesionales de alta calidad de manera integral y con pleno sentido de responsabilidad social de acuerdo a las necesidades del país.
- Proyectar sus acciones y servicios a la comunidad para promover su cambio y desarrollo.
- Colaborar de modo eficaz en la afirmación de la democracia, el estado de derecho y la inclusión social.
- Realizar y promover la investigación científica, tecnológica y humanística; la creación intelectual y artística.
- Difundir el conocimiento universal en beneficio de la humanidad.

- Afirmar y transmitir las diversas identidades culturales del país.
- Promover el desarrollo humano y sostenible en el ámbito local, regional, nacional y mundial.
- Servir a la comunidad y al desarrollo integral.
- Formar personas libres en una sociedad libre.

1.5. MISIÓN Y VISIÓN

MISIÓN

Brindar formación profesional humanística, científica y tecnológica a los estudiantes, con calidad y responsabilidad social y ambiental.

VISIÓN

Todos desarrollan su potencial desde la primera infancia, acceden al mundo letrado, resuelven problemas, practican valores y saben seguir aprendiendo, se asumen ciudadanos con derechos y responsabilidades y contribuyen al desarrollo de sus comunidades y del país combinando su capital cultural y natural con avances mundiales.

1.6. ESTRUCTURA ORGÁNICA

En el siguiente organigrama se muestran los diferentes cargos administrativos y académicos en la Universidad Nacional del Santa. (Figura 3).

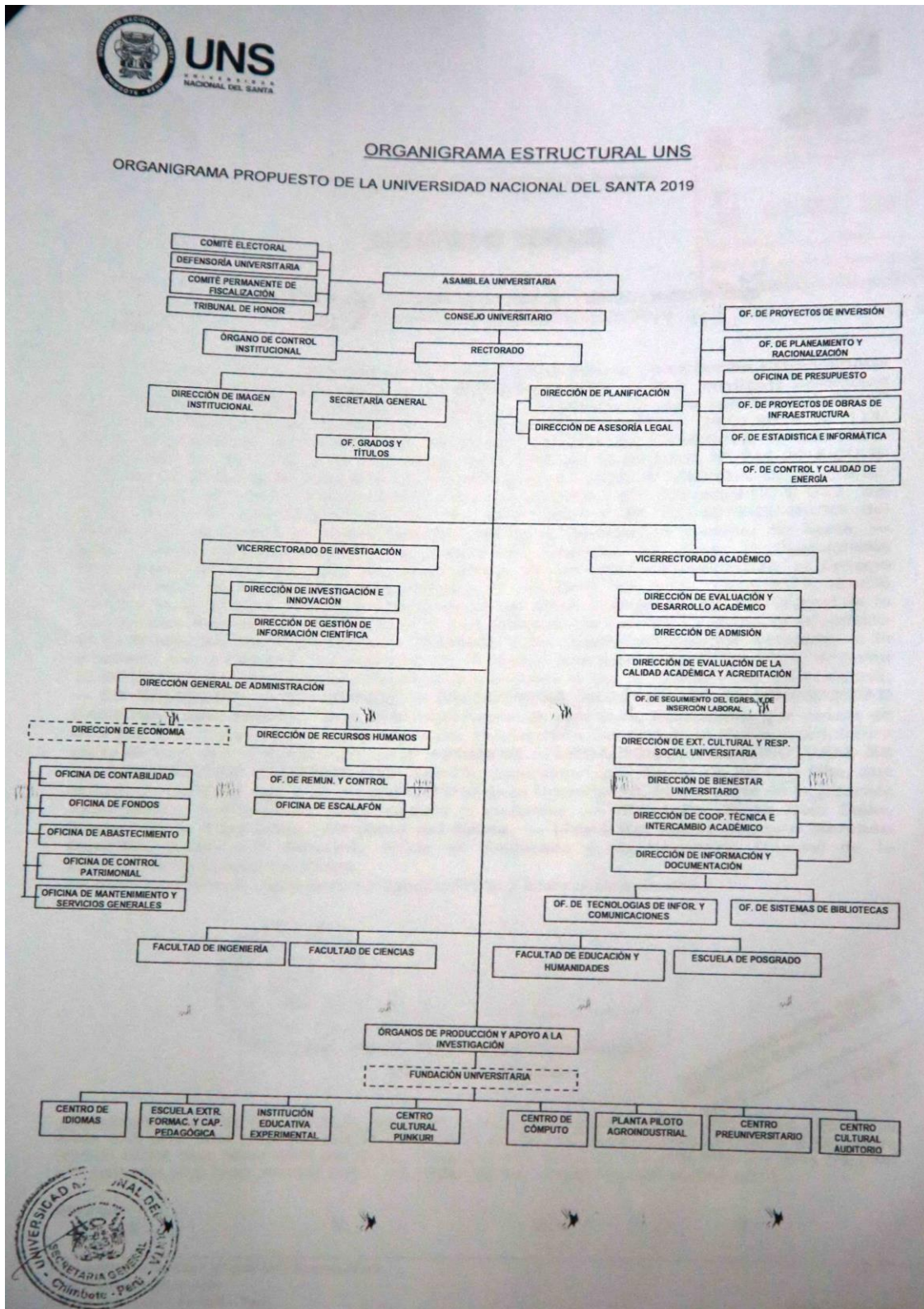


Figura 3. Organigrama de la UNS

1.7. OBJETIVOS

La Universidad Nacional del Santa tiene como objetivos los siguientes:

- Lograr la excelencia académica en todas sus Facultades;
- Asumir liderazgo en la promoción y difusión de la cultura a través de la proyección social, extensión universitaria e investigación;
- Impulsar el desarrollo de la región y el país a través de la investigación científica y tecnológica innovadora y la creación intelectual y artística;
- Lograr una plana docente altamente calificada para el ejercicio de la docencia, la investigación y la proyección y extensión universitaria.

CAPÍTULO II

PLAN DE INVESTIGACIÓN

2.1. EL PROBLEMA

2.1.1. REALIDAD PROBLEMÁTICA

Nos encontramos actualmente en la Era de la Información, donde cada vez las entidades y empresas depende de la información que generan y reciben de la interrelación con sus clientes y usuarios.

Mucha de la información esta digitalizada, y cada día irá incrementándose, viajando por sus redes informáticas, por lo cual el uso de medidas de seguridad es necesario, para impedir el acceso por parte de personas ajenas y que tengan como objetivo realizar daño a los sistemas.

El uso de medidas de seguridad en las instituciones ha ido estandarizándose a través del tiempo y ahora se propone que se creen centros especializados de operaciones de seguridad, de acuerdo al tipo de institución, donde se centralizara y monitoreara la seguridad, estando siempre pendientes de cualquier riesgo en camino.

La Universidad Nacional del Santa, luego de 32 años de funcionamiento, tiene mucha información almacenada en sus bases de datos e información que está siendo digitalizada, ya que son 32 promociones de estudiantes que han generado información en su relación con la universidad.

Debido al crecimiento de la red informática, actualmente se cuenta aproximadamente con 700 hosts (entre PCs, servidores, impresoras, switch, Access Point, lectoras de control de acceso), dentro de las cuales hay 10 servidores (físicos y virtualizados).

Cada equipo conectado a la red informática representa un riesgo, al poder ser una puerta abierta a virus, accesos no autorizados, ataques DoS, etc; y al no existir un sistema que monitoree, no se puede tener acceso a alertas que nos avisen ante una posible vulneración, dándonos cuenta cuando ya se produjo el problema.

La red informática de la UNS, esta basada en un solo dominio de broadcast, lo que hace que los paquetes circulen por toda la red, no existiendo ningún sistema de seguridad para que controle los riesgos en los activos, que son cada uno de los dispositivos conectados a la red.

Ante esto, es necesario poder contar con una Solución de Seguridad adecuada para la red informática de la UNS, teniendo en cuenta los requisitos de hardware y software con que cuenta la universidad. Una vez obtenido todos los requisitos relevantes, se debe diseñar la propuesta de la solución de acuerdo a los activos que se va a asegurar o monitorear.

Es por ello que el presente proyecto de investigación propone la “Implementación de un Centro de Operaciones de Seguridad (COS) para mejorar la Seguridad en la Red Informática de la Universidad Nacional del Santa”.

2.1.2. ANÁLISIS DEL PROBLEMA

La Universidad Nacional del Santa tiene actualmente 15 Escuelas Profesionales, donde se genera información académica de los estudiantes y docentes, la que viaja a través de la red informática, pues es ingresada en los sistemas de información.

La información que se genera en las diferentes oficinas académicas y administrativas de la universidad, así como desde los equipos informáticos

con que disponen los docentes y estudiantes, hacen que los riesgos a la red informática se incrementen, ya que cada punto en la red es una posible puerta de acceso a software dañino y accesos no deseados.

Esta distribución de los riesgos, hacen necesario que la universidad, a través de su oficina de tecnologías de información, implementen un centro de operaciones de seguridad, desde donde se pueda hacer seguimiento y control de todos los riesgos posibles, y puedan reducir al mínimo caídas a la red informática, así como vulneraciones a los datos que circulan en la red.

El crecimiento de la red informática, significa mayor cantidad de datos circulando en la red, de diferentes tipos dependiendo de los tipos de servicios que la universidad provee a sus usuarios, por lo que las medidas de seguridad tienen que ser adecuadas para hacer frente a los diferentes riesgos.

2.1.3. FORMULACIÓN DEL PROBLEMA

Después de Analizar la problemática que presenta la red informática de la Universidad Nacional del Santa, hemos plasmado esta realidad en la siguiente pregunta.

¿De qué manera la Implementación de un Centro de Operaciones de Seguridad (COS) mejorará la Seguridad en la Red Informática de la Universidad Nacional del Santa?

2.1.4. ANTECEDENTES

Existen trabajos de investigación relacionados con el tema tales como:

a) **TESIS DE PREGRADO:** “SEGURIDAD EN INFORMÁTICA

(AUDITORIA DE SISTEMAS)”¹

Autor: LUIS DANIEL ALVAREZ BASALDUA

México, 2005

Los trascendentales cambios operados en el mundo moderno, caracterizado por su incesante desarrollo; la acelerada globalización de la económica, la acentuada dependencia que incorpora en alto volumen de información y los sistemas que la proveen; el aumento de la vulnerabilidad y el amplio espectro de amenazas, tales como las amenazas cibernéticas; la escala y los costos de las inversiones actuales y futuras en información y en sistemas de información; y el potencial que poseen las tecnologías para cambiar drásticamente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos, han impuesto nuevos retos a la práctica de la profesión de auditoria, en particular a la auditoria de sistemas.

- b) **TESIS DE PREGRADO:** “METODOLOGIA DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION Y GESTION DE RIESGOS PARA LA PLATAFORMA SIEM DE UNA ENTIDAD FINANCIERA BASADA EN LA NORMA ISO/IEC 27035 E ISO/IEC 27005”

Autor: YESID ALBERTO TIBAQUIRA CORTES

Bogota, Colombia, 2015

El trabajo desarrollado se basa en la definición de un modelo de gestión de incidentes de seguridad de la información y de gestión de riesgos sobre estos incidentes, que son detectados o derivados de la

¹ <http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf>

implementación y operación de una herramienta SIEM (Correlacionador de Eventos de Seguridad). La definición de los modelos de gestión se realizó bajo las normas ISO 27035 para incidentes de seguridad y 27005 para la gestión de riesgos.

Inicialmente fueron identificaron los activos de información críticos que se encuentran configurados en el SIEM para definir el alcance del diseño en implementación de los modelos. Posterior, se definieron las políticas de seguridad de la información, en donde son descritos los lineamientos que se deben seguir para la gestión de incidentes y riesgos. Por último, fueron definidos los modelos, junto con la implementación y las herramientas que apoyarán su operación, basados en las recomendaciones que expresa cada una de las normas para cada modelo.

c) **TESIS PREGRADO: DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION PARA SERVICIOS POSTALES DEL PERU S.A.**

Autor: David Arturo Aguirre Mollehuanca

Lima, Perú, 2014

La exigencia de la implementación de la norma técnica peruana NTP-ISO/IEC 27001:2008 en las entidades públicas nace de la necesidad de gestionar adecuadamente la seguridad de la información en cada una de estas empresas. Sin embargo, el desconocimiento de estos temas por parte de la alta dirección, ha ocasionado que no se tomen las medidas necesarias para asegurar el éxito de este proyecto en el tiempo estimado por la Oficina Nacional de Gobierno Electrónico e Informática

(ONGEI), entidad responsable de apoyar a las entidades públicas durante el proceso de implementación de la norma.

Debido a ello, para la realización de este proyecto de fin de carrera, se decidió trabajar con una entidad pública como caso de estudio, a fin de diseñar un Sistema de Gestión de Seguridad de Información o SGSI que se acople a la normativa a la cual está sujeta la organización y que pueda, en un futuro, servir como referencia para la implementación del mismo.

En consecuencia, se realizaron varias reuniones con la alta dirección que permitieran definir el alcance y las políticas del SGSI en la organización enfocándose en los procesos institucionales críticos de dicha entidad, posteriormente se realizó una serie de entrevistas que permitieran identificar y valorar los activos críticos de la organización, así como identificar y evaluar los riesgos a los cuales estos estaban sometidos.

Por último, se presenta un documento llamado Declaración de Aplicabilidad en el cual se indica que controles de la NTP ISO/IEC 17799:2007 se pueden implementar dentro de la organización basado en el trabajo realizado dentro de la organización.

d) TESIS POSGRADO: “BUENAS PRACTICAS PARA LA IMPLEMENTACION DE LA SEGURIDAD EN UN CENTRO DE COMPUTO”.²

Autor: Leticia Hernandez Sanchez

Mexico, 2014.

² <http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/3735/Tesis.pdf?sequence=1>

Actualmente hay diferentes tipos de tecnologías las cuales van en aumento, dejando atrás la parte de seguridad en la información y en los distintos dispositivos con los que se cuenta. Por ejemplo, el caso de computadoras, celulares, tabletas, impresoras, etcétera.

En este tipo de dispositivos continúan surgiendo problemas de seguridad, debido a la falta de interés por parte de los usuarios, por no identificar la importancia de resguardar su información o datos personales, o simplemente al no elaborar una buena contraseña para sus correos electrónicos, cuentas bancarias, etcétera. En algunos casos hay filtros de información confidencial y personal, como colocar datos personales en encuestas, en páginas de redes sociales, fotografías, ubicación, posesión de bienes materiales, entre otros datos.

e) **TESIS POSGRADO: “METODOLOGIA PARA LA SEGURIDAD DE TECNOLOGIAS DE INFORMACION Y COMUNICACIÓN EN LA CLINICA ORTEGA”³.**

Autor: Goyo Francisco Guzman Pacheco

Huancayo, Peru, 2015

Es un hecho que los sistemas de gestión y de información están muy arraigados en los procesos productivos, industriales, de servicios, gubernamentales y casi cualquier sector activo de la sociedad. Esta dependencia de los sistemas de información en general, requiere dotar de seguridad a los mismos para preservar la calidad de los servicios y velar por la eficacia y eficiencia de los procesos de negocio y el valor de sus activos. Ya no es suficiente con establecer controles en forma

³ <http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/1478/Tesis-Goyo%20Francisco%20Guzman%20Pacheco.pdf?sequence=1&isAllowed=y>

aislada ni ad hoc, tampoco es suficiente actuar de modo meramente reactivo y defensivo, se requiere de un sistema de gestión de seguridad de tecnologías de información y comunicaciones y un accionar proactivo. Si consideramos un grupo empresarial, donde dos o más empresas se integran verticalmente, el desafío de gestionar la seguridad de una manera conveniente es aún mayor.

2.1.5. JUSTIFICACIÓN DEL PROYECTO

ECONÓMICA

- La Universidad Nacional del Santa podrá reducir costos en el mantenimiento de la seguridad en la red informática, al contar con un Centro de Operaciones de Seguridad (COS) permanente.
- Se evitará pérdidas de información, así como interferencias, lográndose reducir reclamos de los usuarios de la red informática y posibles estafas o uso indebido de los datos.
- La Universidad será reconocida por su alto nivel de seguridad, dando mayor confianza a los usuarios y sirviendo de modelo y consultoría para proyectos afines en otras instituciones públicas.

TÉCNICA

- La Universidad hará uso de un modelo de seguridad moderno para la red informática, a fin de garantizar la transferencia de datos entre todos los niveles.
- Prevención, Detección y Corrección de Riesgos en la red informática de la universidad.

OPERATIVA

- El proyecto permitirá robustecer el sistema de seguridad de información en la Universidad.
- El traslado de los datos a través de la red informática será segura, rápida y eficiente.
- El Centro de Operaciones de Seguridad (COS) permitirá que la administración de la seguridad sea fácil y transparente.

PERSONAL

Permitirá que los investigadores profundicen en los temas referentes a Seguridad de la Información, Redes Informáticas y Centro de Operaciones de Seguridad; y asimismo les permitirá obtener su título profesional.

2.2. OBJETIVOS

2.2.1. OBJETIVO GENERAL

Mejorar la Seguridad en la Red Informática de la Universidad Nacional del Santa a través de la implementación de un Centro de Operaciones de Seguridad (COS).

2.2.2. OBJETIVOS ESPECÍFICOS

- Lograr reducir el tiempo de respuesta en identificar riesgos en la red informática a través de sensores o alertas y realizar las acciones correctivas necesarias.

- Mejorar el nivel de confianza en la detección de fallas de seguridad en la red informática de la universidad nacional del santa, a través de la monitorización de los activos estratégicos.
- Incidir favorablemente en la toma de decisiones oportunas de los responsables de la red informática de la universidad, a través de indicadores gráficos.
- Construir el prototipo del Centro de Operaciones de Seguridad (COS) en la Red Informática de la UNS, para evaluar la mejora en la seguridad.

2.3. HIPÓTESIS

“La implementación de un Centro de Operaciones de Seguridad (COS) Mejora la Seguridad en la Red Informática de la Universidad Nacional del Santa”.

2.4. VARIABLES

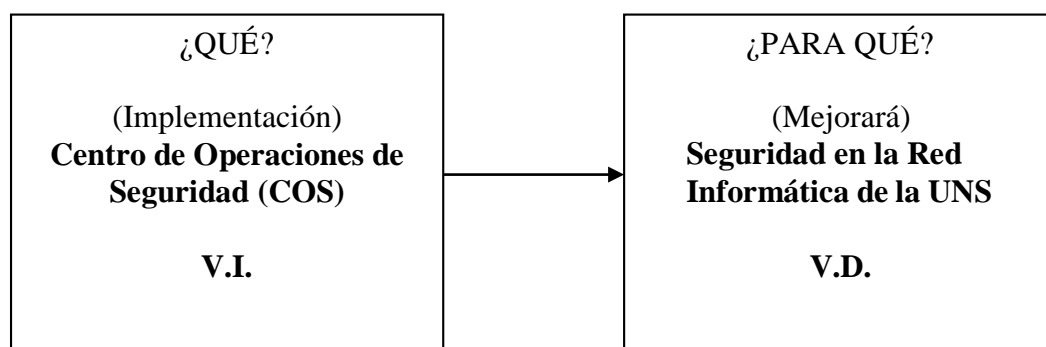
Para este proyecto de Investigación se han definido las siguientes variables:

2.4.1. Variable Independiente

Centro de Operaciones de Seguridad (COS).

2.4.2. Variable Dependiente

Seguridad en la Red Informática de la Universidad Nacional del Santa.



Indicadores

- VARIABLE INDEPENDIENTE: Centro de Operaciones de Seguridad (COS).
 - ✓ Facilidad de Gestión
 - ✓ Costos Reducidos
 - ✓ Nivel de Alcance

- VARIABLE DEPENDIENTE: Seguridad en la Red Informática de la UNS.
 - ✓ Tiempo de Respuesta
 - ✓ Fallas de Seguridad
 - ✓ Toma de Decisiones Oportunas

CAPITULO III

MARCO TEÓRICO

3.1. SEGURIDAD INFORMÁTICA

Si nos referimos a la seguridad en términos generales, hablamos de un estado de bienestar, de la ausencia de riesgo por la confianza que existe en alguien o algo. Con la finalidad de lograr esa confianza es que se determinan acciones sin importar el área en el que se apliquen.

Por tal motivo, autores como Urbina definen a la seguridad informática como: *“la disciplina con base en políticas y normas internas y externas de la empresa que se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático contra cualquier tipo de amenazas, minimizando los riesgos físicos y lógicos a los que está expuesta”* (Urbina Baca, 2016, pág. 12).

“La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnica destinados a conseguir un sistema de información seguro y confiable”.

Para establecer las medidas de seguridad es necesario realizar un análisis de riesgos donde se identifiquen los elementos que componen el sistema, su nivel de vulnerabilidad y los peligros que lo afectan. (Aguilera López, 2011)

La seguridad informática es una novedosa disciplina que se encuentra en crecimiento continuo, por el gran valor que dan a la información que fluye por las redes informáticas de las organizaciones. Mientras más se garantice la seguridad de los datos que circulan en forma de bits a través de los diferentes medios de

comunicación, más valor tendrá la información y la organización que las genera y procesa.

3.1.1. OBJETIVOS

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

- La infraestructura computacional: Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas, robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.
- Los usuarios: Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en

entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.

- La información: es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios. **(Ferro Veiga, José Manuel; 2020)**

3.1.2. AMENAZAS

No solo las amenazas que surgen de la programación y el funcionamiento de un dispositivo de almacenamiento, transmisión o proceso deben ser consideradas, también hay otras circunstancias que deben ser tomadas en cuenta e incluso «no informáticas». Muchas son a menudo imprevisibles o inevitables, de modo que las únicas protecciones posibles son las redundancias y la descentralización, por ejemplo, mediante determinadas estructuras de redes en el caso de las comunicaciones o servidores en clúster para la disponibilidad.

Las amenazas pueden ser causadas por:

- Usuarios: causa del mayor problema ligado a la seguridad de un sistema informático. En algunos casos sus acciones causan problemas de seguridad, si bien en la mayoría de los casos es porque tienen permisos sobre dimensionados, no se les han restringido acciones innecesarias, etc.
- Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador, abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano

informático, un troyano, una bomba lógica, un programa espía o spyware, en general conocidos como malware.

- Errores de programación: La mayoría de los errores de programación que se pueden considerar como una amenaza informática es por su condición de poder ser usados como exploits por los crackers, aunque se dan casos donde el mal desarrollo es, en sí mismo, una amenaza. La actualización de parches de los sistemas operativos y aplicaciones permite evitar este tipo de amenazas.
- Intrusos: persona que consiguen acceder a los datos o programas a los cuales no están autorizados (crackers, defacers, hackers, script kiddie o script boy, viruxers, etc.).
- Un siniestro (robo, incendio, inundación): una mala manipulación o una mala intención derivan a la pérdida del material o de los archivos.
- Personal técnico interno: técnicos de sistemas, administradores de bases de datos, técnicos de desarrollo, etc. Los motivos que se encuentran entre los habituales son: disputas internas, problemas laborales, despidos, fines lucrativos, espionaje, etc.
- Fallos electrónicos o lógicos de los sistemas informáticos en general.
- Catástrofes naturales: rayos, terremotos, inundaciones, rayos cósmicos, etc. (**Editorial CEP, 2017**)

3.2. CENTRO DE OPERACIONES DE SEGURIDAD

Para Oracle, un *Centro de Operaciones de Seguridad, SOC*, se refiere al equipo responsable de garantizar la seguridad de la información, cuyo objetivo es detectar, analizar y corregir incidentes de ciberseguridad utilizando soluciones tecnológicas

y enfoques diferentes. Las facultades de un SOC involucran supervisar y analizar la actividad en redes, servidores, terminales, bases de datos, aplicaciones, sitios web y otros sistemas en busca de señales débiles o comportamientos anormales que puedan indicar un incidente de seguridad o un compromiso. El SOC debe garantizar que los posibles incidentes de seguridad se identifiquen, analicen, defiendan, investiguen e informen adecuadamente. Los SOC están generalmente compuestos por analistas e ingenieros de seguridad, así como por gerentes que supervisan las operaciones de seguridad. Las capacidades adicionales de algunas SOC pueden incluir el análisis avanzado, el criptoanálisis y la ingeniería inversa del malware para analizar los incidentes. Los equipos de SSC trabajan en estrecha colaboración con los equipos de respuesta para garantizar que el problema de seguridad se aborde adecuadamente una vez que se ha descubierto. (ORACLE, s.f.)



Figura 4. Propuesta de un Centro de Operaciones de Seguridad

Según Biggeri (2018): “los centros de operaciones de seguridad se constituyen como un área de gestión capaz de articular procesos, personas y tecnologías con el fin de proteger los activos de la organización”.

3.1.3. Objetivo

Se dice que la información es el oxígeno de la edad moderna. Por ello, diversas entidades hacen uso de nuevas tecnologías para proteger su información. El objetivo general del COS es garantizar que los bienes y las personas estén seguros y protegidos en todo momento.

“El SOC se enfoca en la predicción, prevención, detección, análisis y respuesta a incidentes de seguridad cibernética con la ayuda de la tecnología y procesos bien definidos”

- Lograr capacidad operativa en la detección de incidentes de ciberseguridad, 7x24 on-site.
- Procesar y analizar grandes volúmenes de datos.
- Lograr colaboración operativa entre el sector público, el privado, la academia y la sociedad civil en forma continua.
- Compartir conocimiento de forma efectiva.
- Optimizar los procesos, recursos humanos y tecnológicos transversales a todo el departamento de seguridad. (Agesic, 2017).

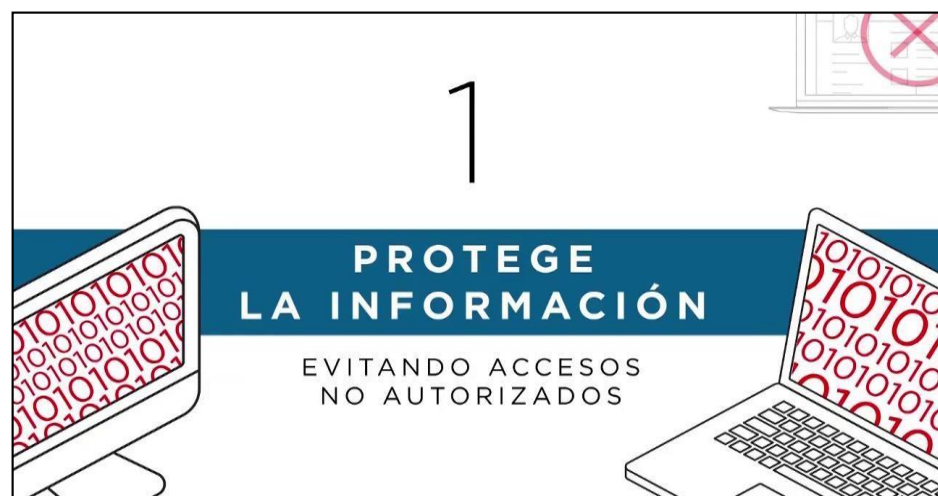


Figura 5. Principal Objetivo del Centro de Operaciones de Seguridad

3.1.4. Problemas que resuelve

- Monitoreo y respuesta ininterrumpida 24 horas al día los 365 días del año.
- Configuración de procesos de seguridad para automatizar tareas repetitivas e integrar los flujos de trabajo relacionados.
- Aumento de la productividad, cumplimiento de políticas e implementación mejores prácticas para detectar y responder a las amenazas.
- Optimización de la manera en que las tecnologías, el personal y el proceso trabajan en conjunto es fundamental para escalar las funcionalidades de seguridad según los riesgos que presentan amenazas cibernéticas avanzadas.
- Automatización de la tecnología, que implica aprovechar al máximo del tiempo del analista.
- Mesa de relacionamiento con colaboración estratégica a nivel nacional.
- Implementación de un LAB propio permanente.

3.1.5. Características

Según la (UPADEC02, 2012), una vez organizado el Centro de Control de Seguridad se debe formular un plan de reacción inmediata como parte del plan general de seguridad integral.

El plan de reacción inmediata se sustenta en cinco matrices:

1) Análisis de Riesgos

- Aplicación directa de un método.
- Evitar sobre valorización de riesgos.

- Establecer los recursos que se van a utilizar para cobertura adecuada de las emergencias.
- 2) Organización del Centro de Control de Seguridad.
- Establecer asignación de personal.
 - Establecer estructura requerida.
 - Establecer una definición lógica de perfiles.
- 3) Medios Técnicos Necesarios.
- Definir los sistemas necesarios para la cobertura de riesgos.
 - Establecer método para una valoración económica adecuada.
- 4) Valoración Económica.
- Establecer estimación económica adecuada.
 - Establecer diferencia entre gasto e inversión.
 - Contemplar en las estimaciones costos de mantenimiento.
 - Aceptar margen +/- 10 % del proyecto inicial.
- 5) Operaciones y Medidas de Ejecución:
- Formular manuales de procedimientos.
 - Ejecutar programas de formación.
 - Realizar auditorías de gestión y técnicas de Seguridad.

3.1.6. Ventajas

Su misión principal es cumplir con el Triángulo Crítico de Emergencias.

- Detección del riesgo.
 - Comunicación oportuna.
 - Respuesta inmediata.
- ❖ Otras funciones.
- Aviso técnico de fallas en su funcionamiento.

- Realización de maniobras sencillas de cambio de estado.
- Control de alarmas por omisión o error de procedimientos
- Análisis de datos para mejorar rendimiento de los sistemas operativos.
- ❖ Redes de Comunicación:
 - Deben estar implantadas en el sistema integral.
 - Deben estar seguras y estables.
 - Deben admitir el grado de prioridad deseado.
 - Tener un costo de manejo operativo asumible.
 - Tener una velocidad de comunicación y nivel de saturación asumible.
- ❖ Los Protocolos de Comunicación:
 - Deben ser lo más Standard posible.
 - Deberán soportar de forma adecuada, los equipos necesarios en el presente y el futuro.
 - Tener la capacidad para guardar toda la información deseada y necesaria.
 - Tener accesibilidad adecuada entre un simple código hasta la encriptación.

3.1.7. Servicios de valor agregado del COS

Según Biggeri (2018), su trabajo final de maestría menciona que los servicios de valor agregado del COS identificados por la empresa IBM son los siguientes:

- Gestión de incidentes de seguridad: Abarca acciones como la detección, análisis y la respuesta a incidentes (IBM Corporation, 2013). Este servicio se materializa mediante la ejecución del proceso de gestión de

incidentes y tendrá como objetivo la rápida y eficaz contención y respuesta a incidentes para minimizar el impacto.

- **Gestión de recursos de auditoría:** Es intrínseco a los COS que brinden el servicio de colección, análisis y almacenamiento de registros de auditoría y eventos de seguridad. Esto permitirá llevar a cabo la detección de incidentes de seguridad y el análisis forense en caso de resultar necesario.
- **Gestión de vulnerabilidades:** En caso de que el COS realice la gestión completa, incluyendo el descubrimiento y la remediación, entonces el servicio es brindado íntegramente por éste. Alternativamente, el COS puede actuar como nexo con proveedores que suministren información sobre vulnerabilidades descubiertas en la organización, como también actuar como nexo con los administradores encargados de implementar las medidas correctivas.
- **Monitoreo del cumplimiento:** Es un servicio que puede ser asignado a los centros de operaciones de seguridad y que contribuye tanto a la disminución del riesgo como también a la prevención de ser multados, con el impacto financiero y de reputación que podría conllevar. Este monitoreo puede ser tanto de normativa interna como externa en materia de seguridad informática.
- **Concientización:** Son actividades útiles para capacitar al personal sobre la detección de incidentes, cómo reportarlos y cómo reaccionar ante una situación de riesgo. Es dirigida para la educación en materia de seguridad informática.
- **Investigación forense:** Es un servicio brindado por el centro de operaciones de seguridad, actuando como referente técnico ante

eventuales cuestiones legales. Por ello el personal del COS debe estar capacitado para actuar en los casos utilizando tecnología dedicada y preservando al mismo tiempo la cadena de custodia.

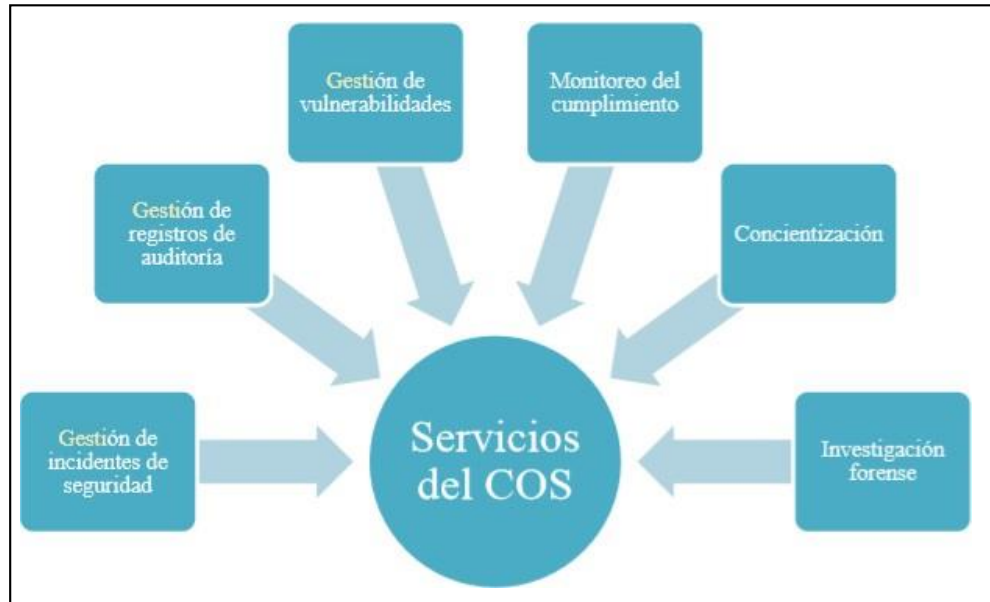


Figura 6. Esquema de los Servicios del centro de Operaciones de Seguridad
Recuperado de: " Centro de operaciones de seguridad. Estrategia, diseño y gestión", (Biggeri, 2018).

Por lo tanto, un Centro de Operaciones de Seguridad viene a ser un equipo centralizado de seguridad informática que monitorea la red informática corporativa las 24 horas del día, los 7 días de la semana, con el objetivo de diagnosticar vulnerabilidades, repeler ataques informáticos, detectar, mitigar y resolver las posibles intrusiones.

Presenta limitaciones por la alta rotación en el personal de seguridad haciendo que el proceso sea menos eficiente.

Las pequeñas y medianas empresas tienen poca capacidad económica para contratar personal especializado, que permita identificar ataques avanzados o resolver intrusiones.

Las ventajas que tiene implementar un SOC, son las siguientes:

- Personal Dedicado
- Mejor conocimiento del entorno
- Las soluciones son generalmente más fáciles de personalizar
- La comunicación durante un ataque es más rápida
- Por defecto, toda la información es controlada por la propia empresa.

Un Centro de Operaciones de Seguridad (SOC en inglés) es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet.

Los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, administración de riesgos y alertas de antivirus informáticos.

Hoy en día, la información es el activo más valioso de las empresas y su seguridad se ha vuelto de misión crítica dado que la mayoría de esta es almacenada en forma digital y el riesgo de sufrir algún tipo de ataque o riesgo va en aumento.

Dotado de servidores, firewalls, sistemas de detección de intrusos, software antivirus y otros sistemas especializados, un COS monitorea la actividad en las redes e Internet en tiempo real, las 24 horas del día, los 7 días de la semana. Los datos eventos son analizados y rastreados por expertos certificados en estándares de seguridad.

El mercado de la seguridad informática es el que más ha crecido en el segmento de servicios de tecnologías de la información.

Son escasos los centros con características de clase mundial. La mayoría se concentran en Europa, Estados Unidos y Asia-Pacífico.

Una adecuada política de implantación de las políticas de seguridad de una organización requiere de una adecuada monitorización, gestión y operación de la seguridad que permita responder lo antes posible y en cualquier momento ante un evento de seguridad.



Figura 7. Modelo de COS de la Empresa Ingenia

Fuente: <https://www.ingenia.es/es/servicio/centro-de-operaciones-de-seguridad-esoc>

3.3. FUNDAMENTOS DE LA CIBERSEGURIDAD

Los pilares de la seguridad de la información se fundamentan en esa necesidad que todos tienen de obtener la información, de su importancia, integridad y disponibilidad de la información para sacarle el máximo rendimiento con el mínimo riesgo.



Figura 8. Pilares de la Seguridad.

Fuente: Elaboración de los Autores

Para los autores, la seguridad está fundamentada por 3 pilares:

- Confidencialidad, que consiste en asegurar que sólo el personal autorizado acceda a la información que le corresponde y para garantizar la confidencialidad se recurre principalmente 3 recursos: autenticación de usuarios, gestión de privilegios y el cifrado de la información.
- Integridad, que consiste en asegurar que la información no se pierda y no se vea comprometida voluntaria e involuntariamente, si la manipulación de la información no es adecuada puede originar una cadena de errores acumulativos y que sucesivamente se tome decisiones equivocadas. Para garantizar la integridad de la información debemos considerar lo siguiente: monitorear el tráfico de red para descubrir posibles intrusiones, auditar los sistemas para implementar políticas de auditoría, implementar sistemas de control de cambios y gestionar copias de seguridad de la información que se genere en la institución.

- Disponibilidad, para decir que se dispone de una seguridad mínima en lo que a la información respecta, se debe implementar las medidas necesarias para que tanto la información y los servicios estén disponibles, si el acceso a la misma es tedioso o imposible, la información no resulta útil o valiosa.

Se debe considerar el riesgo como la probabilidad de que una amenaza concreta aproveche una determinada vulnerabilidad, para los autores, el riesgo se puede representar como el resultado de sumar el impacto producido por la amenaza y la probabilidad de que una vulnerabilidad permita que dicha amenaza tenga éxito.



*Figura 9. Fórmula para medir el riesgo.
Fuente: Elaboración de los autores*

En un sistema de evaluación de riesgo sencillo, se podría asignar un valor numérico a la importancia de una vulnerabilidad y otro valor a la importancia de una amenaza.

Tabla 1. Comparativa de evaluación de riesgos

Amenaza	Impacto	Probabilidad	Riesgo
Robo de credenciales en un sistema de control biométrico.	3	0	0
Infección por Spyware	3	2	6
Pérdida de suministro eléctrico	1	1	1

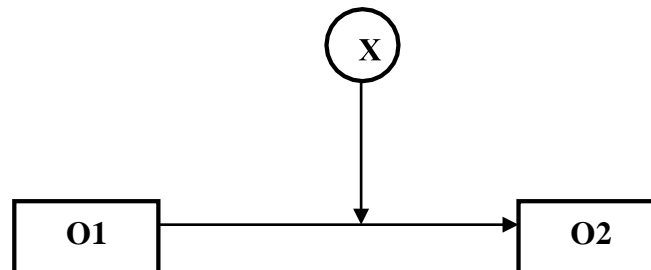
Fuente: Elaboración de los autores

Según la tabla anterior diseñada por los autores, las amenazas que no causan daño tendrían un impacto 0, mientras que las que causan un gran daño tendrían un valor de impacto 3, del mismo modo la probabilidad puede ser nula, baja, media o alta, con lo que se podría dar valores de probabilidad de 0 a 3, multiplicando ambos valores se obtendría el valor de riesgo. De esta forma se podría clasificar los distintos riesgos a los que se está expuesto y actuar en consecuencia, empezando por los de mayor gravedad. (Romero Castro, y otros, 2018)

CAPÍTULO IV

MATERIALES Y MÉTODOS

4.1. DISEÑO DE INVESTIGACIÓN



- **Observación N°01:** Situación Actual
- **Observación N°02:** Situación Final
- **X:** Implementación de un Centro de Operaciones de Seguridad.

4.2. METODOLOGÍA A SEGUIR

En el presente proyecto, se va a utilizar el método experimental que consistirá en 7 fases, con el fin de realizar una investigación más completa y precisa, permitiendo realizar correcciones en la etapa que la necesite.

1^{ra} Fase: Estudio bibliográfico sobre Seguridad Informática y Centro de Operaciones de Seguridad.

2^{da} Fase: Recopilación y análisis de la información obtenida en la Universidad Nacional del Santa sobre la Red Informática.

3^{ra} Fase: Evaluación de la Seguridad en la Red Informática de la UNS.

4^{ta} Fase: Análisis y Diseño de la propuesta del Centro de Operaciones de Seguridad (COS).

5^{ta} Fase: Implementación del Centro de Operaciones de Seguridad (COS).

6^{ta} Fase: Realización de la contrastación de la Hipótesis.

7^{ma} Fase: Desarrollo del Informe de Resultados Finales.

4.3. COBERTURA DEL ESTUDIO

4.3.1. POBLACIÓN:

Red Informática de la UNS

4.3.2. MUESTRA:

50% de los hosts que componen la Red Informática de la UNS

4.4. FUENTES TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

TÉCNICAS	INSTRUMENTOS
Prácticas de laboratorio	Fichas de laboratorio.
Observación	Ficha de observación
Revisión Bibliográfica.	Fichas bibliográficas.
Entrevista	Formato de Entrevista
Encuesta	Cuestionario

CAPITULO V

RESULTADOS

5.1. ESTADO DEL ARTE DE LA SEGURIDAD INFORMÁTICA Y CENTRO DE OPERACIONES DE SEGURIDAD

5.1.1. Actualidad de la Seguridad Informática

La seguridad informática, una disciplina en constante crecimiento, se desarrolla ante la necesidad de proteger nuestro activo más valioso que es la información, viene a ser la defensa en contra de los ataques digitales. Los métodos varían según la necesidad, la vulnerabilidad, y las amenazas que se encuentran presentes. El Departamento de Seguridad Nacional de los Estados Unidos ya lo dijo: “Nuestra vida diaria, la economía y la seguridad nacional dependen de un ciberespacio estable”.

Sin embargo, no todos los ataques son iguales, existen tres tipos reconocidos de hackers:

- **Hacker de Sombrero Blanco.** Estos hackers son profesionales que irrumpen legalmente en sistemas protegidos con el fin de probar su seguridad. Estos personajes son hackers ‘éticos’ que buscan detectar vulnerabilidades en redes y sistemas antes de que un hacker malicioso lo haga.
- **Hacker de Sombrero Negro.** Estos hackers irrumpen sistemas y redes con fines maliciosos, tales como propagar malware, robar datos, o espiar sistemas.

- Hackers de Sombrero Gris. Los hackers de sombrero gris también exponen vulnerabilidades y reportan problemas a sus dueños. Pero, estos usuarios nunca han pedido permiso para realizar los ataques. Generalmente llevan a cabo pruebas no autorizadas y luego piden una recompensa por sus logros.

El mundo de la seguridad digital evoluciona y cambia continuamente, por lo que es importante entender el estado del arte para proteger tus equipos. Para poder ilustrar el estado actual de la seguridad informática es necesario conocer las principales estadísticas determinada a finales del año 2018:

A) Seguridad Informática

- 70% de las organizaciones cree que su riesgo de seguridad creció considerablemente en el 2017. (Ponemon Institute)
- Se estima que para el 2020, el número de contraseñas utilizadas crecerá a 300 billones. (SC Media)
- 43% de los ciberataques afectan a pequeños negocios. (Small Business Trends)
- 230,000 nuevos malware son producidos cada día, y se predice que este número crecerá. (Panda Security)
- 90% de los hackers cubren sus rastros utilizando encriptación. (Vanson Bourne)
- A una compañía le toma entre 6 meses, o 197 días, detectar una brecha de seguridad. (ZD Net)
- Windows es el sistema operativo más atacado por hackers, Android viene en segundo lugar. (Computer World)

- Hubo más de 3 millones de golpes de crypto jacking entre enero y mayo del 2018. (Quick Heal)
- El número de variantes de malware de crypto jacking creció de 8 en el 2017 a 25 en mayo del 2018. (Quick Heal)

B) Costos de la Seguridad Informática

- El mercado de la seguridad informática crecerá un 8.7% en el 2019, llegando a los \$124 billones. (Computer Weekly)
- El costo total de un ciberataque exitoso es de más de \$5 millones de dólares, o \$301 por empleado. (Ponemon)
- El componente más caro de un ataque virtual es la pérdida de datos, que representa un 43% de los costos. (Accenture)
- Se proyecta que el daño relacionado a ciberataques llegará a los \$6 trillones de dólares anuales para el 2021. (CyberSecurity Ventures)
- La brecha de seguridad de Equifax le costó más de \$4 billones a la empresa. (Time)
- Los dos ataques más frecuentes son los ataques de malware y aquellos basados en la web. Las empresas gastan un estimado de \$2.4 millones en defensa. (Accenture)

C) Ransomware

- Ocurren más de 4,000 ataques de ransomware por día. (FBI)
- 75% de las organizaciones infectadas con ransomware tenían protección activa. (Sophos)

- Los daños globales relacionados a ataques de ransomware llegarán a \$11.5 billones en el 2019. (Cybersecurity Ventures)
- Se estima que habrá un ataque de ransomware cada 14 segundos para el fin del 2019. Esto no incluye ataques a individuos, que ocurren con mayor frecuencia. (Cybersecurity Ventures)
- 91% de los ataques comienzan con la técnica de spear phishing, que apunta a vulnerar correos e infectar organizaciones. (KnowBe4)

D) Phishing

- En una encuesta realizada a más de 1300 profesionales de TI se descubrió que 56% de las organizaciones identificaron al phishing como su mayor riesgo de seguridad informática. (CyberArk)
- 76% de los negocios reportaron ser víctimas de ataques phishing en el último año. (Wombat Security)
- Verizon reporta que usuarios estadounidenses abren un 30% de todos los correos maliciosos y un 12% de ellos dan clic al enlace peligroso. (Verizon)
- Kaspersky's ha detectado 246,231,645 intentos de phishing en el 2017, y evidenció un crecimiento de 91 millones con respecto al 2016. (Kaspersky).

Recientemente, miles de dispositivos QNAP NAS han sido infectados con el malware "QSnatch" a nivel mundial⁴ y se sigue expandiendo, este ataca el firmware para obtener persistencia de reinicio. El código del malware tiene las siguientes capacidades, pero aún se desconoce cuál es su objetivo:

- Modificar trabajos y scripts temporizados del sistema operativo (cronjob, scripts de inicio).
- Evita futuras actualizaciones de firmware sobrescribiendo las URL de origen de la actualización.
- Impide que se ejecute la aplicación QNAP MalwareRemover nativa.
- Extrae y roba nombres de usuario y contraseñas para todos los usuarios de NAS.

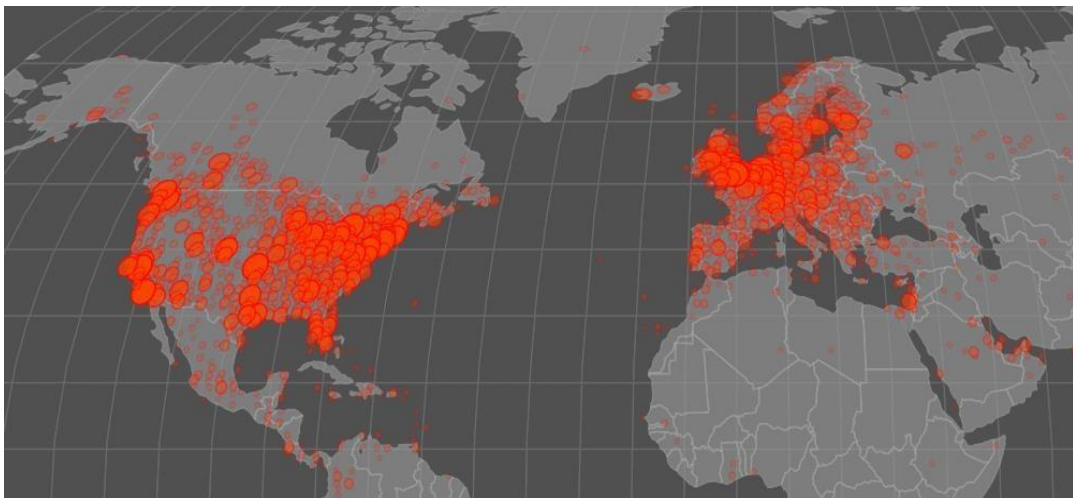


Figura 10. Mapa de Infección del QSnatch

Recuperado de <https://www.zdnet.com/article/thousands-of-qnap-nas-devices-have-been-infected-with-the-qsnatch-malware/>

⁴ <https://www.zdnet.com/article/thousands-of-qnap-nas-devices-have-been-infected-with-the-qsnatch-malware/?fbclid=IwAR109ghS9yDYZdV2WCxfurXIUw4RJBW13MG4ng6-1OGsb-w8M088vhEyTQE>

5.1.2. Actualidad de los Centros de Operaciones de Seguridad

Los Centros de Operaciones de Seguridad son una necesidad latente en todas las organizaciones, existiendo en el mercado de las TIC soluciones dadas por diferentes fabricantes, siendo los proveedores de soluciones de seguridad más conocidos: Symantec, McAfee, Cisco, Trend y otros (Biggeri, 2018).

“Es una solución del servidor de cliente que protege equipos portátiles, equipos de escritorio y servidores en su red contra el software malicioso, los riesgos y las vulnerabilidades” (Symantec, 2019).



Figura 11. Logo de Symantec.

Recuperado de www.symantec.com

“Es una empresa de ciberseguridad de vanguardia, ofrece soluciones de seguridad avanzadas a particulares, pymes, grandes empresas y organismos públicos. Las tecnologías de seguridad de McAfee utilizan una función predictiva y exclusiva, con tecnología McAfee Global Threat Intelligence, lo que permite a los usuarios particulares y a las empresas ir un paso por delante de la siguiente oleada de ataques sin archivos, virus, malware y otras amenazas online” (McAfee, 2019).



Figura 12. Logo de McAfee Corporation.

Recuperado de www.mcafee.com

“Ayuda a aprovechar las oportunidades del mañana al demostrar que pueden suceder cosas asombrosas cuando se conecta a los desconectados. Una parte integral del ADN es crear asociaciones duraderas con los clientes, trabajando juntos para identificar las necesidades de los clientes y brindar soluciones que impulsen su éxito” (Cisco, 2019).



Figura 13. Cisco Corporation.

Recuperado de: <https://newsroom.cisco.com/overview>

“Trend Micro: Es líder mundial en ciberseguridad, ayuda a hacer que el mundo sea seguro para el intercambio digital de información. En un mundo cada vez más conectado, nuestras soluciones innovadoras para consumidores, empresas y gobiernos proporcionan seguridad por capas para centros de datos, entornos de nube, redes y puntos finales” (Micro, 2019).



Figura 14. Logo de Trend Micro.

Recuperado de: https://www.trendmicro.com/es_es/about.html

APLICACIONES

Un centro de operaciones de seguridad(COS) es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en internet.

Existen en el mercado varias empresas a nivel internacional las cuales proveen dichos servicios como lo son Symantec, Telefónica, McAfee, Cyttek, entre otras.

Aplicación 1: COS de telefónica

Telefónica es una de las mayores compañías de telecomunicaciones del mundo con más de 127.000 empleados y presente en 24 países, siendo sinónimo de seguridad, pero esta seguridad solo tiene sentido si como empresa es capaz de acercarla a sus millones de clientes.

Prevención, detección y respuesta forma parte del ADN de Eleven Paths la unidad de ciberseguridad de telefónica. La capacidad operativa de telefónica se basa en la actividad de sus centros de operaciones de seguridad, los cuales están localizados en distintos puntos del mundo (ElevenPaths, 2016).

Sus centros de operaciones de seguridad se basan en una gestión inteligente, enfocada en la monitorización y respuesta en tiempo real de la experiencia del cliente. Los SOC de telefónica se han visto reforzados con la firma de la mayor alianza mundial de seguridad de telecomunicaciones, lo cual le permite como empresa posicionarse con una completa cartera de servicios.

La SOC de telefónica en Madrid es un espacio en donde más de 400 personas gestionan la seguridad de sus clientes 24 horas al día; 7 días a la semana y que está avalado por más de 400 certificaciones profesionales, aquí se relacionan tecnológicas, procesos y personas para que cada cliente pueda disponer de la máxima seguridad.



Figura 15. Centro de Operaciones de Telefónica

Recuperado de: SOC de Telefónica (Centro de Operaciones de Seguridad)

Aplicación 2: Simulador virtual del centro de operaciones de seguridad de IBM

Este simulador lo que hace es poner en relieve la importancia de que los clientes cuenten con las herramientas y los servicios adecuados para detectar y responder de forma efectiva ante un incidente de seguridad (España, 2018).

Desde IBM se puede ayudar a los clientes con tecnologías como QRADAR que permite monitorizar y responder de forma orquestada antes

esos incidentes , también se puede contar con la parte de servicios con sus centros Soc que pueden ayudar a los clientes a externalizar toda la función de operación de seguridad, así mismo con sus equipos especializados x-force irish que ayudan en toda la parte preventiva en la definición de los planes de respuesta efectivos y también en la parte reactiva donde pueden ayudar a los clientes que hayan sido afectados por un incidente de seguridad ayudarlo a contenerlo y remediarlo.

Un centro de operaciones de seguridad está basado en la plataforma IBM QRADAR que es la solución que propone IBM para resolver este tipo de soluciones.



Figura 16. Centro de Operaciones, IBM.

Recuperado de: Simulador virtual del centro de operaciones de seguridad de IBM

Aplicación 3: Centro de operaciones para la seguridad ciudadana

Este centro se llevó a cabo en San Fernando en el que se inauguró un centro de operaciones para mejorar la seguridad de los ciudadanos, siendo un edificio moderno y de última generación en el que se encuentra el centro de monitoreo de cámaras de seguridad, en la cual 120 operadores vigilan las cámaras de seguridad las 24 horas del día todo el año y que da la posibilidad de expandir la red de dispositivos y alcanzar el objetivo de una cámara cada 300 habitantes.

Además de centralizar las funciones de todos los mecanismos y sistemas de secretaría de protección ciudadana, optimizando la articulación y mejorando los tiempos de respuestas (San Fernando, 2016).



Figura 17. Centro de Operaciones San Fernando.

Recuperado de: Nuevo Centro de Operaciones de Seguridad

Aplicación 4: Centros de operaciones de seguridad de Securitas

La empresa internacional securitas tiene su nuevo centro de operaciones COS que permite la integración y gestión de todo servicio de seguridad en el ámbito nacional (EFE, 2014). Gracias a la utilización de las últimas herramientas tecnológicas securitas se integra en un solo centro de control los 3 pilares claves de su servicio.

La vigilancia física a través de su guardia de seguridad, la vigilancia a través de su tecnología y los servicios de consultoría para particulares empresas y administraciones. Con la presentación y la puesta en funcionamiento del COS securitas quiere dar respuesta a las demandas de sus clientes que siguen iguales o servicios ampliados a precios cada vez más competitivos.



Figura 18. Sicur, Salón Internacional de Seguridad.

Recuperado de: Securitas presenta en Sicur su nuevo Centro de Operaciones y Servicios (COS)

5.2. ANÁLISIS DE LA RED INFORMÁTICA DE LA UNS

Los procesos administrativos y los servicios en la U.N.S. no se encuentran en su totalmente digitalizados, pero si los procesos principales, como el registro de datos académicos de los estudiantes, desde la etapa de postulación a través de la dirección de admisión, hasta que egresa de la universidad, registrándose información a través de las Escuelas Profesionales, la Decanatura, la Dirección de Evaluación y Desarrollo Académico, y Secretaria General.

A pesar de contar con infraestructura moderna en la UNS, el servicio que se viene prestado a la comunidad universitaria no es óptimo, presentando baja velocidad en el acceso a la red, así como caídas en algunos servicios. Siendo una de los parámetros a tener en cuenta para la seguridad de la información.

La universidad está en continuo crecimiento, cada día se necesita almacenar mayor información tanto académica sobre los estudiantes y docentes, como administrativa sobre los administrativos y los procesos administrativos que se desarrollan, lo que hace que la red informática por donde fluyen los datos necesite mayor ancho de banda o una mejor administración. Así se brindará un servicio óptimo.

Existe en la actualidad un reducido número de personal en el área de seguridad de la red informática, no realizándose un control permanente, que pueda evaluar el servicio y los riesgos a los que esta propenso, así mismo el personal no cuenta con conocimientos necesarios sobre seguridad.

La Red Informática se desplaza sobre todo el Campus 1 de la universidad, así como por el edificio del rectorado, siendo localizaciones alejadas. Más aun ahora se está realizando las propuestas para ampliar la red informática al Campus 2, donde se están construyendo nuevas edificaciones.



Figura 19. Edificio de Rectorado

Fuente: Álbum fotográfico de la UNS



Figura 20. Vista del Campus 1 desde edificio de Educación

Fuente: Álbum fotográfico de la UNS

5.2.1. Infraestructura Informática Actual

A) Radioenlace

Existe un radioenlace desde el Campus 1 (antena ubicada en el pabellón de CECOMP), hasta el edificio de rectorado. La línea de vista se aprecia, de aproximadamente 3 kms.



Figura 21. Línea de Vista del Edificio de Rectorado

Fuente: Álbum de Fotos de la UNS

La Universidad está distribuida en el distrito de Nuevo Chimbote, contando con el edificio de Rectorado, en la Av. Pacifico, el Campus 1 que se encuentra en la Av. Universitaria y el Campus 2 que está en la Av. Central.

La red informática tendrá que interconectar los diferentes locales, para permitir la transferencia de los datos.

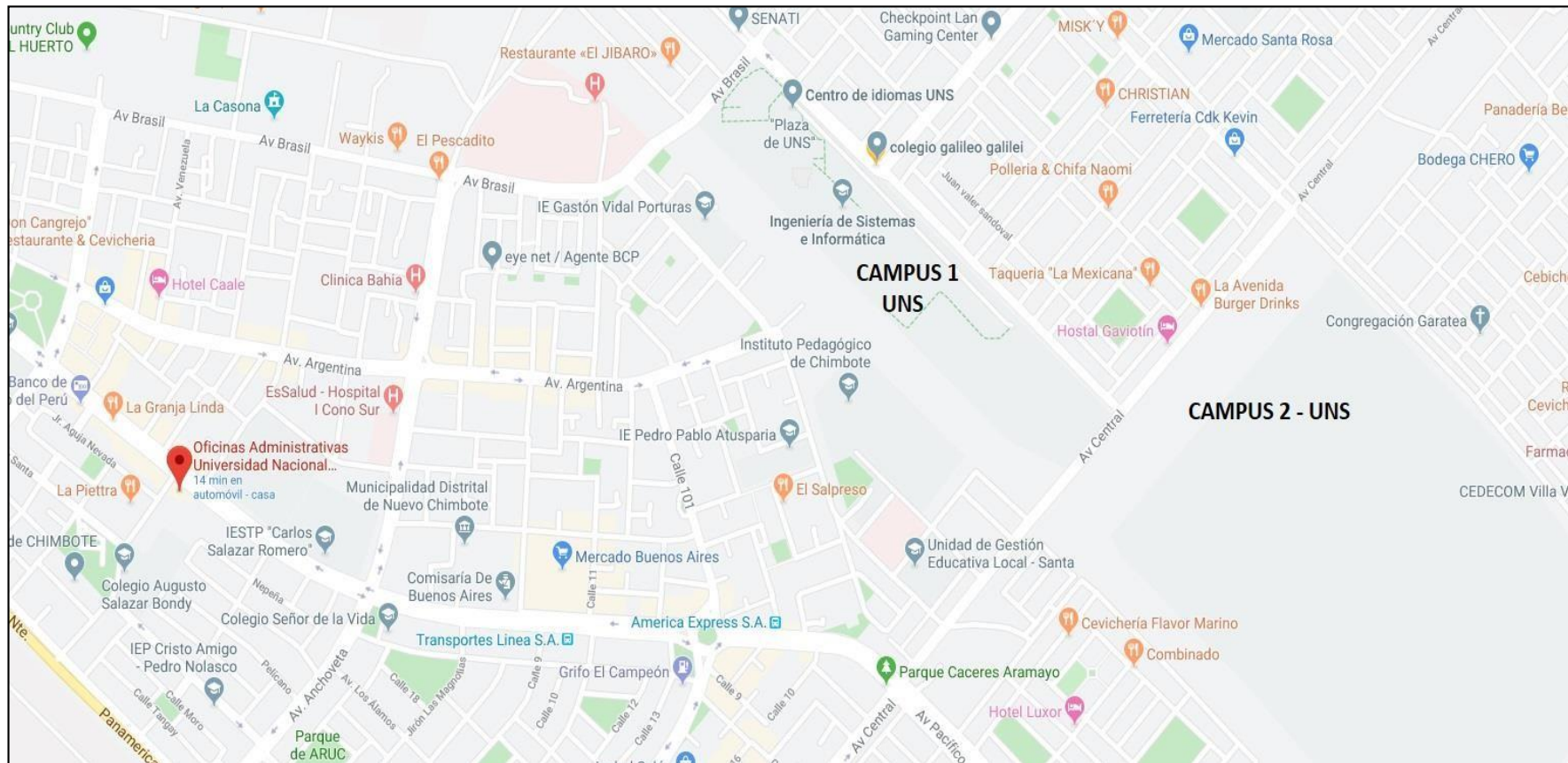


Figura 22. Ubicación de la UNS en Nuevo Chimbote

Fuente: Google Map

B) Red Informática

La Red Informática con cuenta la UNS está distribuida por los diferentes edificios del campus universitario, donde se encuentra el CORE principal (Edificio de CECOMP), y desde allí se distribuye a todo el campus universitario con enlaces de fibra óptica subterráneo.

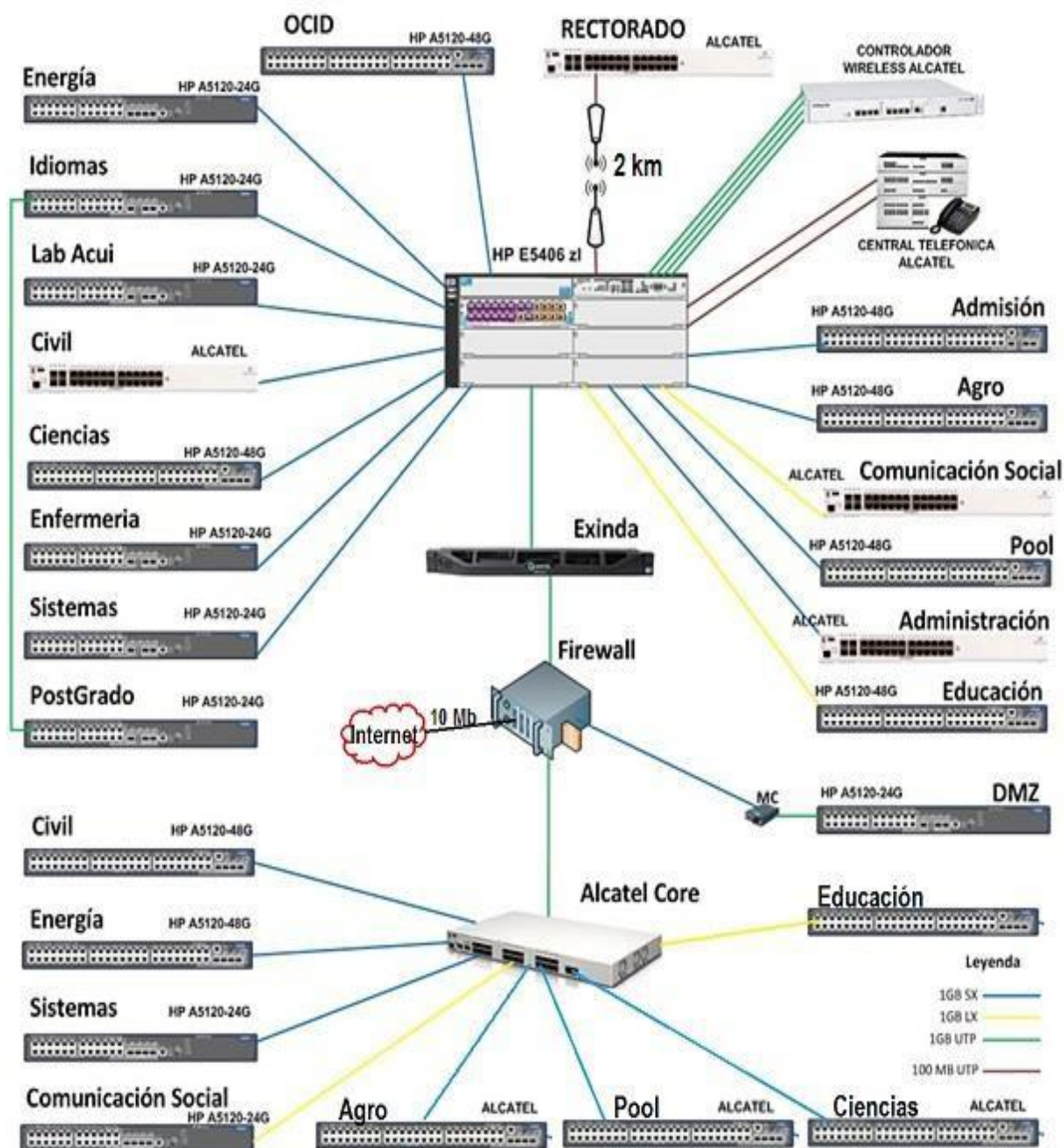
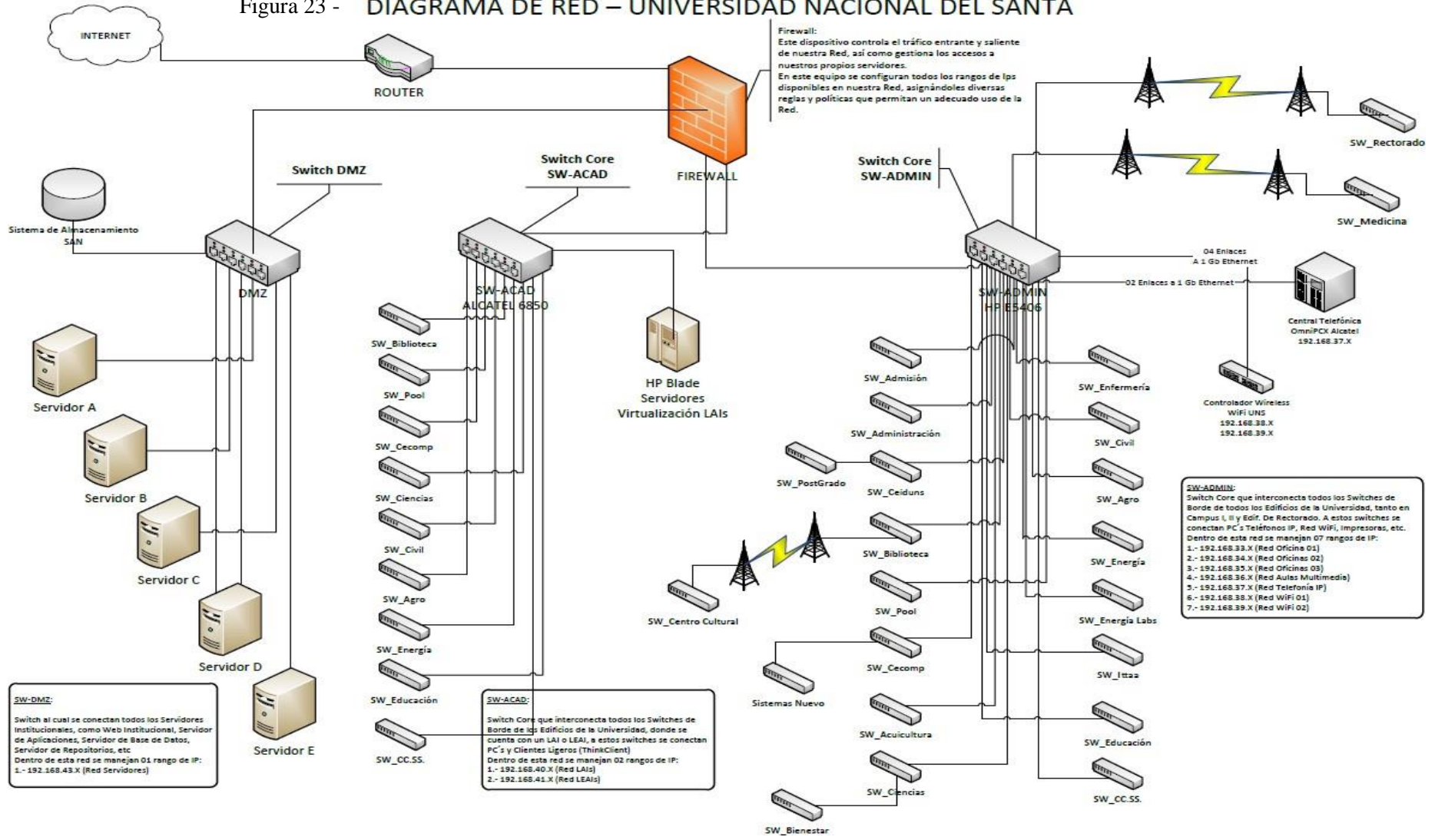


Figura 23. Arquitectura de Red Informática UNS

Fuente: OTIC UNS

Figura 23 - DIAGRAMA DE RED – UNIVERSIDAD NACIONAL DEL SANTA



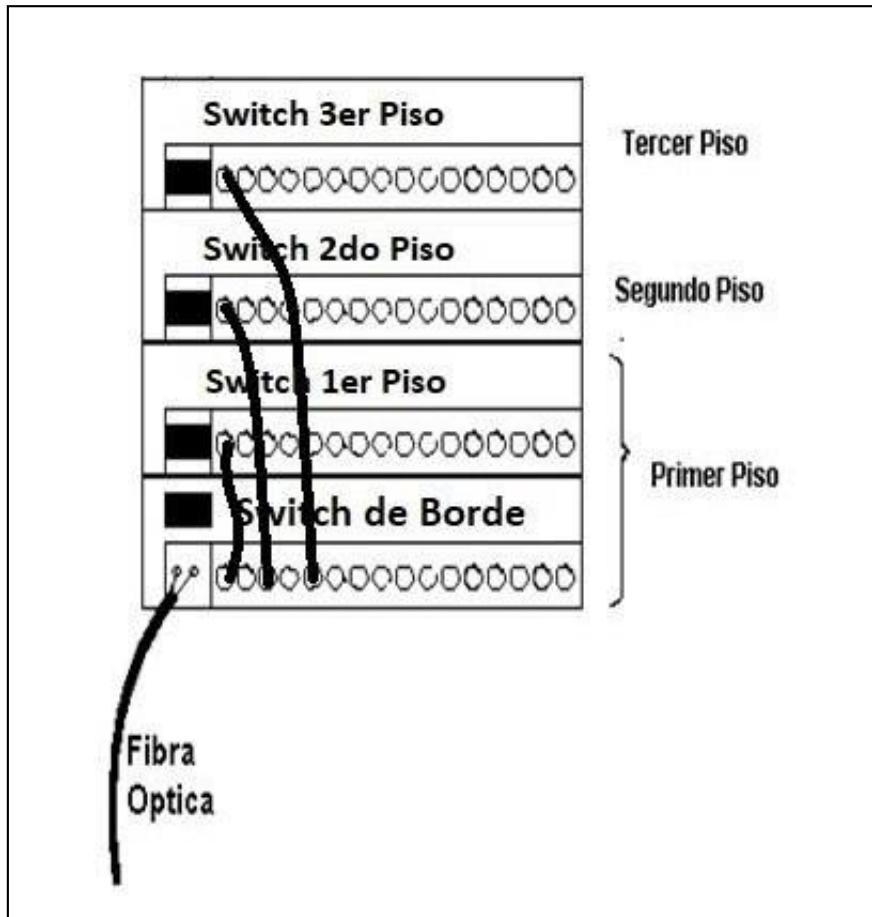


Figura 25. Diseño Lógico de Distribución de Equipos en Edificios

Fuente: Diseño Propio

La Fibra Óptica Multimodo viajara en forma subterránea a 60 cm de profundidad, por la vía principal, dentro de tubos para mejorar la protección.



Figura 26. Fibra Óptica viaja subterránea por la Avenida Principal del Campus Universitario

Fuente: Álbum Fotos de la UNS

C) Hardware de Red

- La troncal de la UNS es de fibra óptica, formando una topología en estrella, teniendo el punto central el edificio de CECOMP. Cable es fibra óptica multimodo, pero para el enlace hacia el edificio de educación el cable es fibra óptica monomodo por superar los 500 mts.
- El medio de comunicación utilizado dentro de los edificios, en el cableado vertical y horizontal, es UTP cat. 6, que puede permitir velocidades de hasta 1 Gbps.
- Hay un Radio enlace desde el Campus 1 hasta el edificio de Rectorado.

- Equipo de comunicación: se cuenta con switches, routers, antenas wifi y antenas de radioenlace.
- 01 Switch Core principal con conectores de fibra óptica, ubicado en el edificio de CECOMP, desde donde se distribuye el cableado de fibra óptica hacia todo el campus universitario.

D) Software de Red

- Sistema operativo de redes: Linux Red Hat para los Servidores y Windows Server 2012.
- Software de sistemas operativos cliente: , Windows 7 y Windows 10.
- Software de servidor web: Apache en Linux Red Hat.
- Software de servidor e-mail: Ahora usa Office 365 en Microsoft
- Software visualizadores: internet explorer, Firefox y Chrome.
- Software adicional: Power Builder, ASE, Java, Antivirus

E) Sistemas de Información Académico y Administrativo

En la UNS existen diferentes sistemas de información, tanto del área académica como administrativa, cada uno transfiriendo diferentes tipos de datos.

En el área académica tenemos los sistemas de información de registro académico, de admisión, de Bienestar universitario, de Seguimiento al Egresado, de los Centros de Producción, etc.

En el área administrativa tenemos los sistemas de información del SIIGA, del SIAF, así como algunos módulos de inventario y pagos.

F) Servicios que se Proveen

- **CORREO ELECTRONICO.** - Se da servicio de correo electrónico a todos los estudiantes, docentes y personal administrativo; todos en el dominio uns.edu.pe.
- **ACCESO A INTERNET.** - La Universidad cuenta con una red de 100 Mbps de acceso a Internet, el cual provee a todos los usuarios a través de la troncal de fibra óptica y las redes wifi distribuidas en todo el campus.
- **TUTORIA INTELIGENTE.** - Existe un servicio de MOODLE, plataforma a través del cual los docentes pueden dar reforzamiento académico a los estudiantes, a través de tutoría y carga de trabajos para su revisión online.
- **SISTEMAS DE INFORMACION.** – Se accede a diversos sistemas de información a través de las redes informáticas, ya sea desde las oficinas de la universidad o desde los dispositivos de estudiantes y docentes.



Figura 27. Servicio de Videoconferencia Local

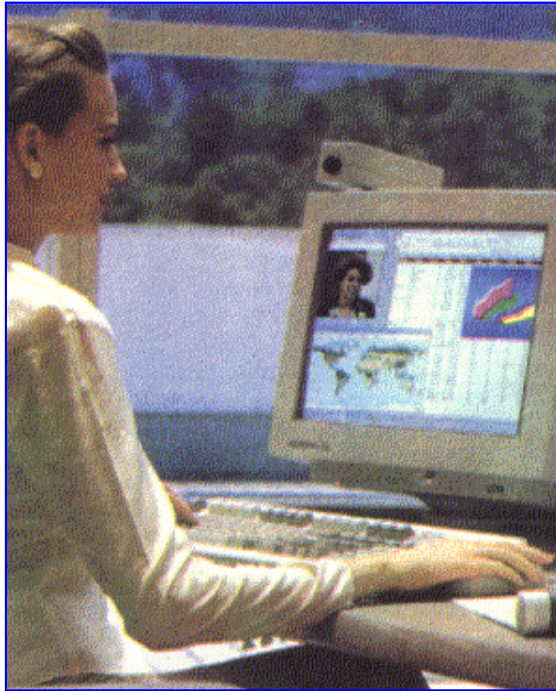


Figura 27. Servicio de Videoconferencia Internacional



Figura 28. Servicio de Trabajo en Grupo

5.3. EVALUACIÓN DE LA SEGURIDAD EN LA RED INFORMÁTICA DE LA UNS

Como se puede apreciar de la información obtenida en la UNS, la red informática se encuentra distribuida por 2 instalaciones: el campus universitario y el edificio de rectorado. Para esto utiliza dispositivos de comunicación alámbricos e inalámbricos (Switch, Routers, Antenas Wifi, etc.).

Como soporte de seguridad contaba con un servidor Firewall basado en IPTABLES, Es un firewall basado en reglas, su funcionamiento se basa en aplicar reglas que el mismo firewall ejecute.

Actualmente cuenta con la Plataforma de Seguridad de Palo Alto, la cual está diseñada para prevenir las brechas y para facilitar al administrador información útil sobre las amenazas detectadas en todas las funciones de seguridad del sistema, Y no sólo eso, sino que tiene la capacidad de analizar malware sobre cualquier puerto, aplicación o protocolo gracias a una tecnología exclusiva de Palo Alto Networks.

Estas son algunas de las características que la Plataforma de Seguridad de Palo Alto posee para lograr sus objetivos:

- El Firewall posee un potente motor para la detección de aplicaciones de manera nativa, no importa sobre qué medio viaje.
- Puede analizar Malware sobre cualquier puerto, aplicación o protocolo.
- Permite analizar todo el tráfico por todos sus módulos de seguridad en un solo paso, mejora así el desempeño y velocidad de análisis.
- Ofrece gran cantidad de información para un mejor análisis.
- Cubre los siguientes módulos de protección: Antivirus, AntiSpyware, IPS, Denial of Service, Filtrado Web, Data Loss Prevention y Filtrado de contenido.

- Cuenta con 2 secciones de hardware, la primera se enfoca en la administración del sistema y la segunda en la inspección y procesamiento del tráfico.
- Da visibilidad y control de políticas detalladas de aplicaciones.
- Reporteo nativo e integrado.
- Hace uso de la nube de inteligencia de WildFire con la que protege contra amenazas de avanzadas y de Zero Day.
- Brinda protección para aplicaciones SaaS en la nube como Office 365, Salesforce, etc. con Aperture con el fin de prevenir fuga de información, clasificación de datos, y detección de amenazas.
- Brinda la certeza de que todos los equipos están seguros, sin importar que se encuentren en un entorno vulnerable gracias a la protección avanzada de Endpoint que ofrece.

Para mejorar el acceso a internet contaba con un servidor proxy llamado SQUID, el cual permite mejorar el rendimiento de las conexiones de empresas y particulares a Internet guardando en caché peticiones recurrentes a servidores web y DNS, acelerar el acceso a un servidor web determinado o añadir seguridad realizando filtrados de tráfico. Actualmente el servicio Proxy viene incluido en la Plataforma de Seguridad Palo Alto.

En cuanto a seguridad antivirus, cuenta con SOPHOS Endpoint Protection, el cual bloquea programas maliciosos e infecciones al identificar e impedir las técnicas y comportamientos utilizados en casi todas las vulnerabilidades.

SOPHOS Antivirus Endpoint Protection: Tecnología innovadora en seguridad informática

SOPHOS Endpoint Protection no depende de firmas para detectar malware, lo que significa que identifica amenazas de día cero sin afectar negativamente al rendimiento de su dispositivo.

Sophos Antivirus trabaja sobre los dispositivos y junto con el firewall para detectar y aislar dispositivos que corren peligro. La seguridad sincronizada ofrece contexto adicional al aportar información procedente de la red.

Características de Sophos Endpoint Protection:

- Análisis de comportamientos. Determina comportamientos sospechosos, lo que permite la detección de malware especialmente diseñado para esquivar las soluciones tradicionales.
- Tráfico malicioso. Prefiltra todo el tráfico HTTP/HTTPS en las redes y hace un seguimiento del tráfico sospechoso, así como de la ruta del archivo del proceso que está enviando tráfico malicioso.
- Red y estación de trabajo integradas. La comunicación instantánea y automática entre los dispositivos en las redes advierte al sistema de control de Sophos de lo que está detectando el firewall exactamente, lo que permite que el agente de protección de la estación utilice esa información inmediatamente para descubrir el proceso detrás de la amenaza.
- Antivirus para Android, iOS, PC y Mac: Escoje si quieres usar tu licencia Sophos para el ordenador, smartphone o tablet.
- Sophos Software ofrece una funcionalidad sofisticada junto con una experiencia de usuario sencilla e intuitiva.
- Implantación rápida y sencilla desde la web o nube o de forma local.
- Políticas predeterminadas que se configuran para equilibrar la protección, usabilidad y rendimiento.

- Eliminación automática de productos de seguridad para estaciones de terceros.
- Configuración sencilla de funciones avanzadas tales como HIPS y control de dispositivos, gracias a los datos continuamente actualizados de Sophos Labs.

Actualmente no existe un Equipo de Seguridad, porque será necesario conformarlo, determinando las capacidades que deberán tener en el equipo. Una agenda donde se establezca sus tiempos y actividades a realizar para asegurar la información que se transfiere a través de la red informática.

Las Capacidades Esenciales que deberá tener el equipo de seguridad son las siguientes:

- Es una tarea extremadamente complicada si solo se ven algunas brechas.
- Tener determinados los activos que se deben proteger
- Ubicar los activos que son vulnerables a los ataques
- De qué forma están siendo atacados mis activos
- Como se si ha tenido lugar una brecha de seguridad
- Que acciones tendrán un impacto mayor sobre la actitud del equipo de seguridad

5.4. ANÁLISIS Y DISEÑO DE LA PROPUESTA DEL CENTRO DE OPERACIONES DE SEGURIDAD

El Establecimiento de un Centro de Operaciones de Seguridad es un paso necesario para que una organización sea capaz de detectar y contener con eficacia una brecha de seguridad, para cual se debe evaluar la siguiente pregunta: ¿Cómo

puede mi organización lograr este objetivo con la mayor eficacia?, se responde esto de manera crítica con las capacidades de la organización.

ACTIVOS A PROTEGER

1. Que sistemas son críticos para que su empresa siga funcionando

La Universidad Nacional del Santa cuenta con diferentes Sistemas de Información, tanto para el área académica como el área administrativa. Tenemos el Sistema de Registro Académico, el Sistema de Seguimiento al Egresado, El Sistema, El Sistema Socioeconómico, el Sistema de Evaluación del Docente, etc. Todos los sistemas corren en servidores de la Oficina de Tecnologías de Información y Comunicación, en plataforma Java y Power Builder, y tienen acceso todos los docentes y estudiantes desde la red interna como desde el exterior a la red.

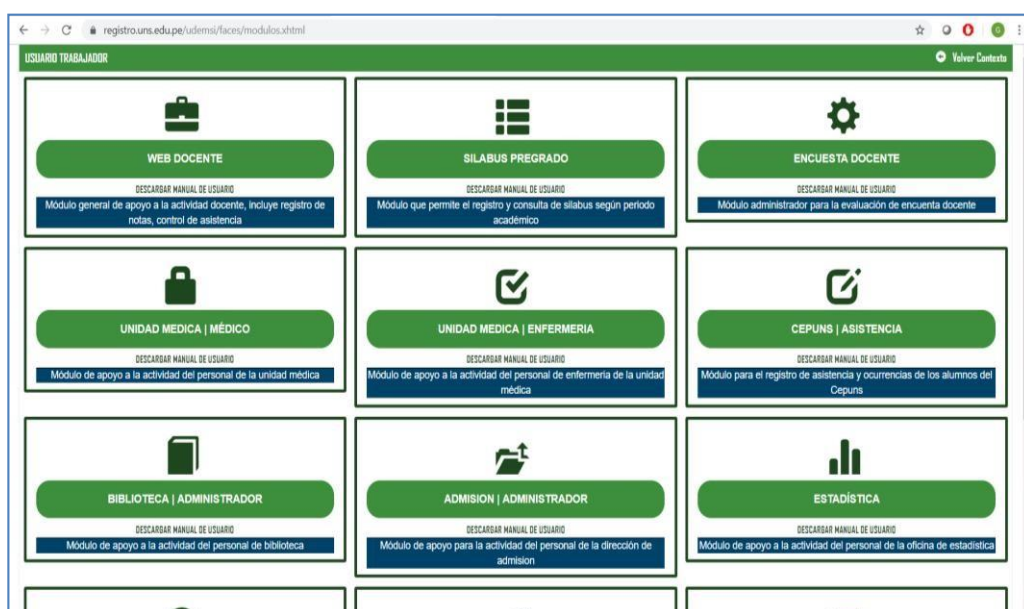


Figura 29. Módulos de Sistemas de Información de la UNS

Fuente: <https://registro.uns.edu.pe/udemsi/faces/modulos.xhtml>

Asimismo, la universidad cuenta con un servidor web, a través del cual publica en la intranet e internet, de todo lo acontecido en la universidad, en el área académica y administrativa, así como los eventos a realizar, las resoluciones expedidas, los reglamentos, etc.



Figura 30. Pagina Web de la Universidad Nacional del Santa

Fuente: <https://www.uns.edu.pe/#/principal>

Existen otros activos como los Servidores de Base de Datos, El Servicio de VoIP Alcatel, los Switches Core y de Borde que permiten interconectar todo el campus, los Servidores SIIGA, el Servidor SIAF, etc.

Todos estos activos manejan información importante de la Universidad, y ante alguna brecha no se tendría acceso a la información y afectaría algún servicio.

2. Que sistemas son críticos para las tareas diarias

El Sistema Académico es el sistema crítico de la UNS en el aspecto académico, allí es donde se van ingresando las asistencias de los estudiantes, así como las notas por evaluaciones y trabajos que van realizando. Se obtiene al final el Acta

de Notas, para determinar su avance en su plan de estudios y su egreso de la universidad.

En el aspecto administrativo, el SIAF es el sistema crítico, pues allí se ve el presupuesto, los fondos para pagar, las compras, etc. Sin este sistema, la universidad se paraliza y no podría hacer ningún trámite administrativo económico.

3. De que otros sistemas dependen dichos sistemas críticos

En la UNS se tienen los sistemas de Cargas Horarias, de Registro de Docentes, de Admisión, de Bienestar Universitario, de Biblioteca; todos los sistemas que ayudan o proveen de datos al sistema principal de registro académico.

El sistema firewall y de antivirus es necesario, para proteger los equipos que se encuentran en la red informática de la UNS.

4. Que sistemas gestionan y almacenan información sensible

Todos los sistemas que se utilizan en la UNS, gestionan y almacenan información sensible de los estudiantes y de la institución.

Todos estos activos que se encuentran en las bases de datos de la UNS y accedido a través de los sistemas de información, son necesarios protegerlos, ya que una alteración, daño o pérdida, ocasionaría problemas tanto internamente como externamente. Algunos datos son íntimos o reservados, que se debe priorizar en su cuidado.

DESCUBRIMIENTO DE ACTIVOS

Monitorización pasiva de Red

Escaneo Activo de la Red

Inventario basado host

GESTION DE VULNERABILIDADES

Escaneo activo de la Red

Análisis en Host

DETECCION DE AMENAZAS

Detección de Intrusos (IDS)

Detección Basada en Host

Detección de Intrusiones Inalámbricas

MONITOREO DE COMPORTAMIENTOS

Monitoreo Activo de Servicios

Análisis de Flujo de Red

Captura de Paquetes

Detección de Intrusos

QUE ACCIONES VAN A TENER UN IMPACTO MAYOR SOBRE LA SEGURIDAD

Que hago primero

Que datos debería analizar

Debería detener un ataque recientemente observado, o intentar y contener una brecha de seguridad recientemente descubierta

Enfoque que permite automatizar la comprensión de los datos:

SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)

5.5. IMPLEMENTACIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD

Para la implementación del Centro de Operaciones de Seguridad se utiliza el software Alien Vault Ossim, que es gratuito, a fin de configurar el Centro de Operaciones desde donde administrar todos los activos de la institución y tener información de alerta de los riesgos, vulnerabilidades y amenazas.

Primero se instala el software Alien Vault Ossim, donde sale un menú principal con 2 opciones, donde se instala la primera opción OSSIM.

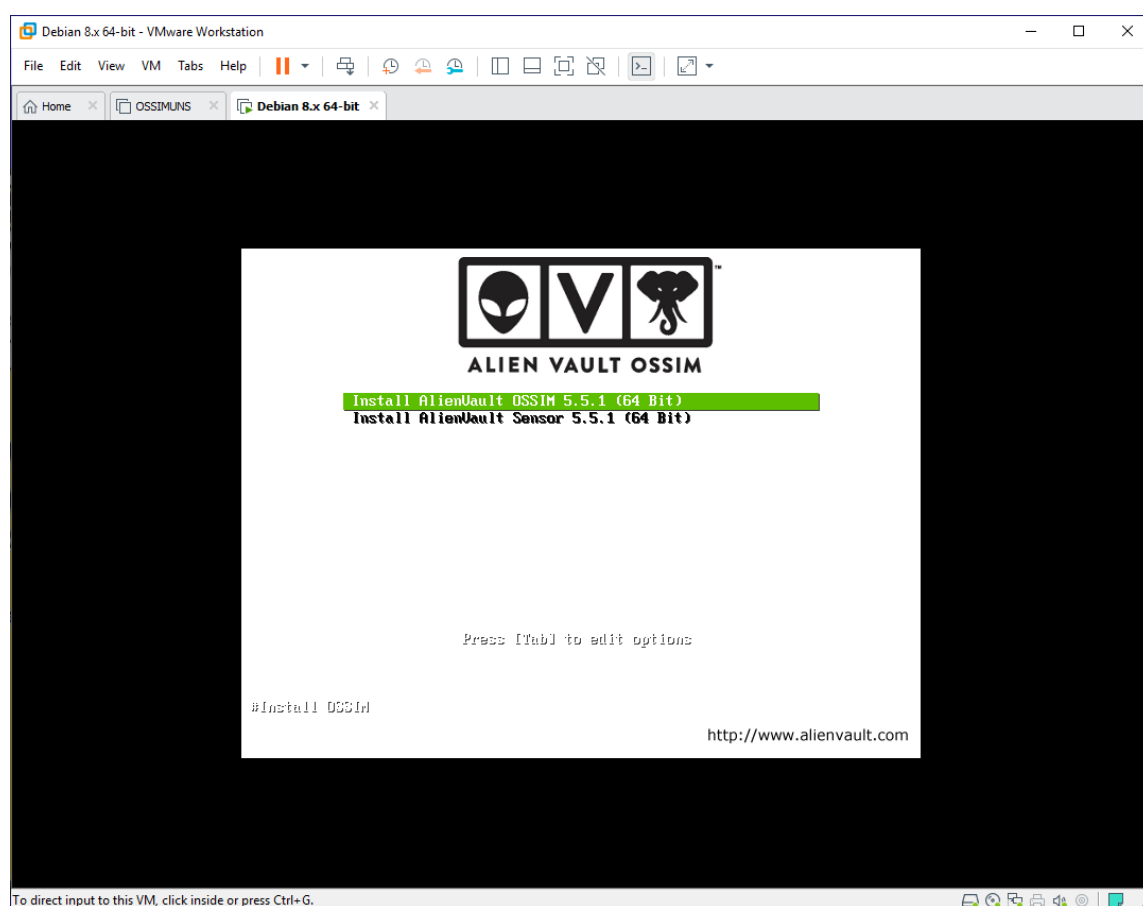


Figura 31. Seleccionando el Modo de Instalación de OSSIM

Fuente: Propia

Luego se avanza a la siguiente ventana, se debe seleccionar el idioma sobre el que va a trabajar el software, siendo para el presente caso el idioma español.

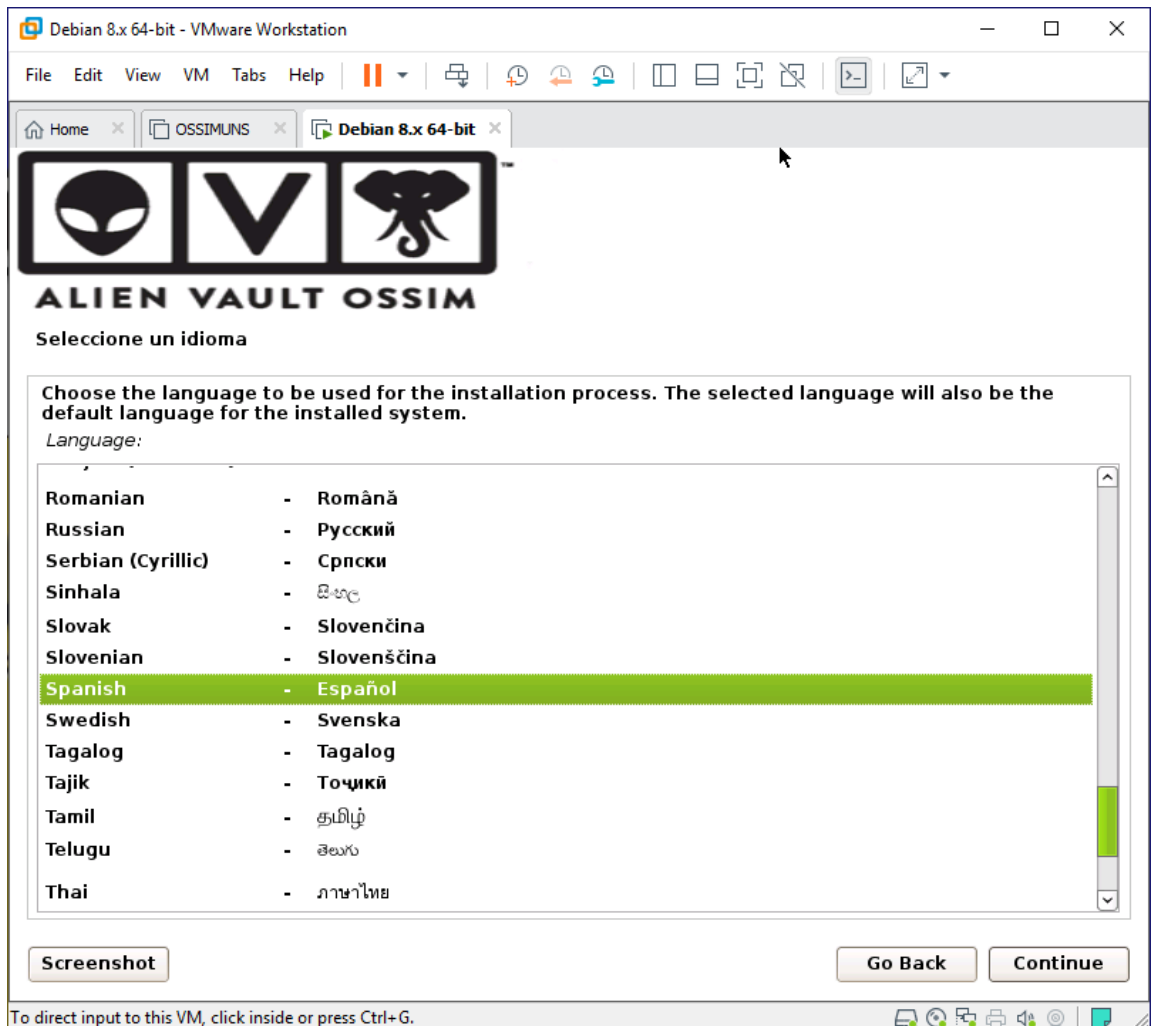


Figura 32. Seleccionando el Idioma de Instalación de OSSIM

Fuente: Propia

En seguida se debe seleccionar la ubicación del Centro de Operaciones de Seguridad administrado a través de OSSIM, se presentan varios países, y para el presente caso es Perú.

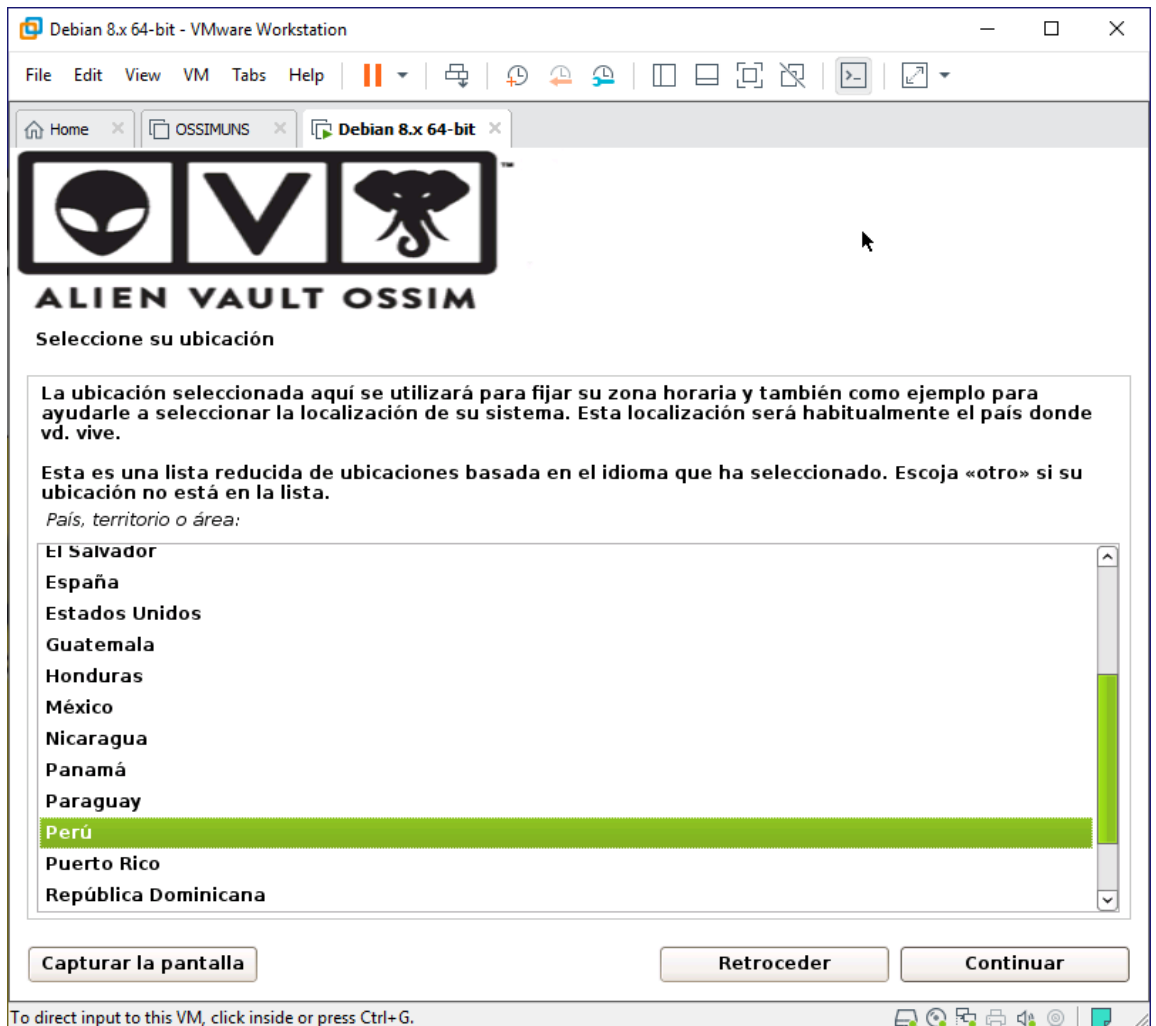


Figura 33. Seleccionando la Ubicación de OSSIM

Fuente: Propia

Se necesita luego configurar el teclado que se utilizara en OSSIM, a fin de tener la configuración adecuada de las teclas-

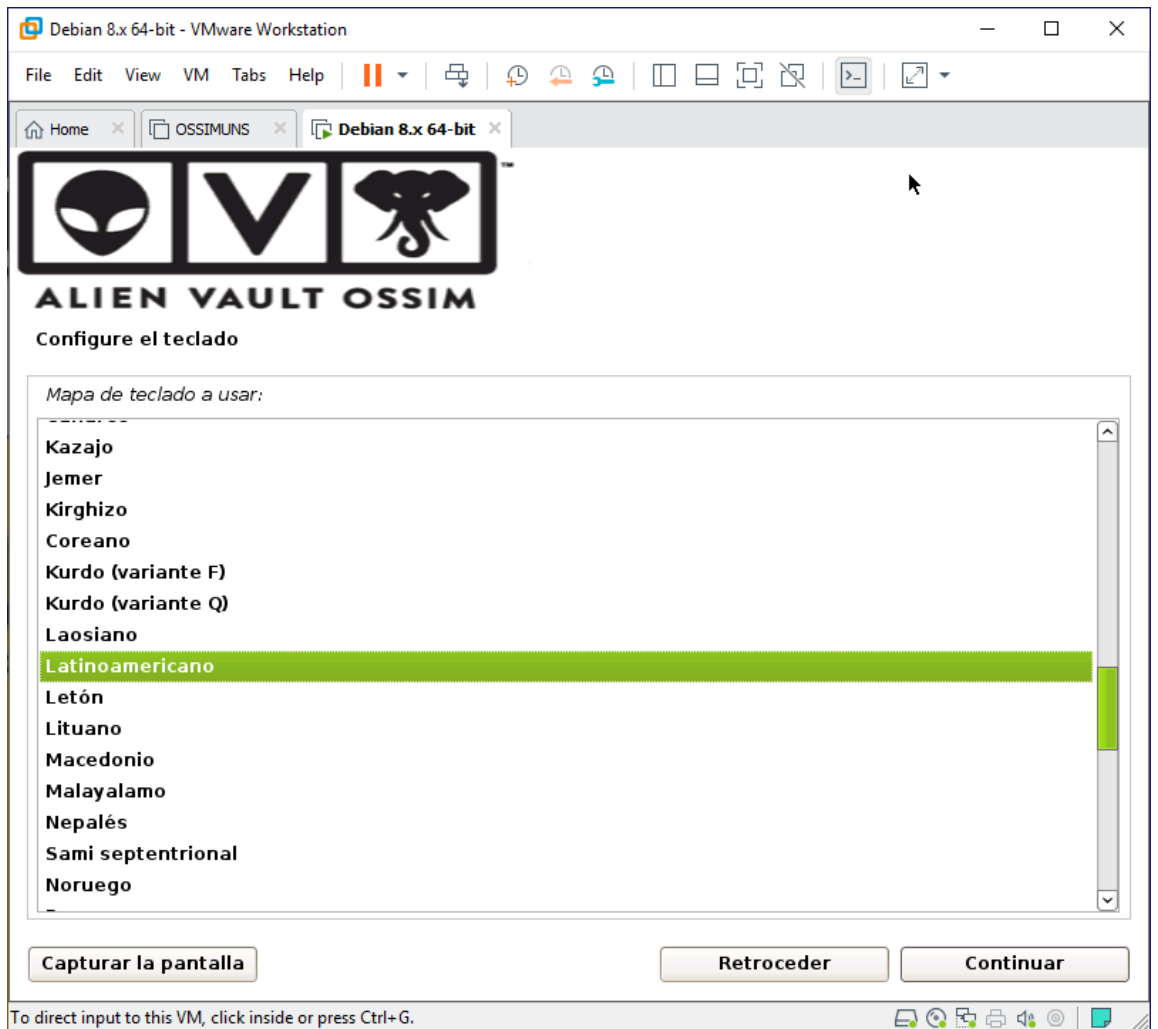


Figura 34. Configurando el Teclado para OSSIM

Fuente: Propia

Luego de seleccionar la configuración principal, se inicia la carga de los componentes necesarios para instalar OSSIM, todo esto puede llevar minutos de acuerdo a la versión. Tener en cuenta que OSSIM trabaja sobre una distribución de Linux Debian.

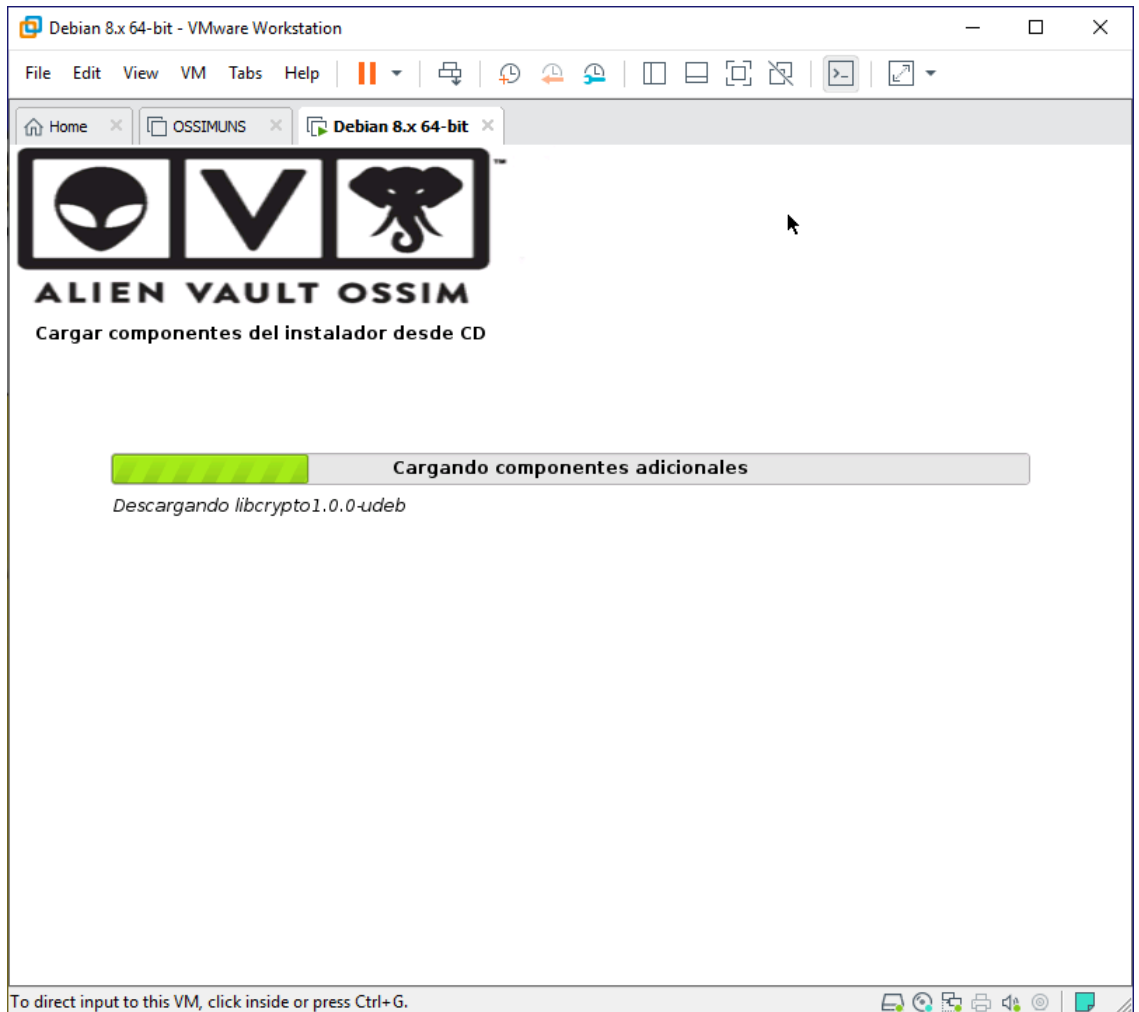


Figura 35. Se inicia la carga de los componentes de instalación OSSIM

Fuente: Propia

Se debe realizar la configuración de la red, debiendo colocar la dirección IP del COS, que será la dirección a través de la cual se va a administrar y monitorear la red informática de la Universidad Nacional del Santa.

La dirección IP a utilizar será 192.168.1.222.

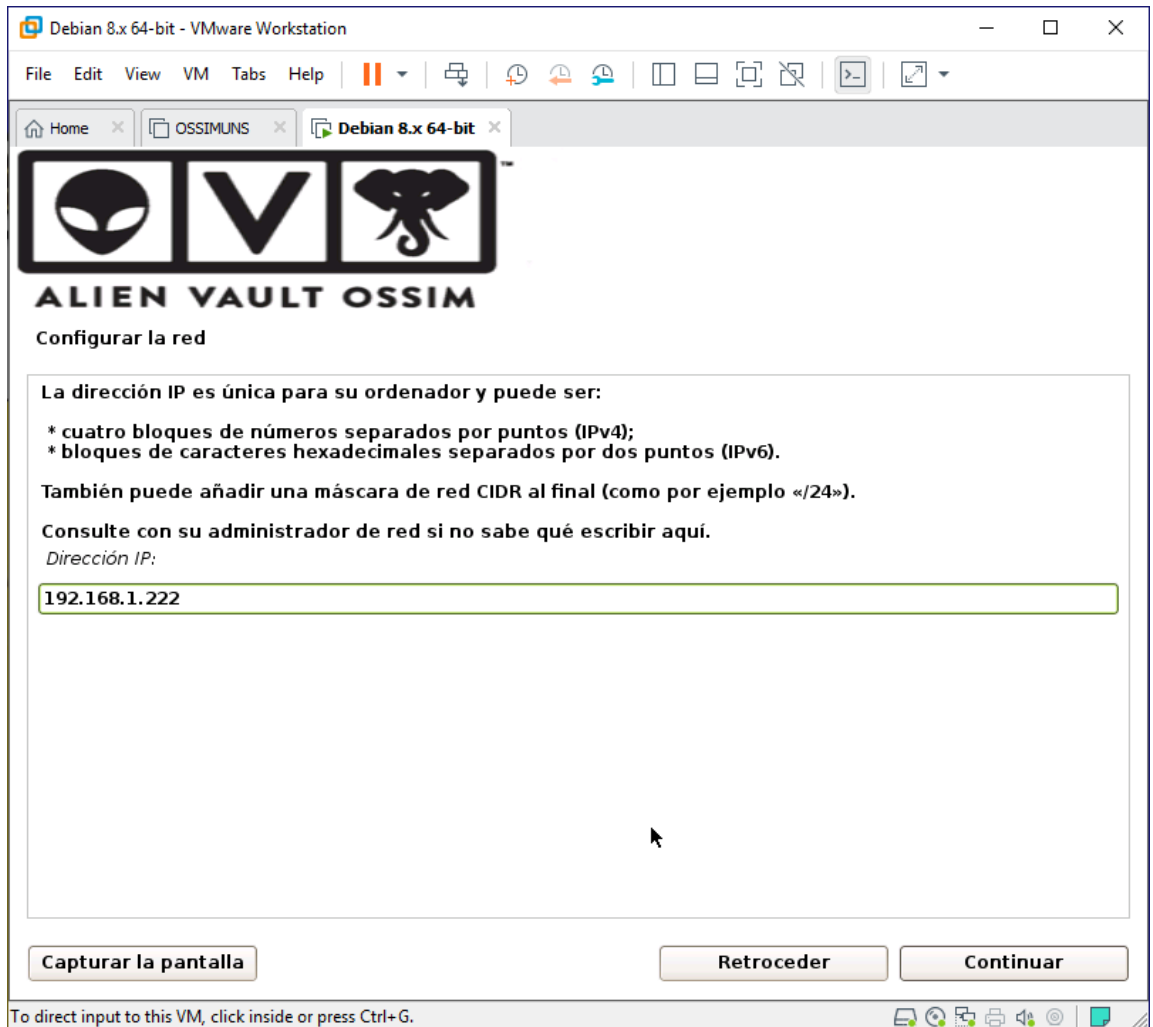


Figura 36. Configuración de la Dirección IP

Fuente: Propia

Se necesita configurar la mascara de red que corresponde a la direccion IP del servidor COS.

En este caso es la mascara 255.255.255.0

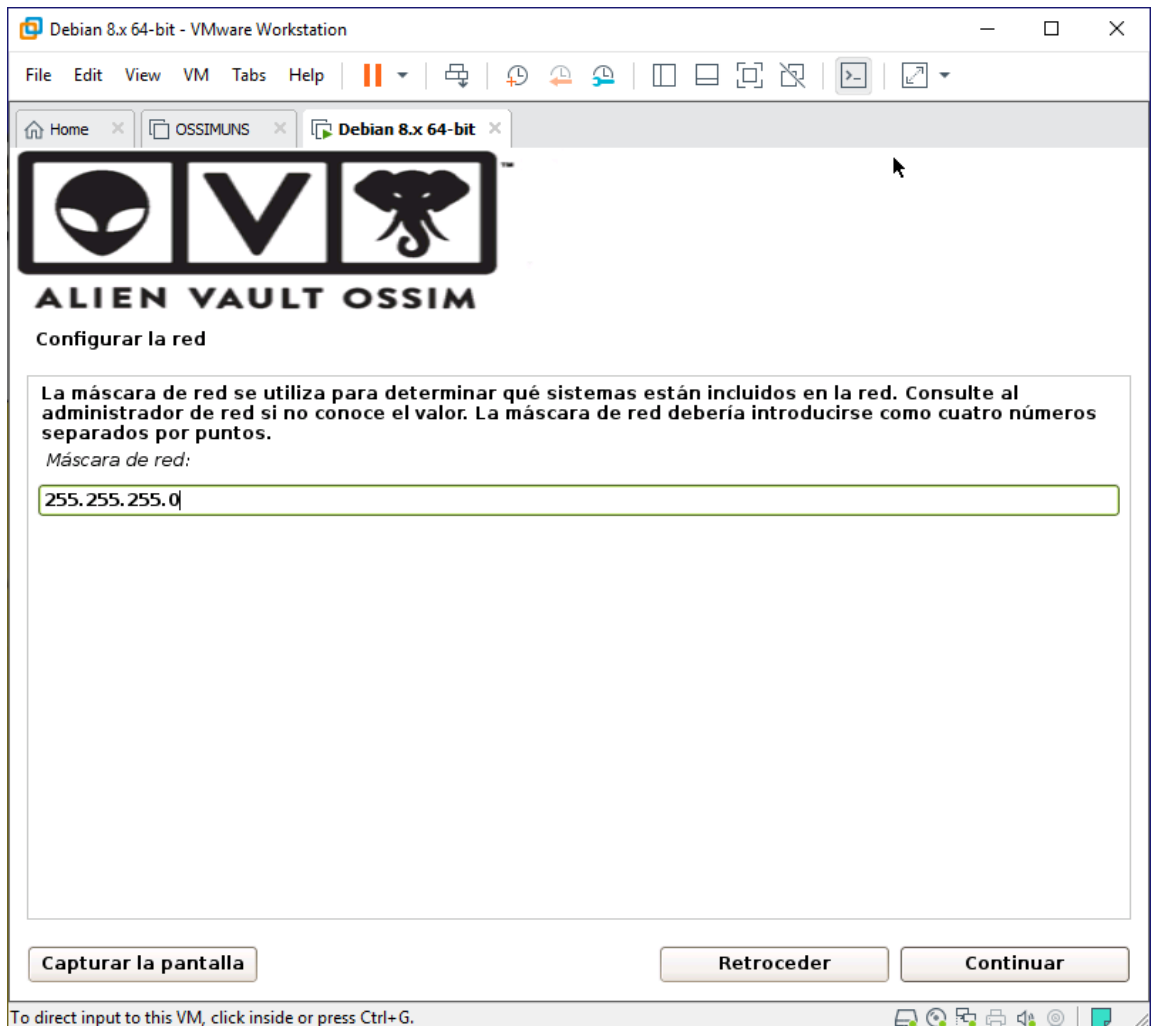


Figura 37. Configuración de la Máscara de la Dirección IP

Fuente: Propia

En seguida se necesita configurar la dirección IP del router o puerta de enlace, que permitirá al servidor COS conectarse con otras redes como Internet.

La dirección IP que se utilizara es 192.168.1.1.

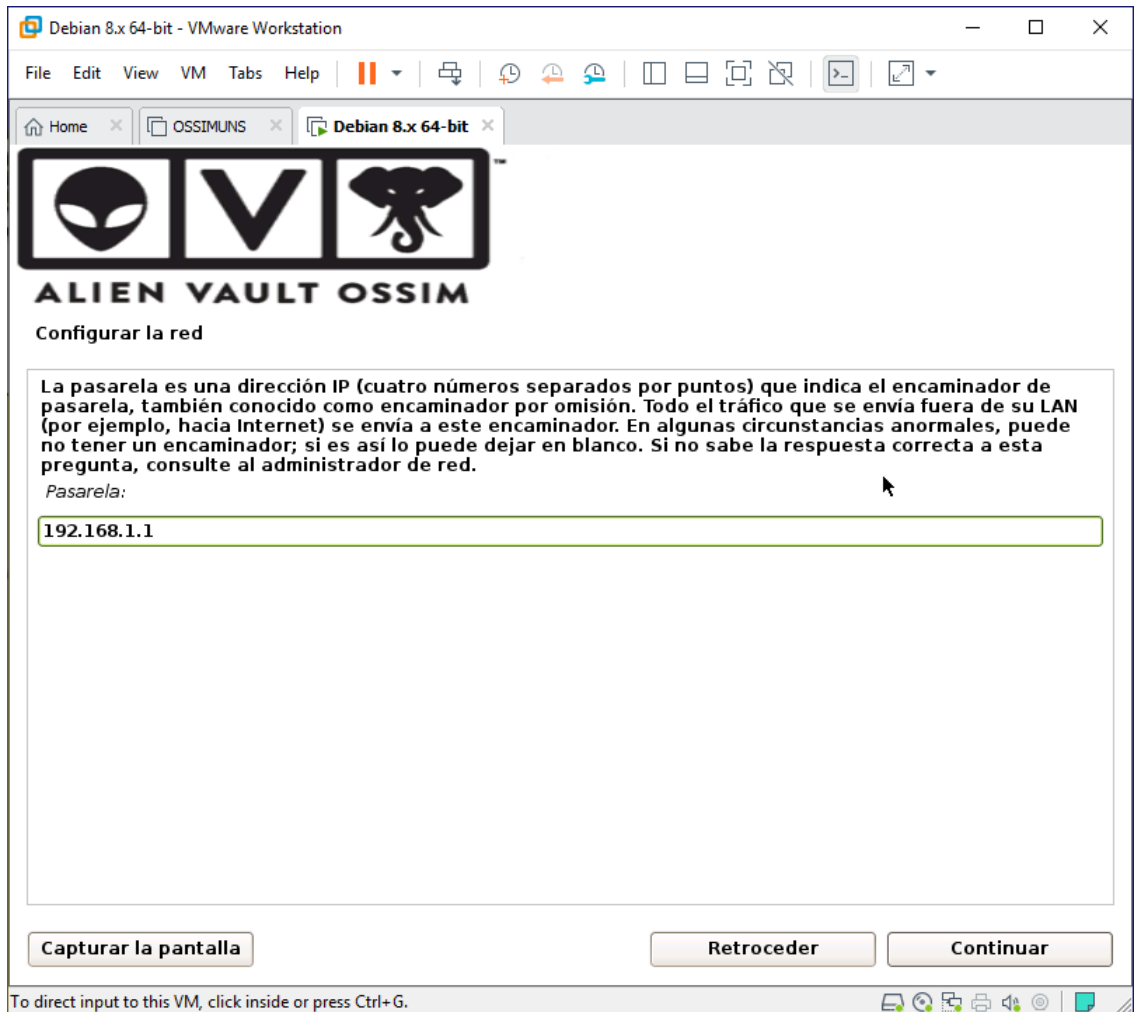


Figura 38. Configuración de la IP de la Puerta de Enlace

Fuente: Propia

Se debe configurar también la dirección IP del Servidor de Nombres, en este caso será la misma dirección IP de la puerta de enlace: 192.168.1.1.

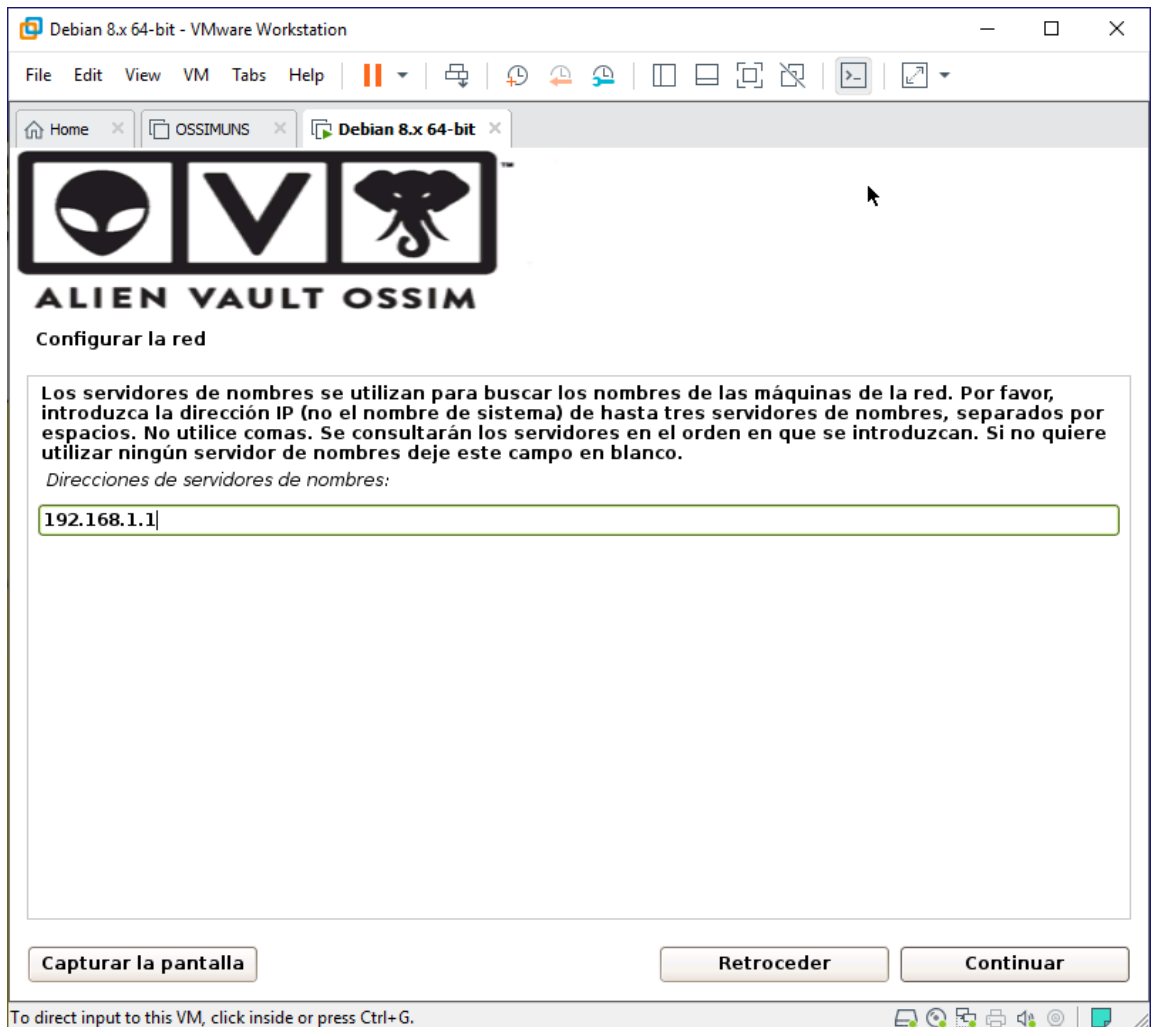


Figura 39. Configuración del Servidor de Nombres

Fuente: Propia

Luego de la configuración realizada, se inicia la instalación del sistema base de OSSIM.

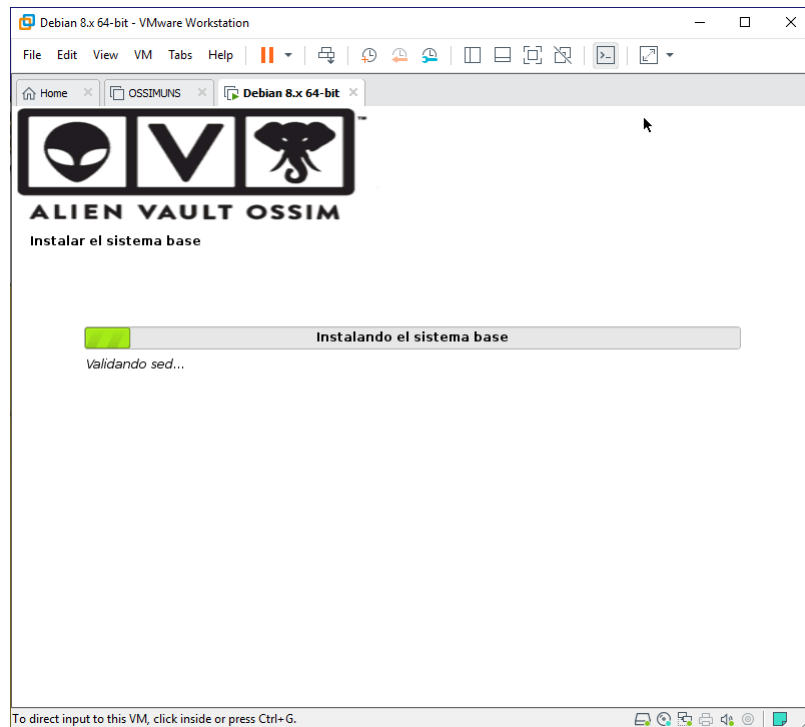


Figura 40. Inicio de Instalación del Sistema Base

Fuente: Propia

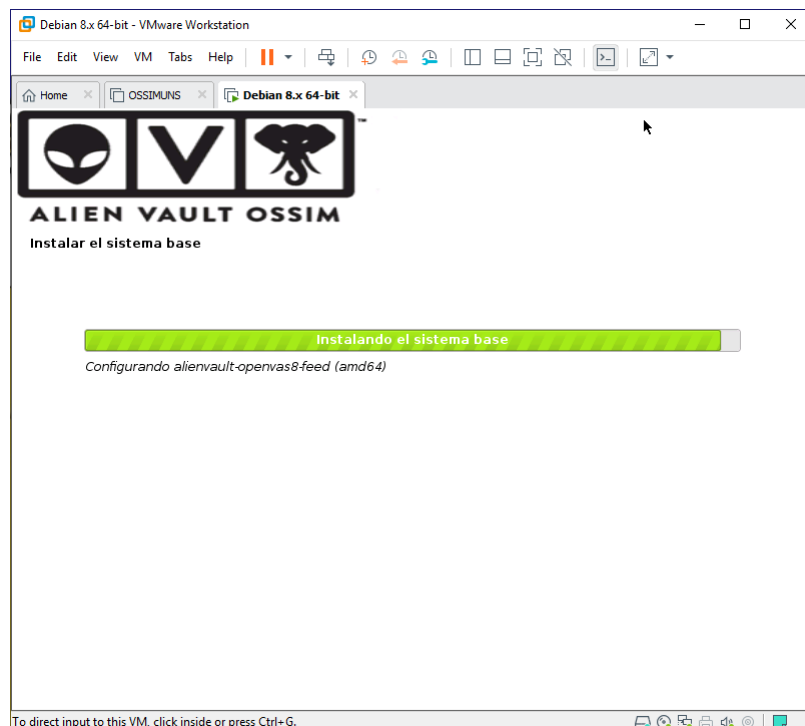


Figura 41. Avance de Instalación del Sistema Base

Fuente: Propia

Al final se instala el sistema OSSIM y se reinicia para iniciar su funcionamiento. Se utiliza el usuario: Jimmysanchez (admin) y el password: Uns2020

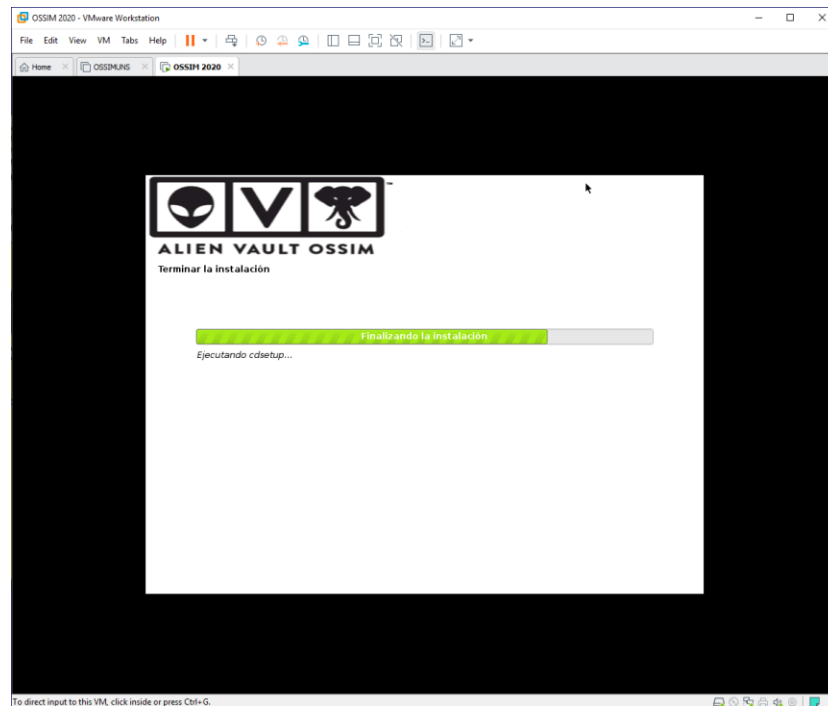


Figura 42. Culminación de Instalación de OSSIM

Fuente: Propia

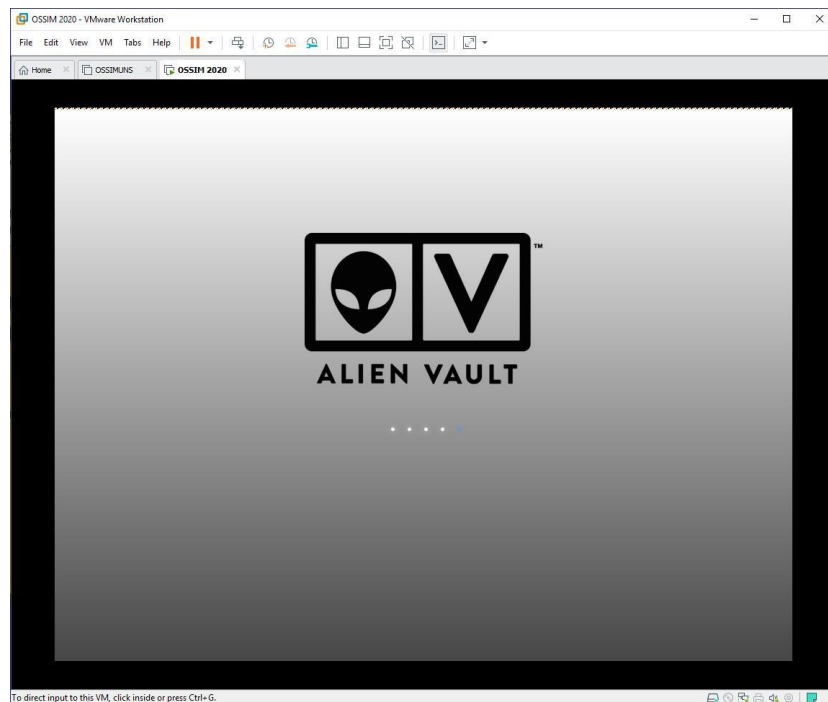


Figura 43. Inicio de OSSIM

Fuente: Propia

Una vez el Sistema OSSIM ya inicio, se puede ingresar a la herramienta, desde un browser a través de la dirección IP 192.168.1.222. Se debe ingresar el usuario y password.

En seguida se selecciona el tipo de monitoreo, eso es solo una vez al inicio.

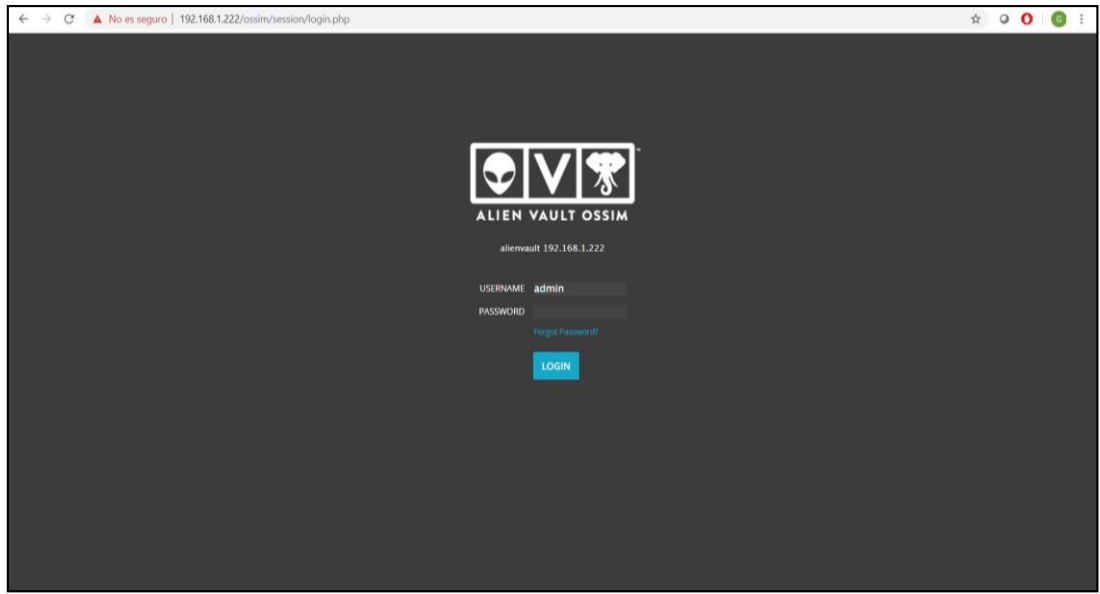


Figura 44. Loguear a OSSIM desde la web 192.168.1.222

Fuente: Propia

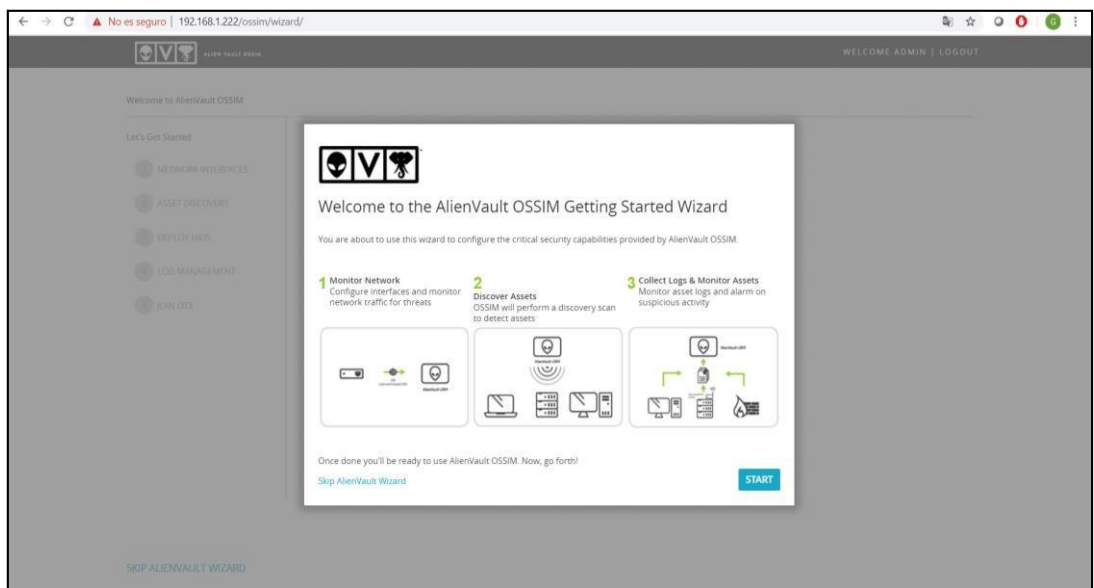


Figura 45. Configurando el tipo de monitoreo de OSSIM

Fuente: Propia

Una vez ingresado al Sistema OSSIM, se muestra la pantalla principal de gestión de la herramienta, a través de graficas estadísticas, que resaltan diferentes tipos de amenazas, riesgos y vulnerabilidades.

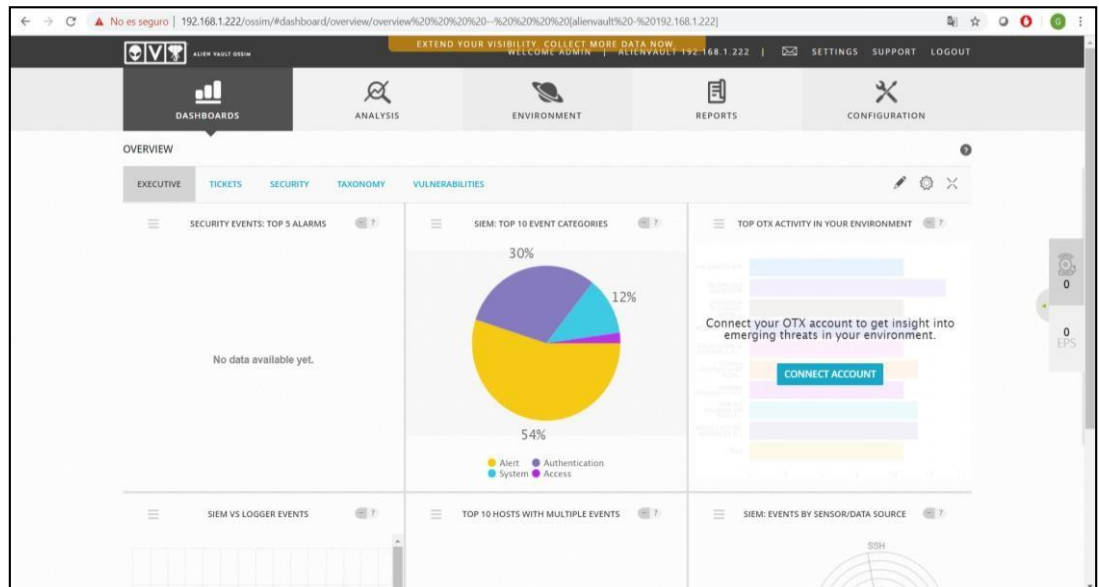


Figura 46. Pantalla Principal Superior de OSSIM

Fuente: Propia

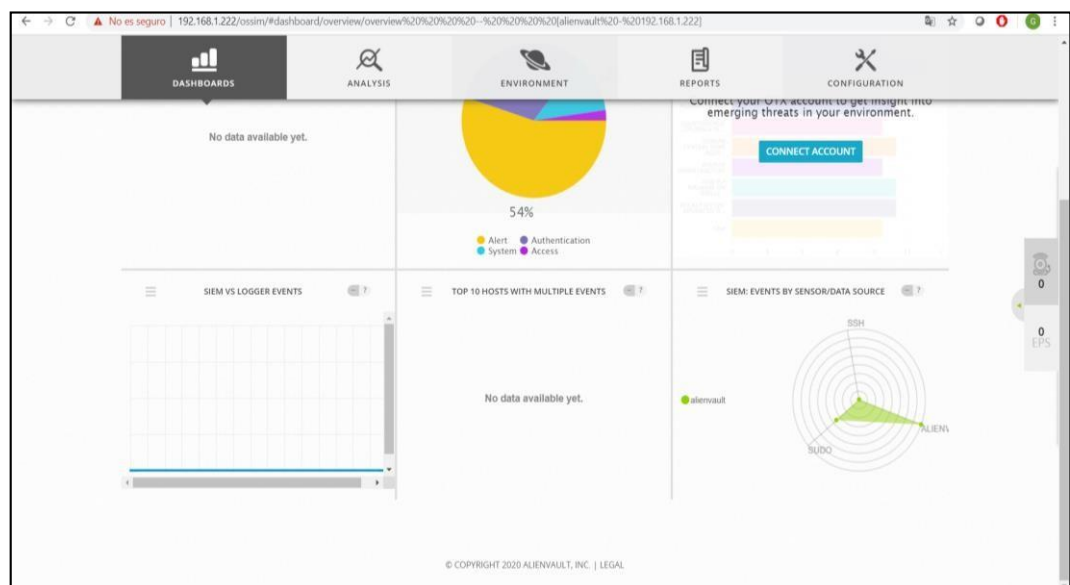


Figura 47. Pantalla Principal Inferior de OSSIM

Fuente: Propia

También se puede ingresar a OSSIM a través de otra computadora, en este caso a través de una máquina virtual Linux Centos 5.0, para lo cual abrimos un terminal y nos conectamos a través de SSH a la dirección 192.168.1.222 que es el servidor OSSIM, donde abrirá su Menú Principal.

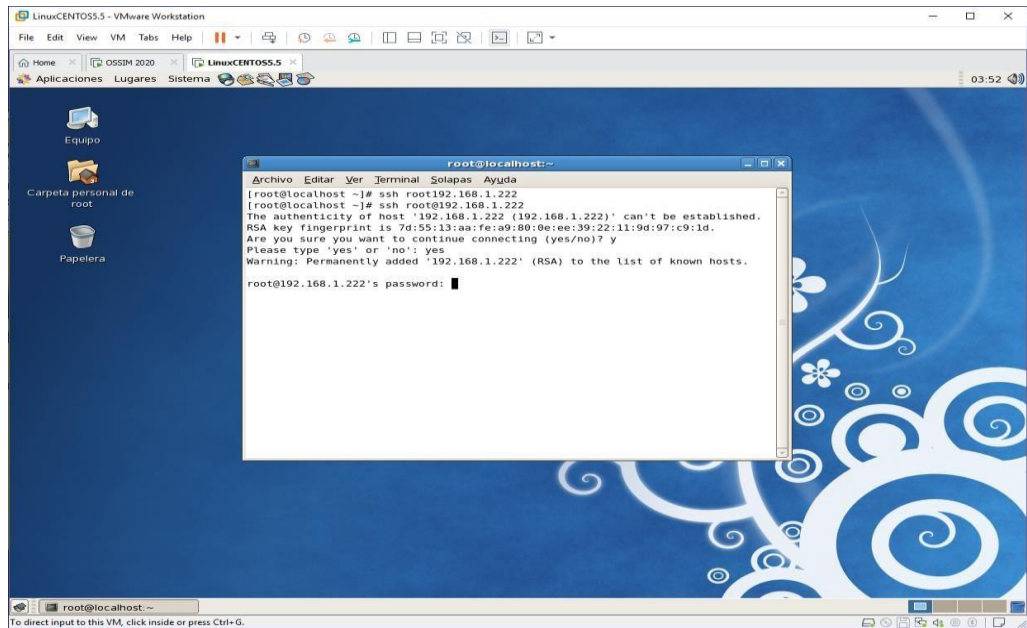


Figura 48. Acceso a OSSIM desde Máquina virtual Linux Centos

Fuente: Propia

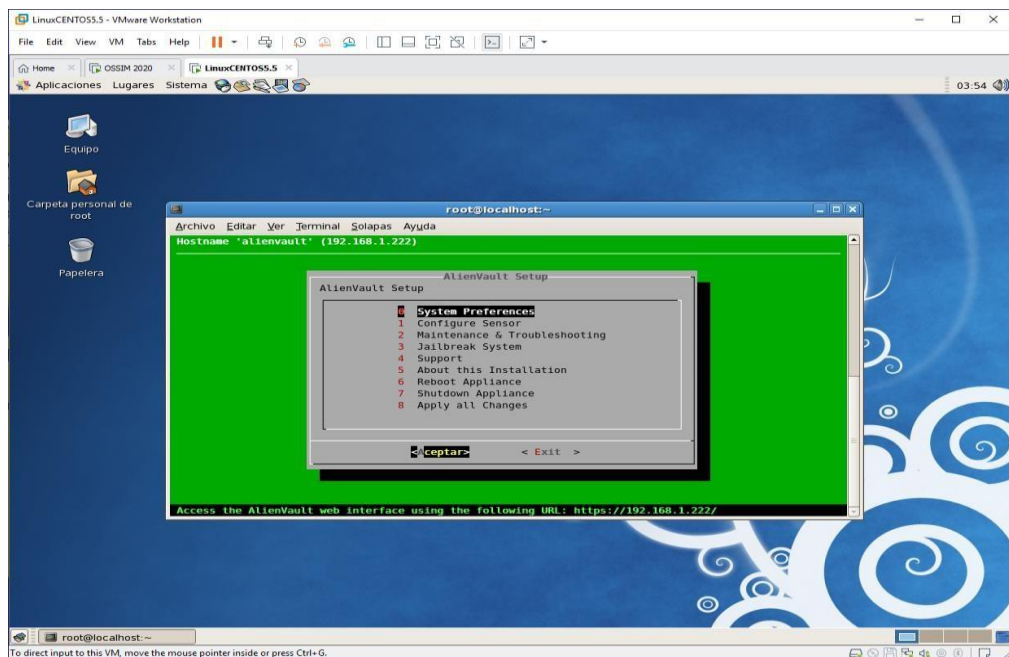


Figura 49. Menú Principal de Configuración de OSSIM

Fuente: Propia

Se tiene el submenú PREFERENCIAS DEL SISTEMA y CONFIGURE SENSOR, donde se puede configurar el servidor en sus opciones principales.

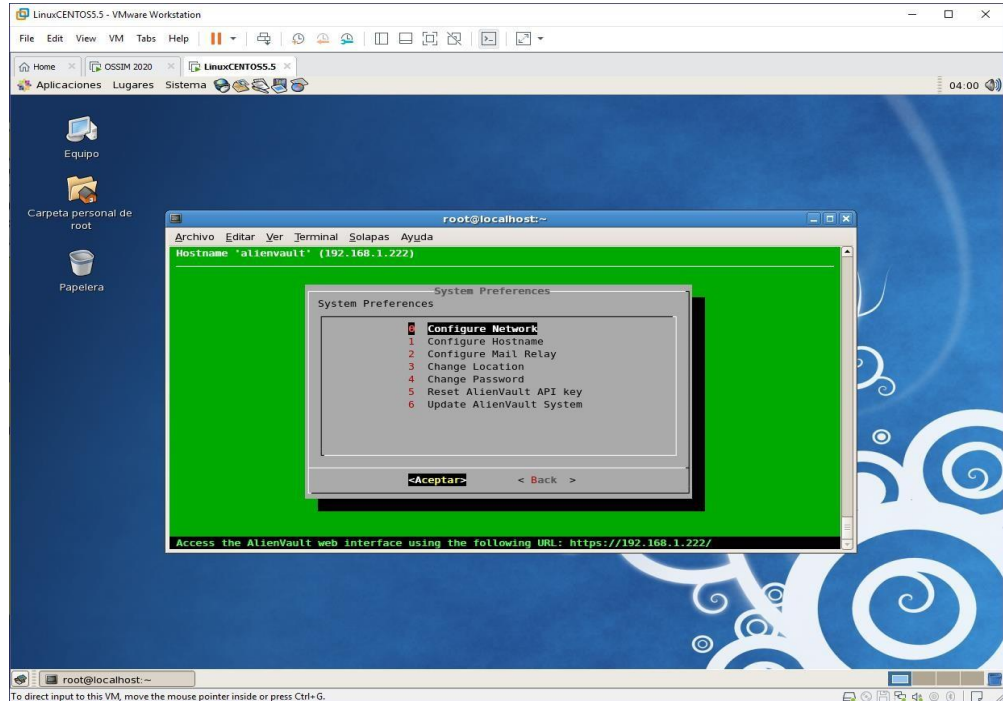


Figura 50. Submenú Preferencias del Sistema

Fuente: Propia

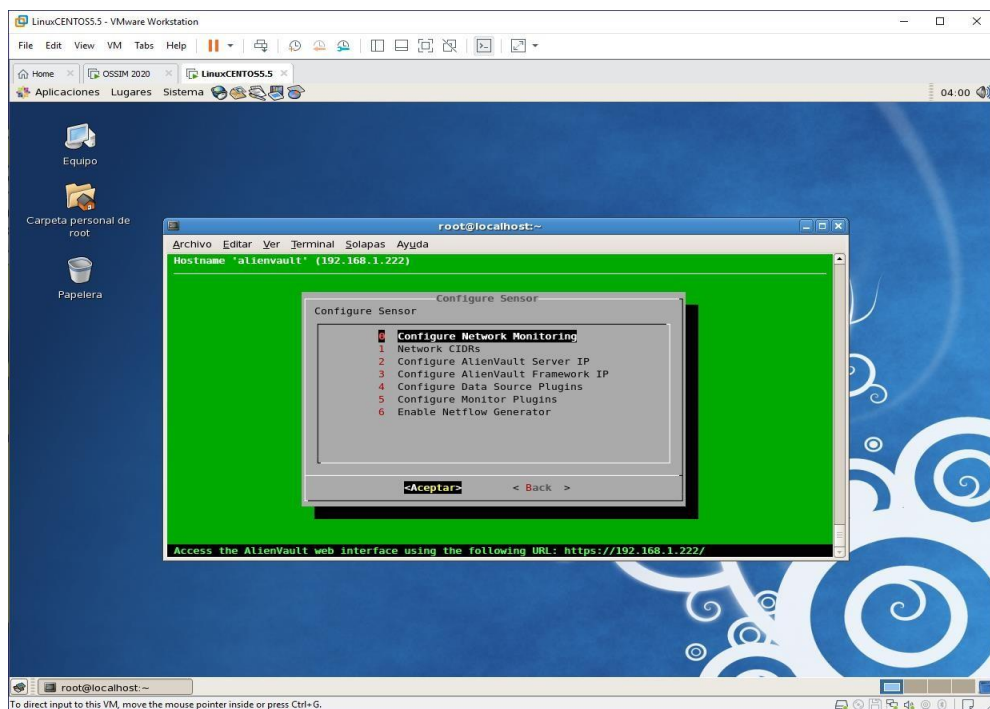


Figura 51. Submenú Configure Sensor

Fuente: Propia

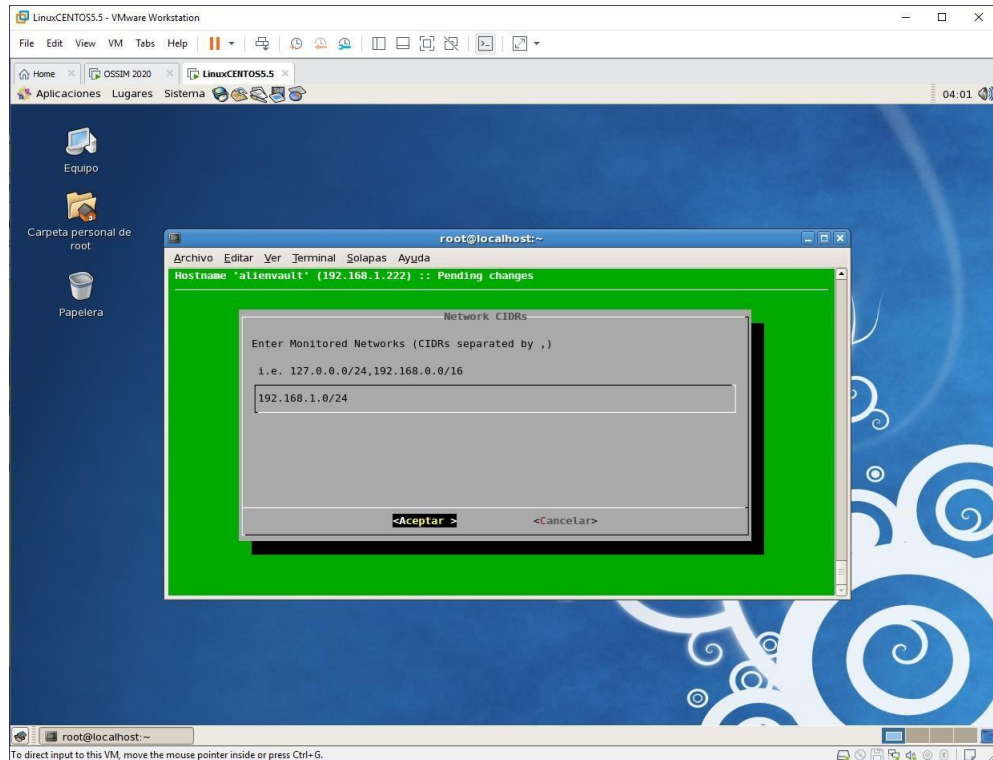


Figura 52. Configurando la Red de Monitoreo

Fuente: Propia

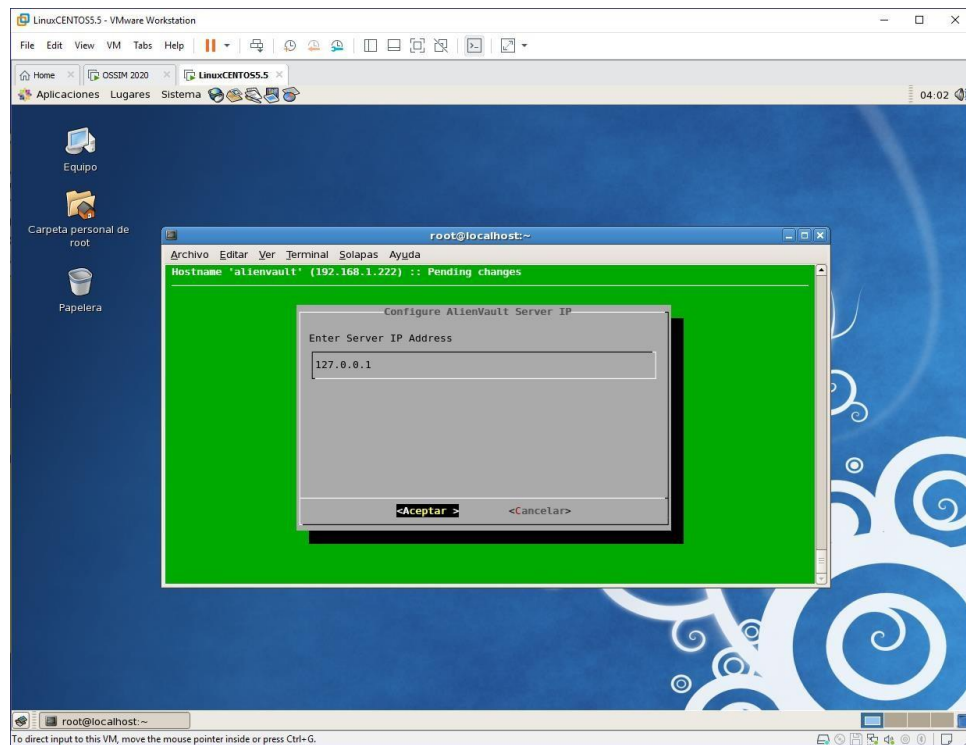


Figura 53. Configurando la Dirección IP del Servidor OSSIM

Fuente: Propia

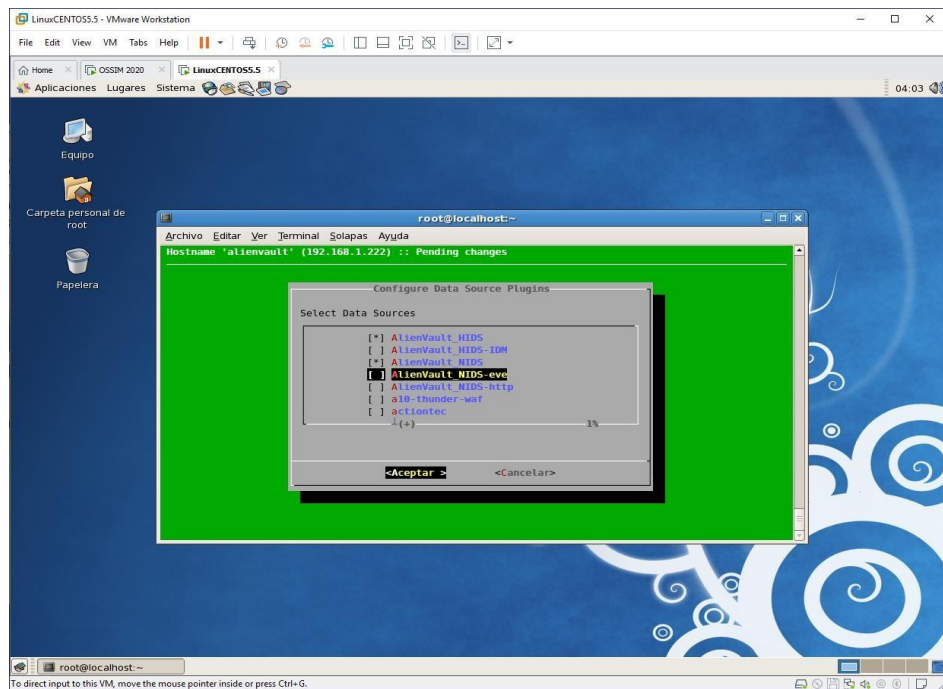


Figura 54. Configurando Plugins de Origen de Datos

Fuente: Propia

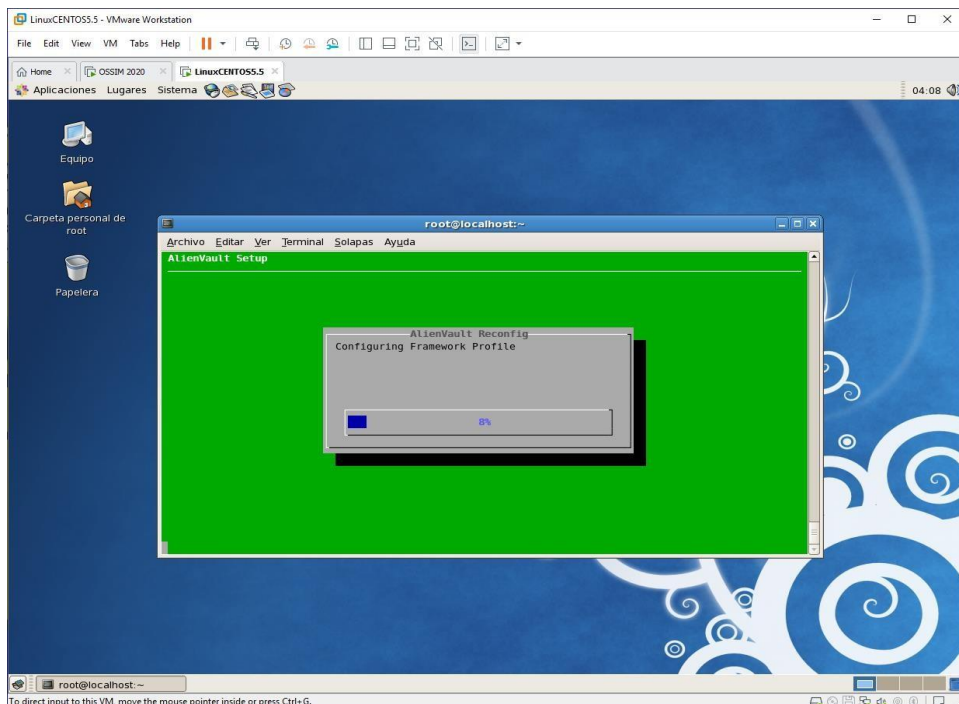


Figura 55. Actualizando la Configuración

Fuente: Propia

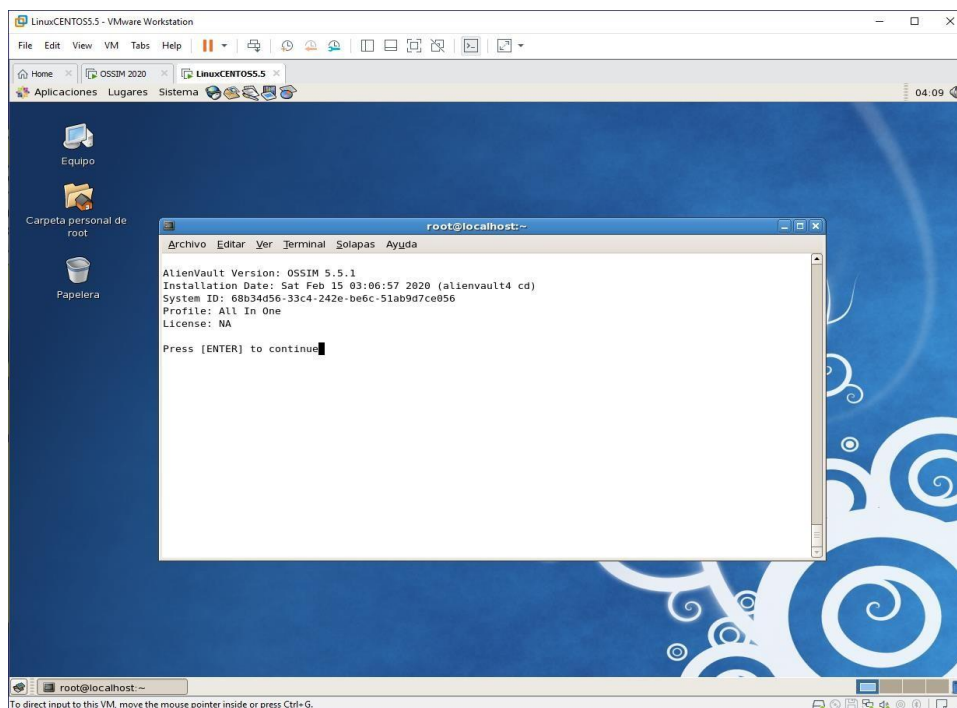


Figura 56. Ingresando a Modo Consola de Comandos

Fuente: Propia

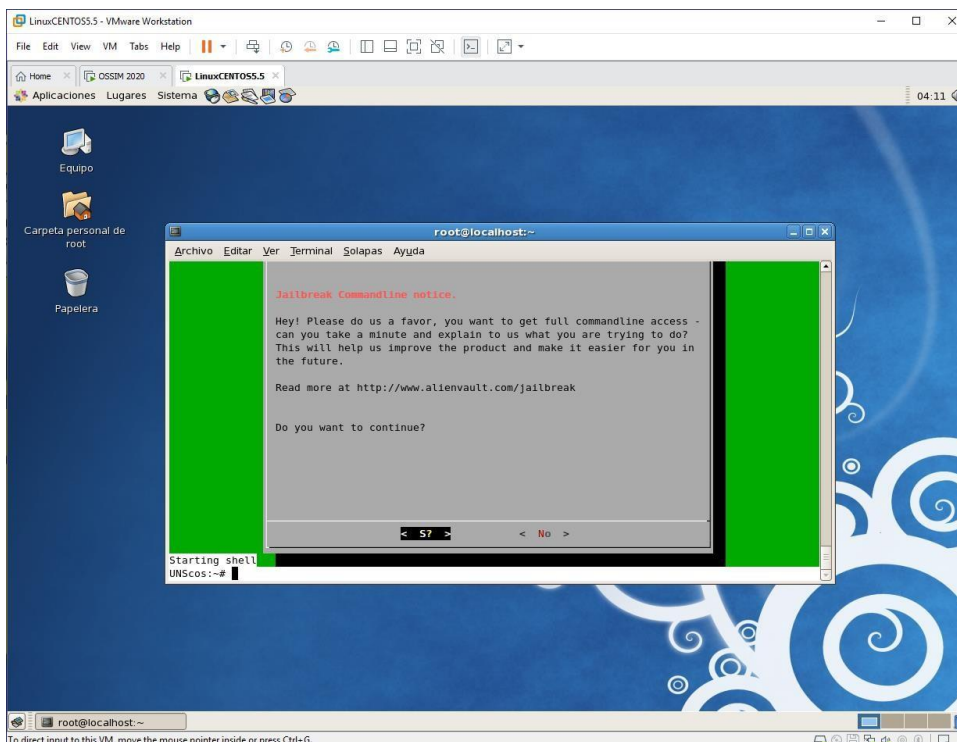


Figura 57. Confirmación para Ingreso a Modo de Comandos

Fuente: Propia

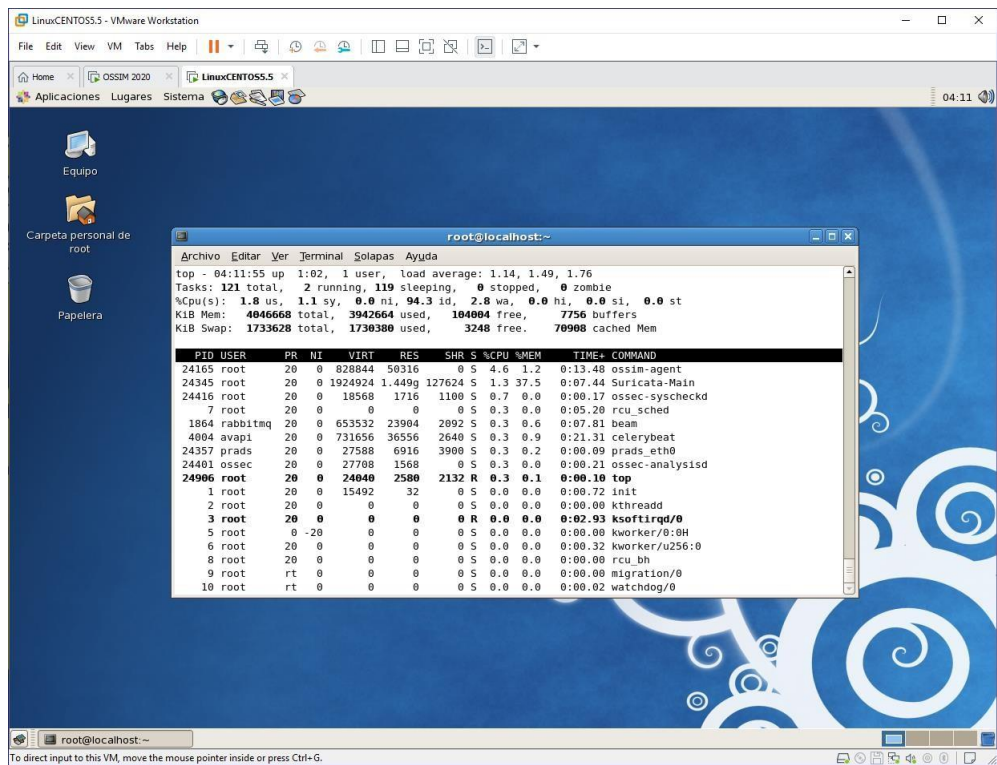


Figura 58. Visualizando los Procesos Ejecutándose en el Servidor OSSIM

Fuente: Propia

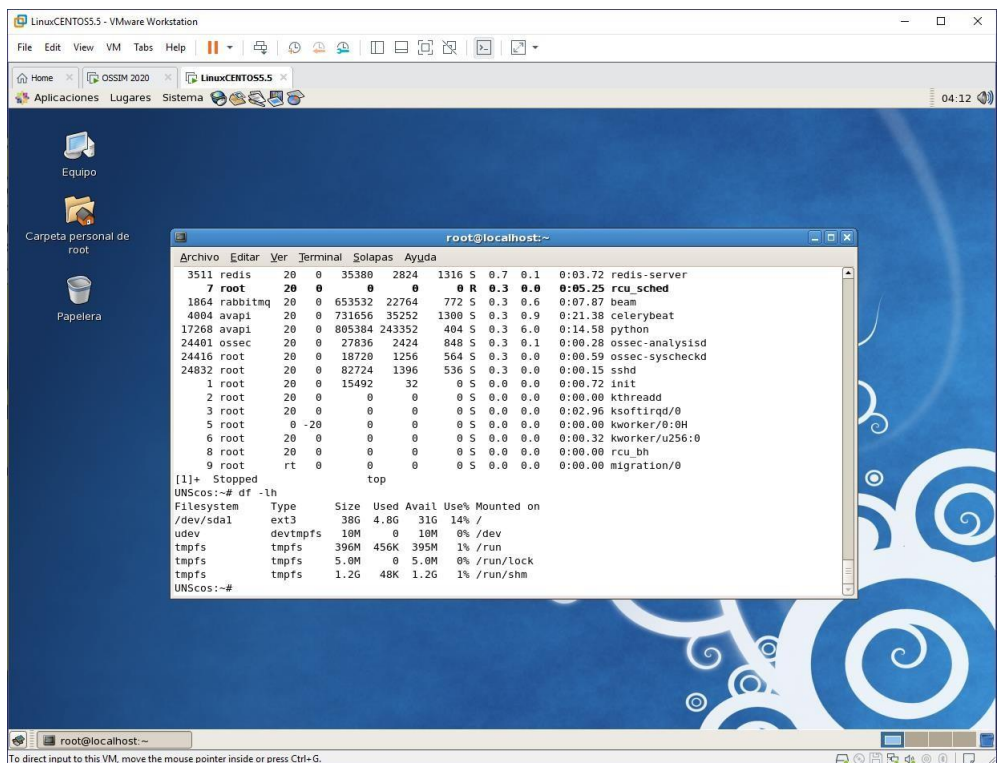


Figura 59. Visualizando las Particiones del Disco Duro del Servidor OSSIM

Fuente: Propia

De la herramienta de administración de OSSIM se puede ingresar a la opción AMBIENTE, y luego dar click a la opción ACTIVOS (ASSETS), para visualizar a todos los activos de la red informática, y así determinar a qué recursos o activos monitorear.

En seguida se muestra algunos de los equipos informáticos que se encuentran instalados en la red informática, mostrando su dirección IP, el sistema operativo detectado, vulnerabilidades detectadas, etc.

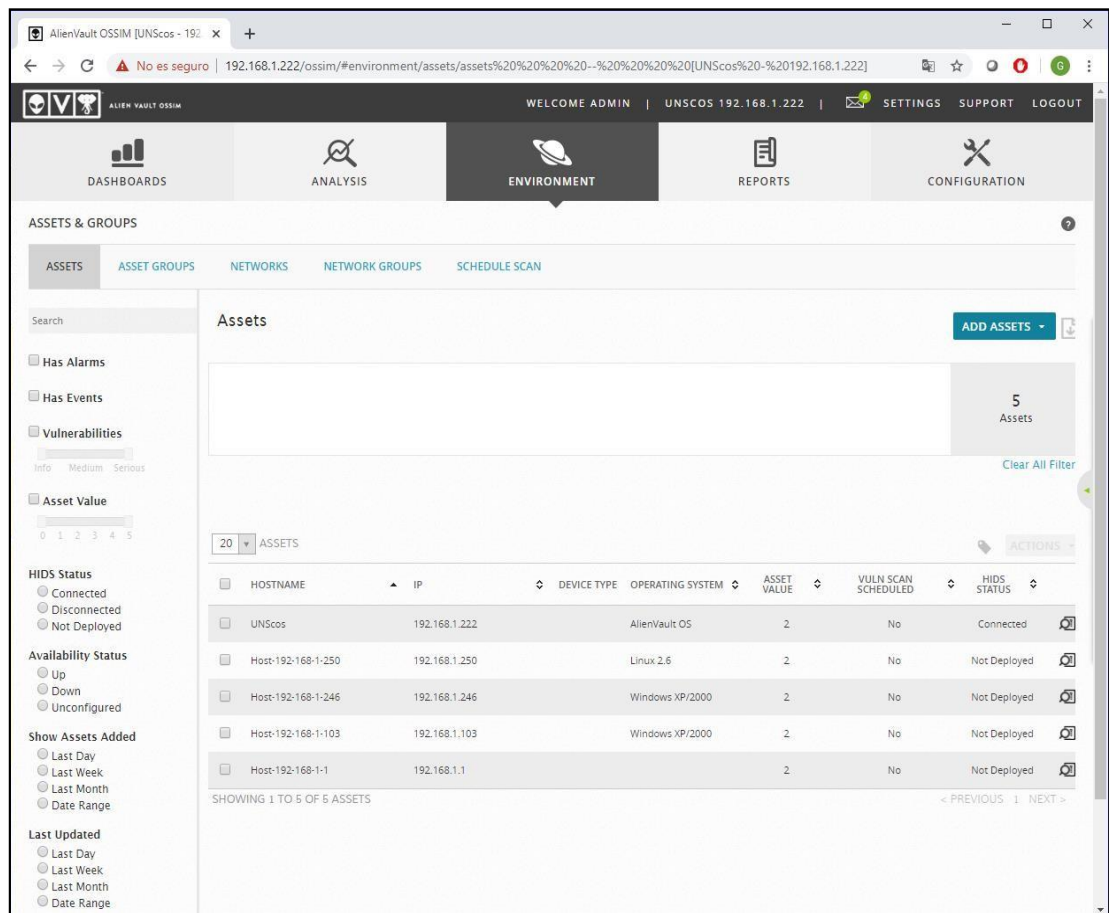


Figura 60. Visualizando las Particiones del Disco Duro del Servidor OSSIM

Fuente: Propia

Para iniciar el proceso del Centro de Operaciones de Seguridad, se tiene que detectar todos los activos de la red informática, por lo cual se tiene que hacer un escaneo, ubicando los diferentes recursos: servidores, estaciones de trabajo, router, switches, etc; los que serán monitoreados.

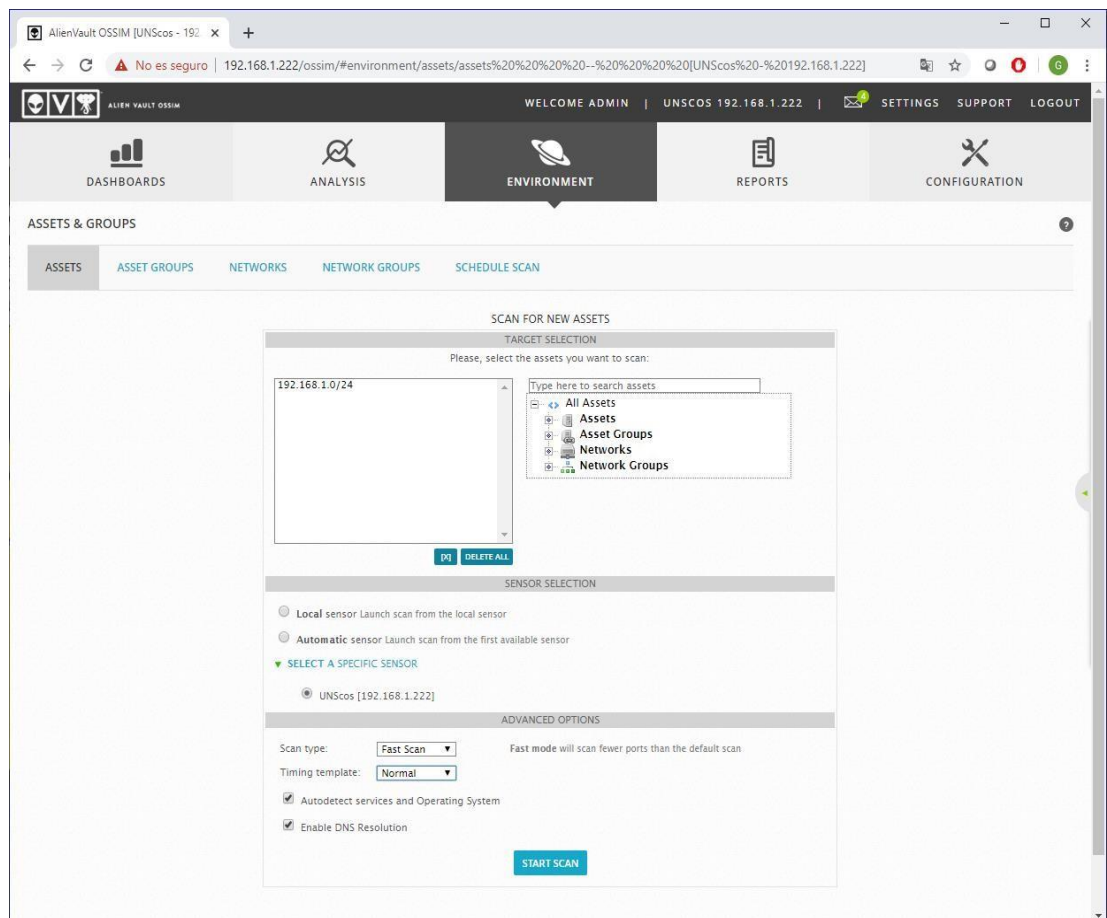


Figura 61. Configurar la Búsqueda de Nuevos Activos en la Red Informática

Fuente: Propia

Al finalizar el escaneo de la red informática, se obtendrá todos los hosts disponibles en la red, que podrán ser monitoreados desde el Centro de Operaciones de Seguridad, configurando posteriormente los servicios que serán detectados.

The screenshot displays the AlienVault OSSIM web interface. At the top, there are navigation tabs for DASHBOARDS, ANALYSIS, ENVIRONMENT (selected), REPORTS, and CONFIGURATION. Below these is an 'ADVANCED OPTIONS' panel with the following settings:

- Scan type: Fast Scan (Note: Fast mode will scan fewer ports than the default scan)
- Timing template: Normal
- Autodetect services and Operating System
- Enable DNS Resolution

A 'START SCAN' button is visible below the options. The main area shows a table of 'SCAN RESULTS' with the following columns: HOST, HOSTNAME, FQDN, DEVICE TYPES, MAC, OS, SERVICES, and FQDN AS HOSTNAME. The table contains 10 rows of scan results for various IP addresses in the 192.168.1.0/24 range.

HOST	HOSTNAME	FQDN	DEVICE TYPES	MAC	OS	SERVICES	FQDN AS HOSTNAME
192.168.1.1	Host-192-168-1-1	-	Switch	1CB0:44:29:9B:1A	eCos 3.X	tcpwrapped, tcpwrapped, http	
192.168.1.101	Host-192-168-1-101	-	General Purpose, Network Device	C4:6E:1F:C8:45:30	Linux 2.6.X	http	
192.168.1.11	Host-192-168-1-11	-	-	A0:CB:FD:77:1C:BA	-	-	
192.168.1.129	Host-192-168-1-129	-	-	A0:91:69:AA:80:49	-	-	
192.168.1.132	Host-192-168-1-132	-	-	14:1F:78:EE:EE:BB	-	-	
192.168.1.222	UNScos	UNScos.alienvault	General Purpose	-	Linux 3.X	ssh, mysql, https, http, otp	
192.168.1.246	Host-192-168-1-246	-	General Purpose	C8:21:58:4E:D4:F5	Windows XP	msrpc, netbios-ssn, microsoft-ds	
192.168.1.250	Host-192-168-1-250	-	General Purpose	00:0C:29:7A:51:CC	Linux 2.6.X	ssh	
192.168.1.5	Host-192-168-1-5	-	General Purpose	F8:3F:51:3B:35:82	Linux 3.X	http	
192.168.1.8	Host-192-168-1-8	-	-	10:32:7E:8D:57:4E	-	-	

At the bottom of the table, there are buttons for 'CLEAR SCAN RESULT' and 'UPDATE MANAGED ASSETS'. The footer of the page reads '© COPYRIGHT 2020 ALIENVAULT, INC. | LEGAL'.

Figura 63. Resultados de Búsqueda de Hosts

Fuente: Propia

Luego de detectados los activos disponibles en la red informática, se puede agrupar los activos, para lo cual se debe crear los grupos de activos asignándole un nombre, un valor y el sensor que se utilizara para monitorear.

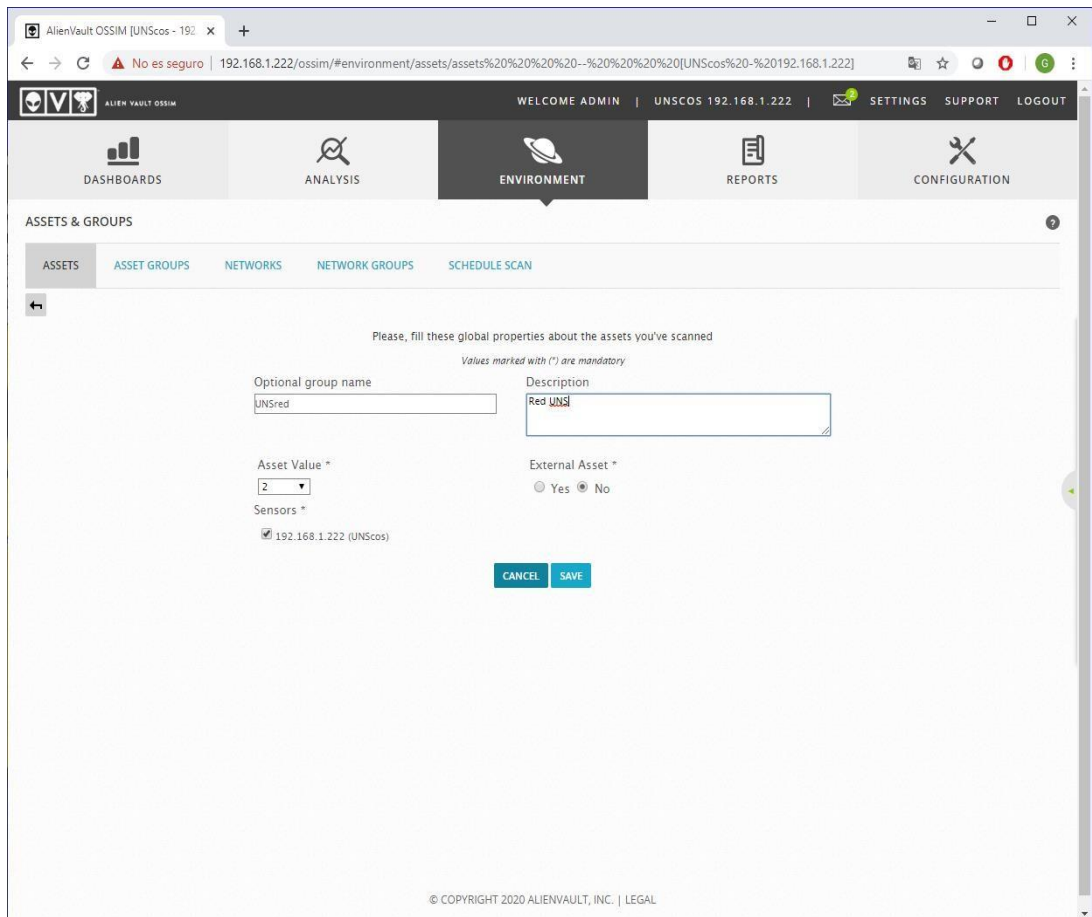


Figura 64. Configurando Grupo de Activos de la Red Informática

Fuente: Propia

En seguida se muestra el grupo recién creado UNSred, donde se mostrarán los activos que la componen y sus principales indicadores.

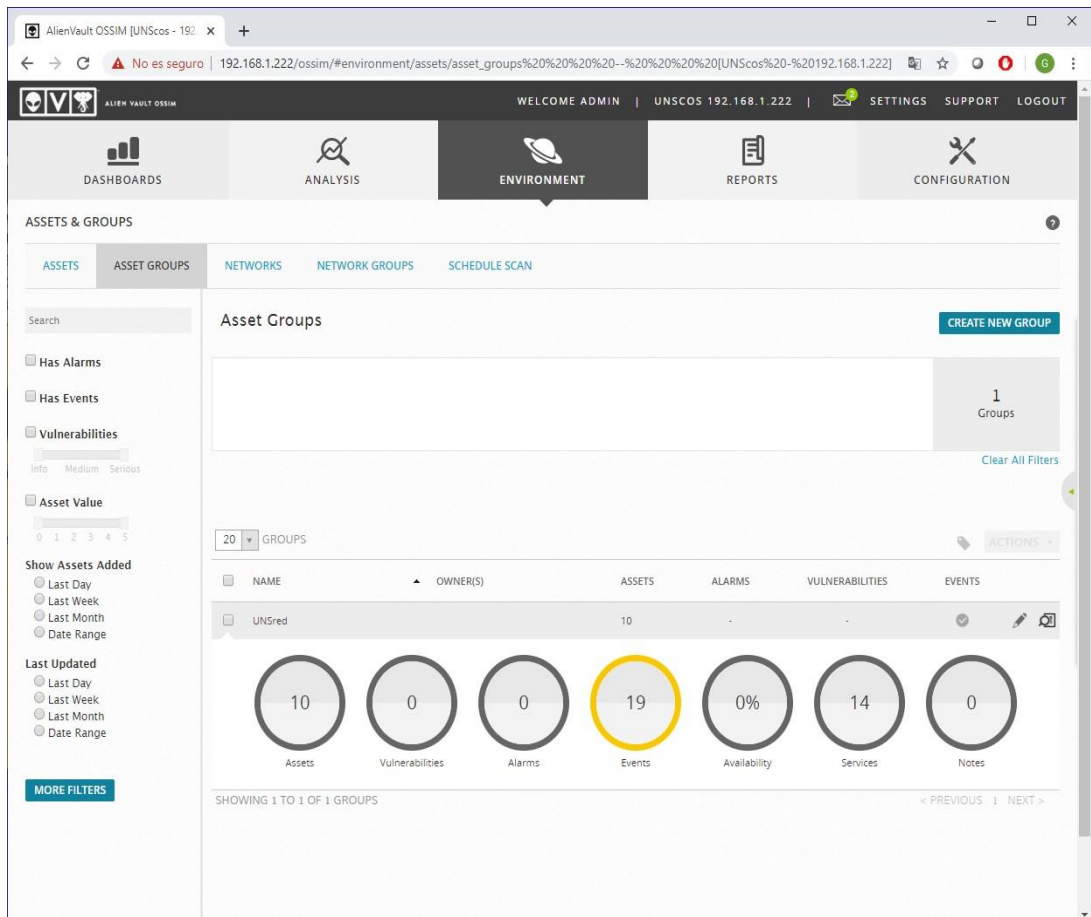


Figura 65. Grupo UNSred recién creado

Fuente: Propia

En la pestaña REDES se muestran las diferentes redes configuradas para la Red Informática de la Universidad Nacional del Santa, pudiéndose agregar o suprimir las redes que se consideren. A estas redes es a las que se realizara el monitoreo.

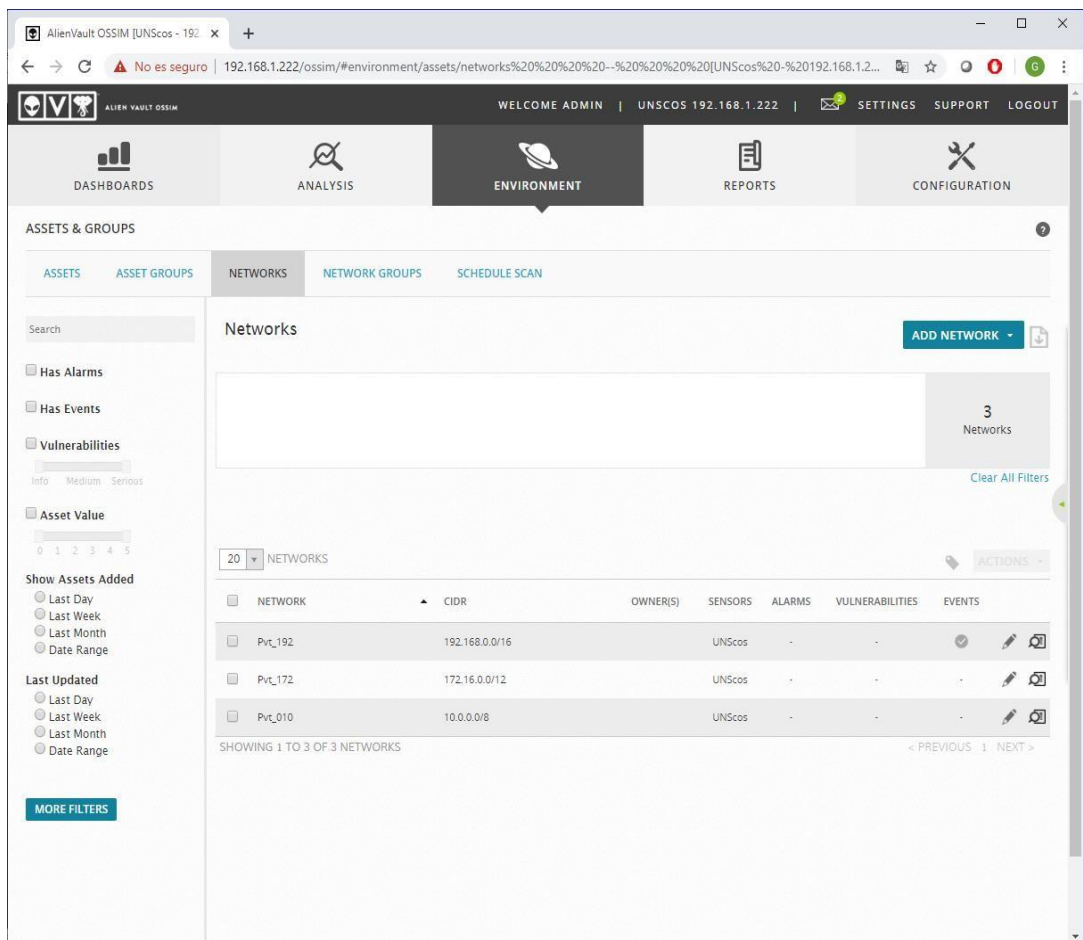


Figura 66. Redes Configuradas

Fuente: Propia

En OSSIM podemos visualizar la información detallada de un ACTIVO, en este caso sobre la estación de trabajo Windows 192.168.1.246 y de la estación de trabajo Linux 192.168.1.250.

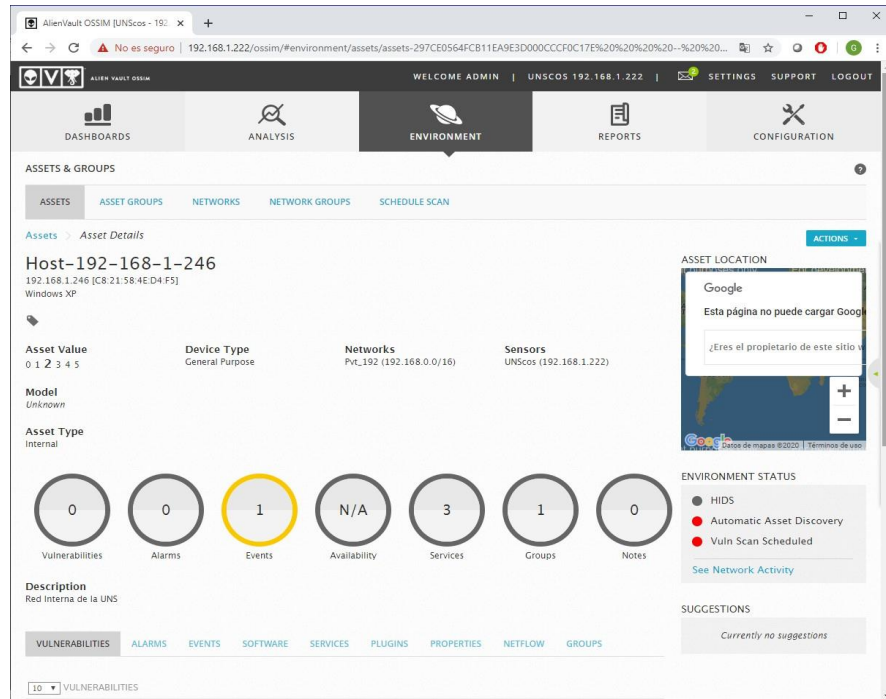


Figura 67. Visualizando Detalle de Estación de Trabajo Windows

Fuente: Propia

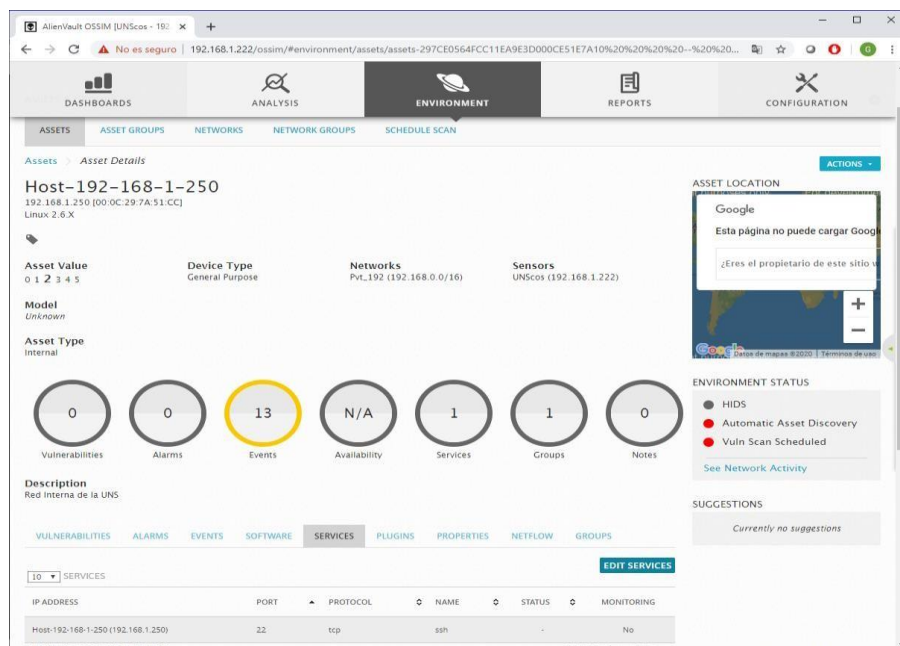


Figura 68. Visualizando Detalles de la Estación de Trabajo Linux

Fuente: Propia

En OSSIM también se puede mostrar información detallada de un servidor. En este caso se muestra la información del Servidor Web.

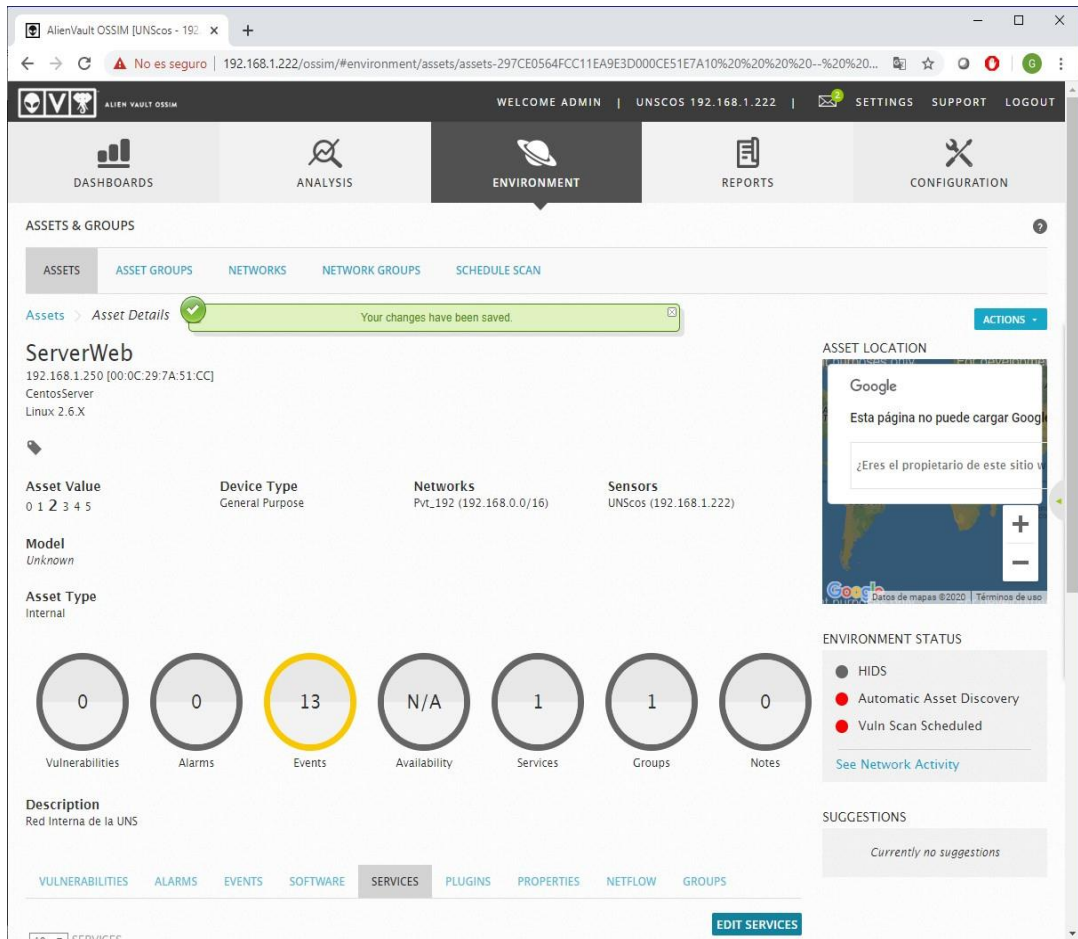


Figura 69. Visualizando Información Detallada del Servidor Web

Fuente: Propia

Para personalizar algún activo de la red informática, se puede editar sus características, como descripción, dirección ip, valor, sistema operativo, modelo, alias, tipo de activo, etc.

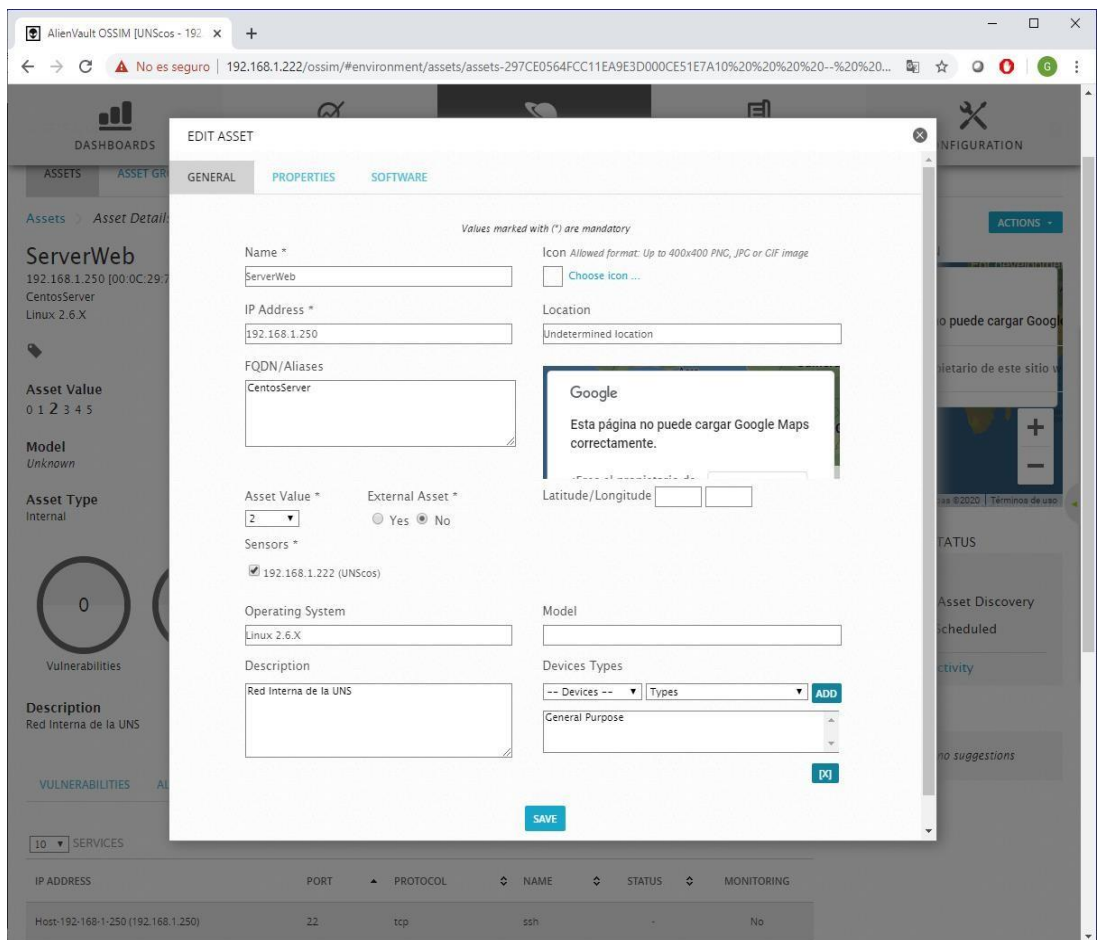


Figura 70. Edición de Detalles de un Activo

Fuente: Propia

Se puede configurar para que el Servidor OSSIM monitoree la Disponibilidad del Servidor Web, para ello se va al Menú Acciones.

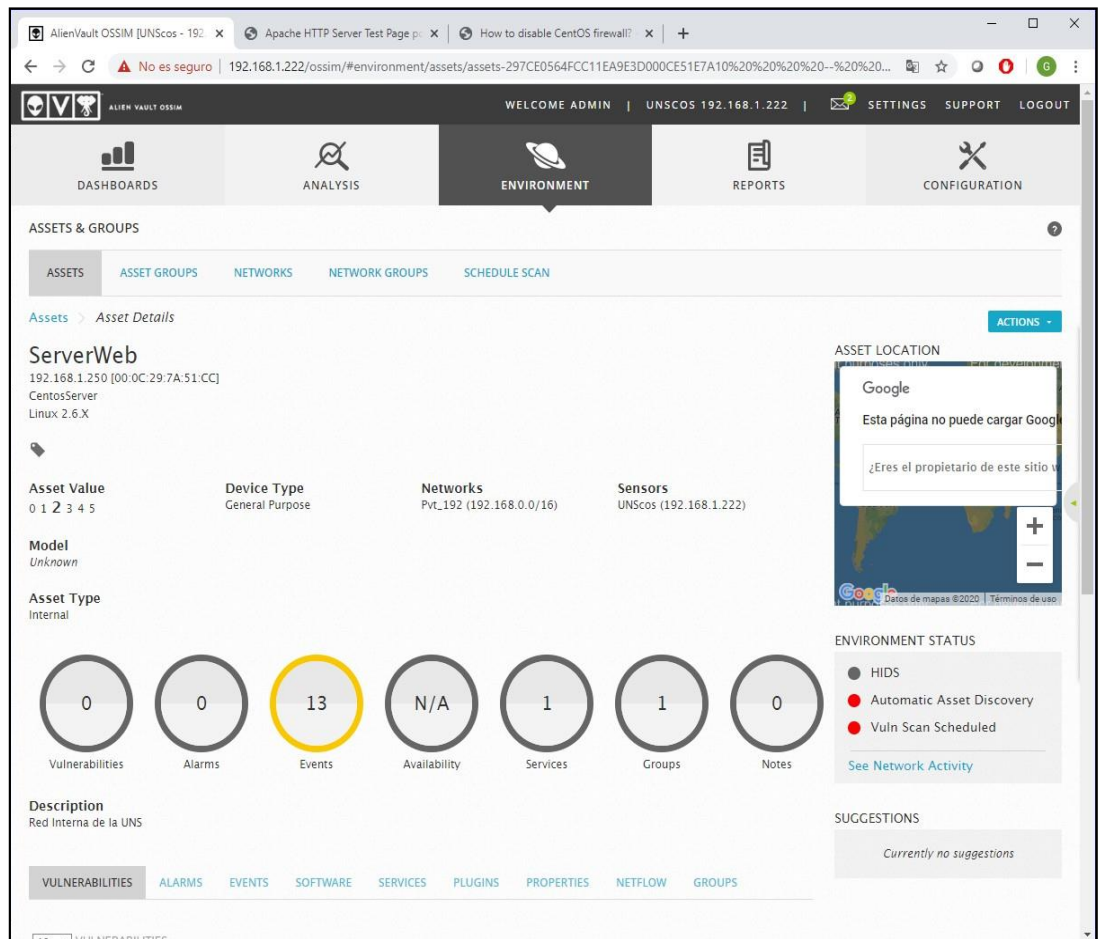


Figura 71. Configurando la Disponibilidad del Servidor Web

Fuente: Propia

Como resultado se activa la el monitoreo de la Disponibilidad del Servidor Web.

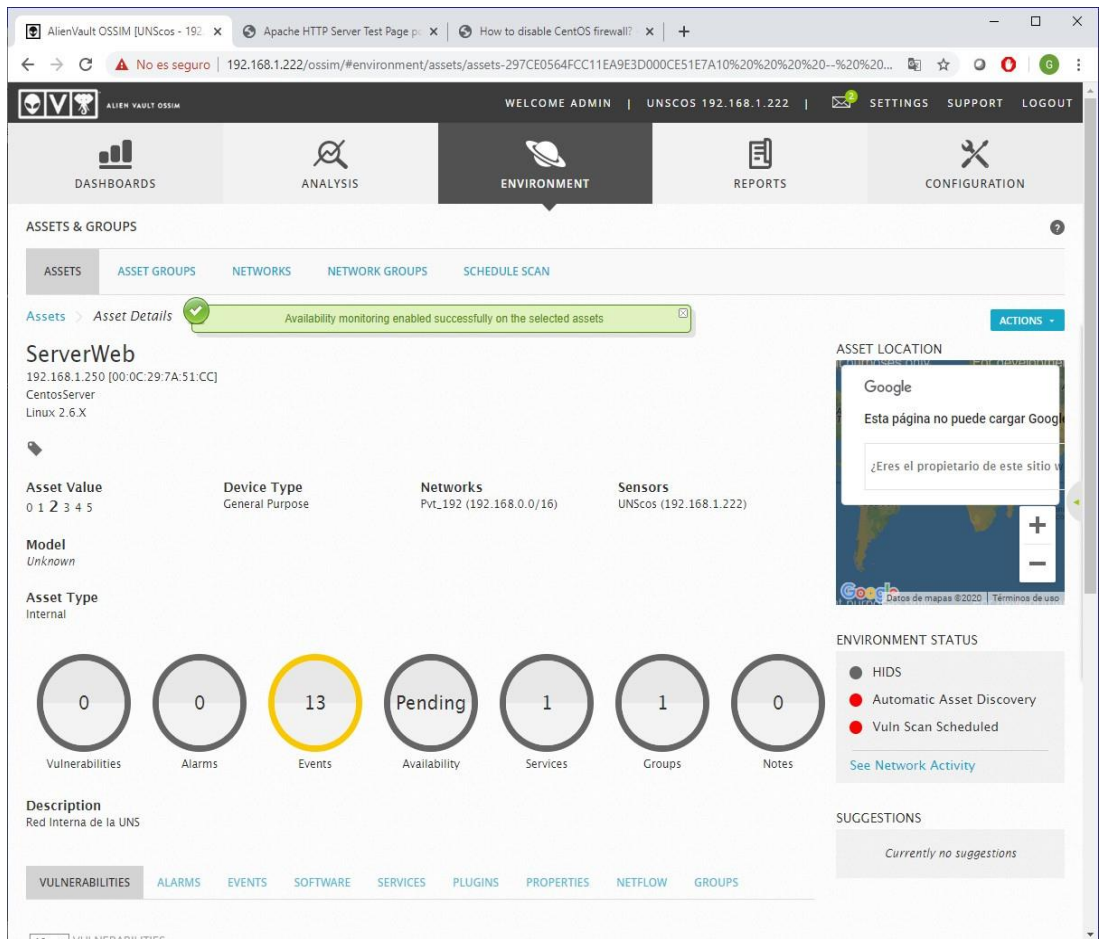


Figura 72. Disponibilidad configurada para el Servidor Web

Fuente: Propia

Después de que el Servidor OSSIM empieza a monitorear el Servidor Web, se van mostrando valores en los principales indicadores, como Vulnerabilidades, Alarmas, Eventos, Disponibilidad, Servicios, Grupos, Notas, etc.

Aquí el Servidor Web presenta 12 eventos, 8 servicios disponibles en la red, y pertenece a 1 grupo.

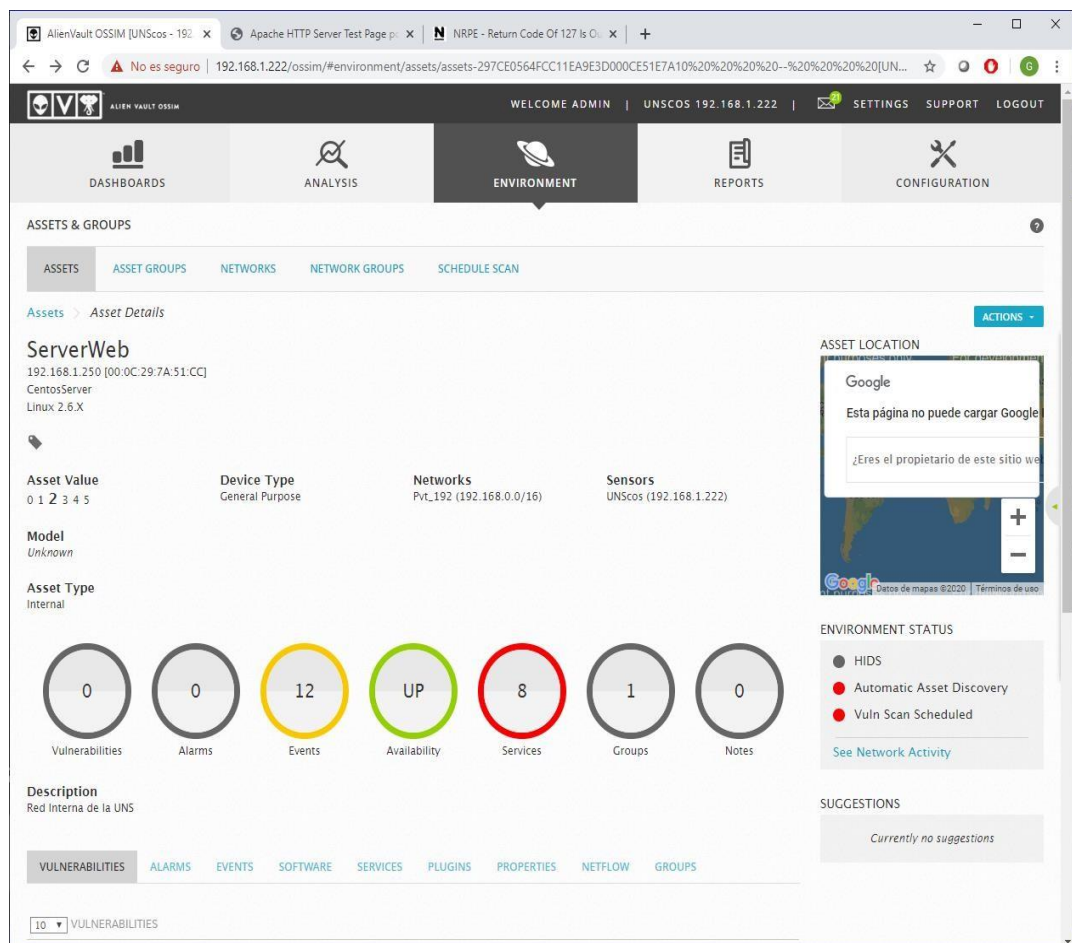


Figura 73. Resultados de Monitoreo del Servidor Web

Fuente: Propia

Los Servicios que se encuentran ejecutando en el servidor Web se pueden monitorear, por lo cual se puede editar esos servicios.

Allí se aprecia los puertos, el tipo de protocolo y su status.

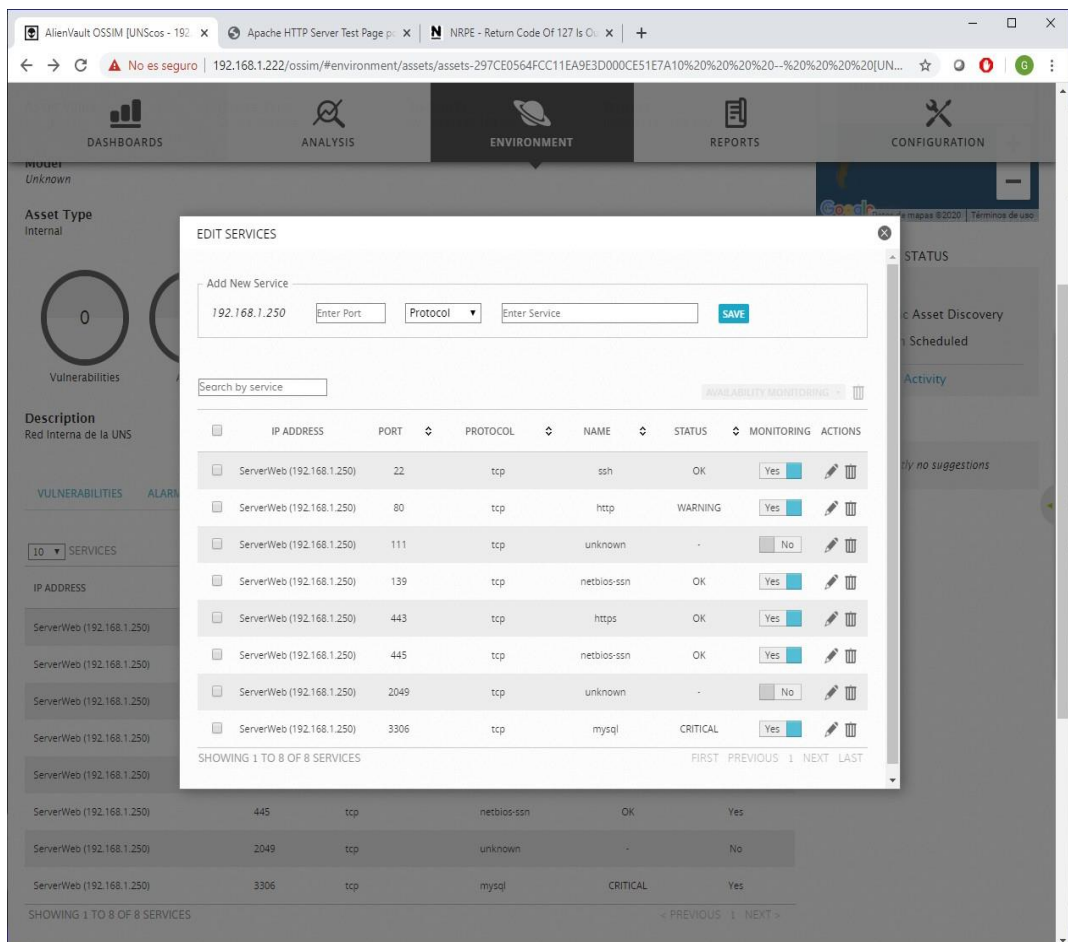


Figura 74. Edición de Servicios del Servidor Web

Fuente: Propia

Luego de configurar los servicios que serán monitoreados en el Servidor Web, se muestran en la ventana principal de gestión, se muestran 8 servicios.

Cualquier cambio o alerta en algunos de los servicios se mostrarán inmediatamente en la pantalla, pudiendo hacerse la consulta.

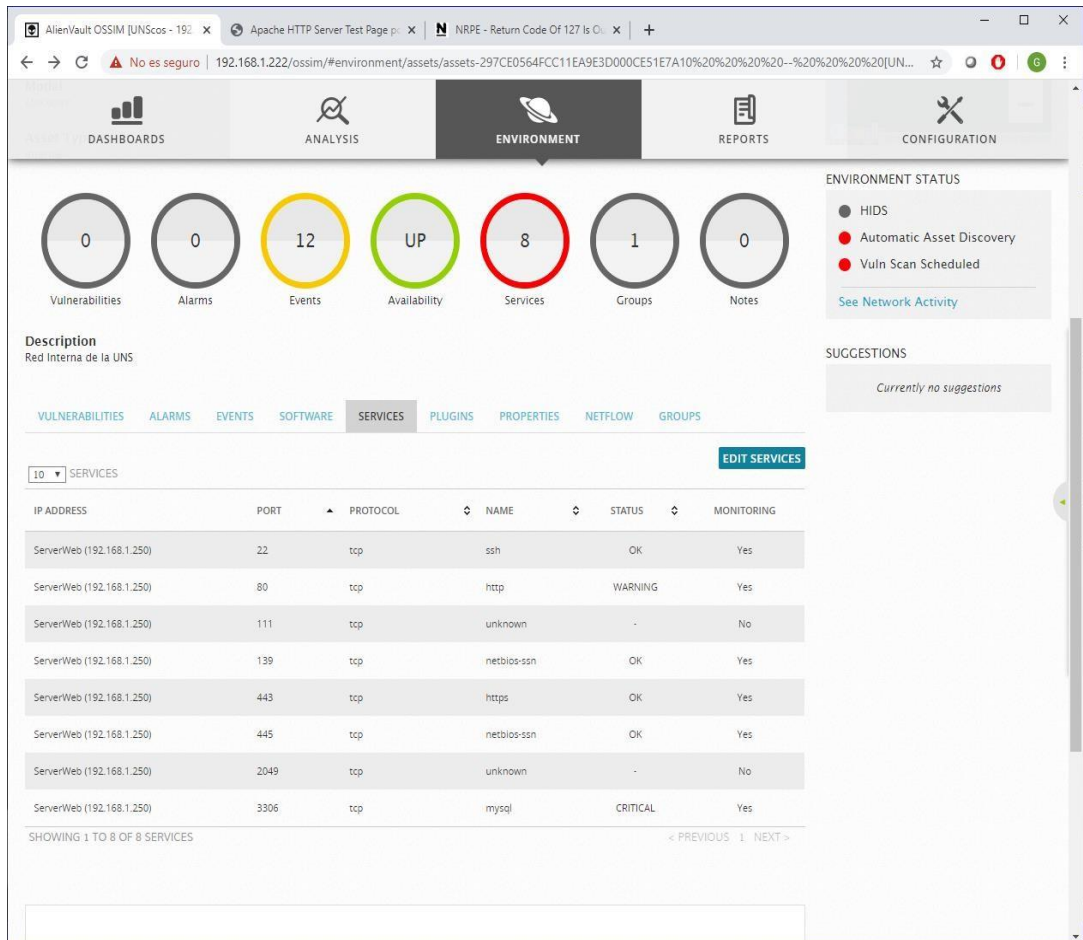


Figura 75. Los Servicios del Servidor Web configurados para monitoreo

Fuente: Propia

Si se quiere visualizar todos los hosts y servicios monitoreados en la red, se selecciona Ambiente y Monitoreo. Allí se puede visualizar indicadores de monitoreo tanto críticos, advertencias o satisfactorios.

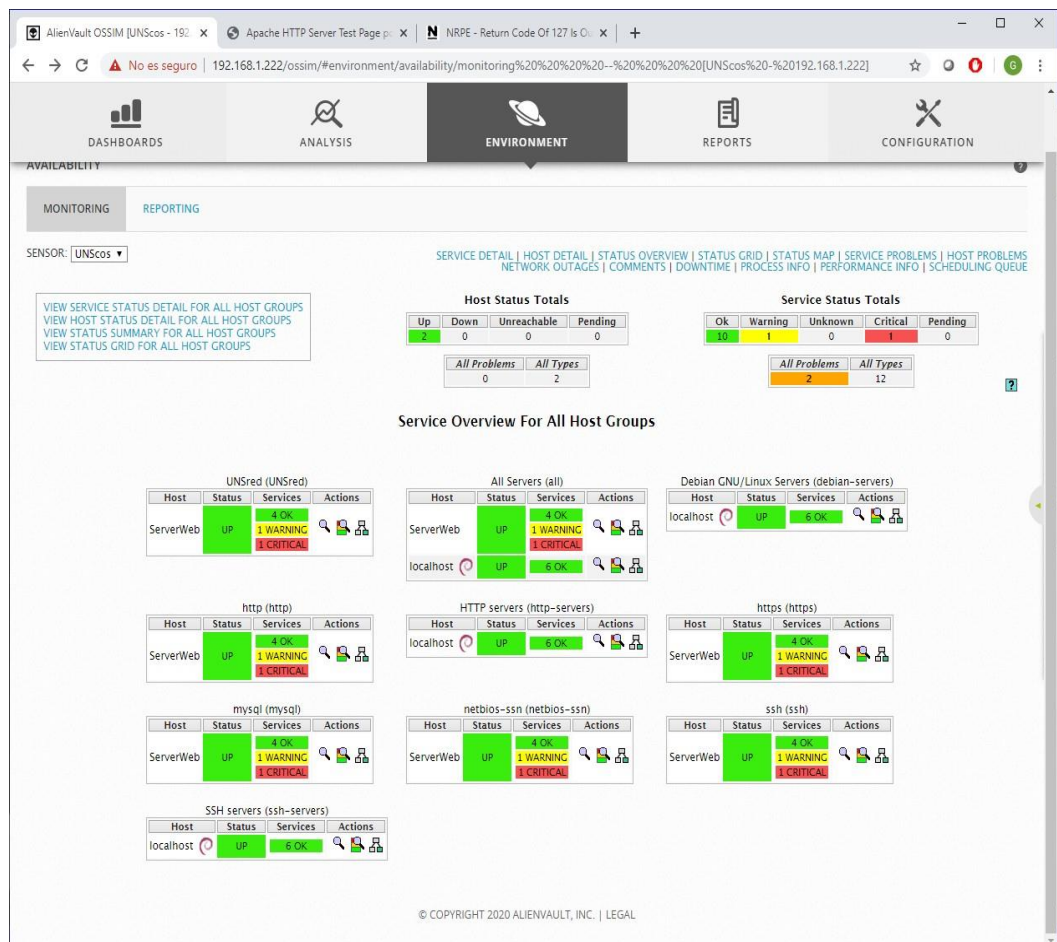


Figura 76. Servicios Monitoreados en la Red UNS

Fuente: Propia

Se puede mostrar en detalle información de un Host, para una respuesta rápida de seguridad. Aquí se muestra el detalle del Servidor Web.

Host State Information

Host Status: **UP** (for 2d 23h 25m 9s)

Status Information: PING OK - Packet loss = 0%, RTA = 0.96 ms

Performance Data: rta=0.959000ms;5000.000000;5000.000000;0.000000 pl=0%;100;100;0

Current Attempt: 1/10 (HARD state)

Last Check Time: 2020-02-24 12:49:03

Check Type: ACTIVE

Check Latency / Duration: 0.007 / 0.056 seconds

Next Scheduled Active Check: 2020-02-24 12:54:13

Last State Change: 2020-02-21 13:28:25

Last Notification: N/A (notification 0)

Is This Host Flapping? **NO** (0.00% state change)

In Scheduled Downtime? **NO**

Last Update: 2020-02-24 12:53:33 (0d 0h 0m 1s ago)

Active Checks: **ENABLED**

Passive Checks: **ENABLED**

Obsessing: **ENABLED**

Notifications: **ENABLED**

Event Handler: **ENABLED**

Flap Detection: **ENABLED**

Host Commands

- Locate host on map
- Disable active checks of this host
- Re-schedule the next check of this host
- Submit passive check result for this host
- Stop accepting passive checks for this host
- Stop obsessing over this host
- Disable notifications for this host
- Send custom host notification
- Schedule downtime for this host
- Schedule downtime for all services on this host
- Disable notifications for all services on this host
- Enable notifications for all services on this host
- Schedule a check of all services on this host
- Disable checks of all services on this host
- Enable checks of all services on this host
- Disable event handler for this host
- Disable flap detection for this host

Host Comments

Add a new comment Delete all comments

Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
This host has no comments associated with it							

Figura 77. Visualizando Detalles del Hosts Servidor Web

Fuente: Propia

En la opción de Monitoreo se puede mostrar el detalle del status de un Servidor, para visualizar las alertas, riesgos o problemas existentes, a fin de poder ser corregidos. Aquí se muestra el Servidor Web, donde muestra 4 servicios que están Ok, un servicio con un posible error (http) y un servicio con un error critico (MySQL).

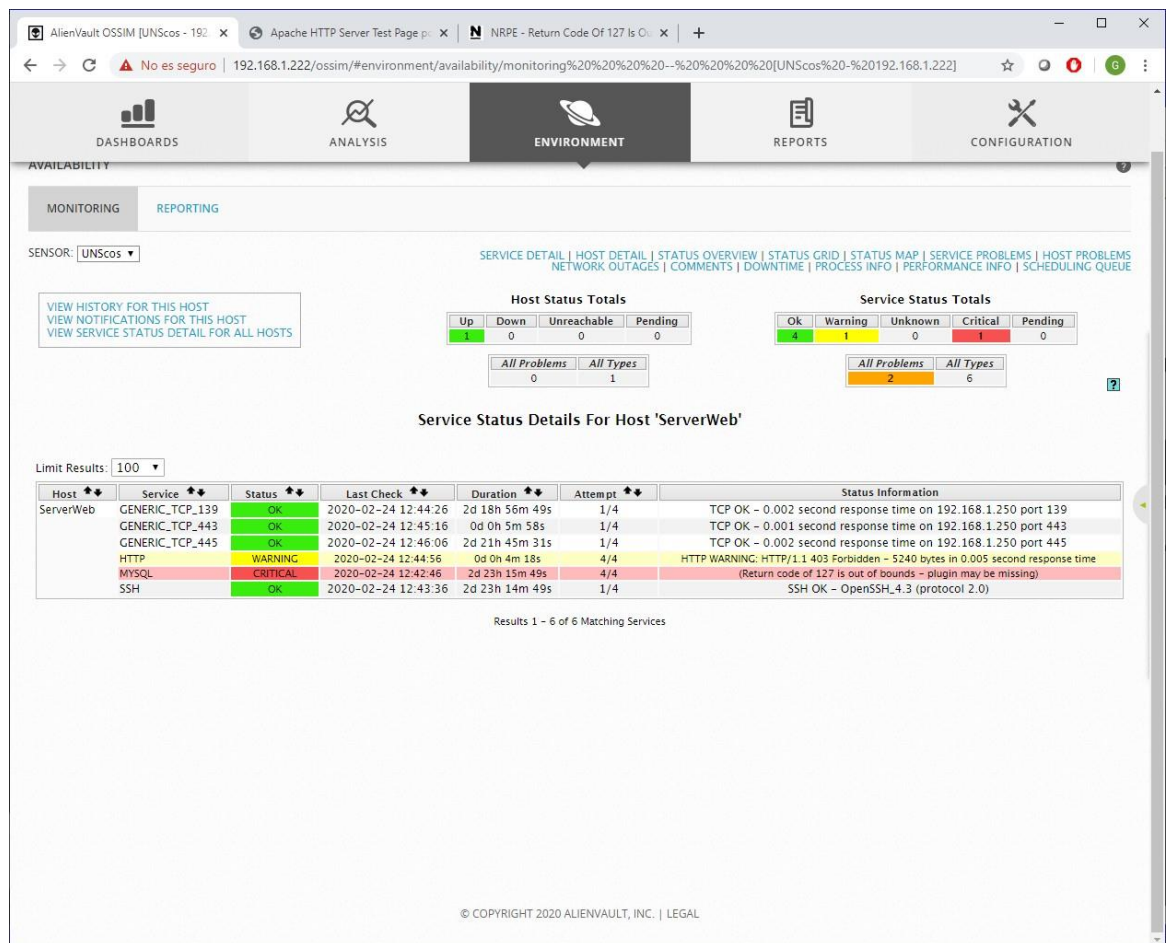


Figura 78. Visualizando el Status del Servidor Web

Fuente: Propia

Se puede mostrar solo los errores críticos de un servidor, a fin de ser más selectivo. Para el presente caso se muestra el error crítico del Servidor Web, que corresponde al servicio MySQL, que al parecer por versión no instalo el correcto plugin.

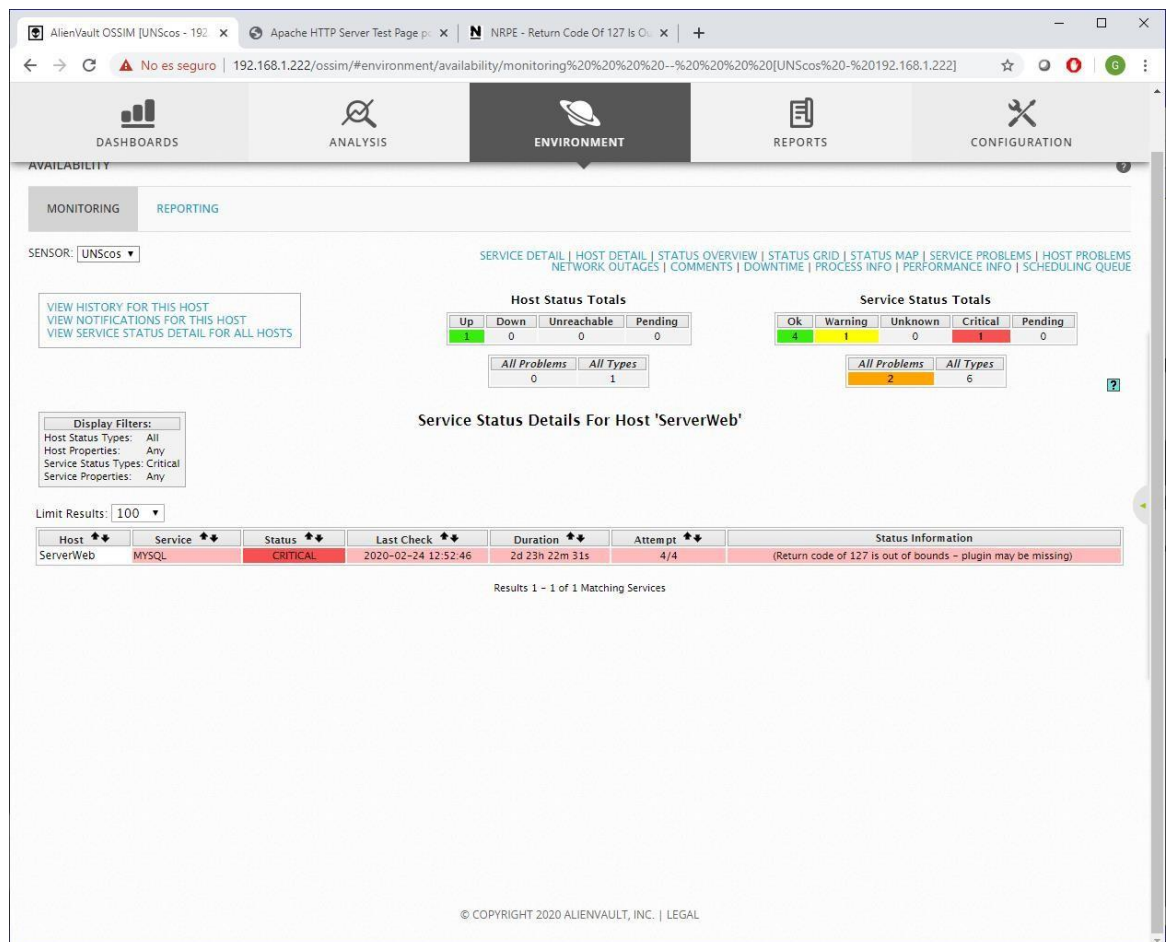


Figura 79. Visualizando los Servicios con Error Críticos

Fuente: Propia

Se puede obtener soporte técnico sobre errores y advertencias encontradas por OSSIM en alguno de los activos monitoreados en la red informática, para lo cual se selecciona el error y nos accede a la base de datos de soporte técnico de nagios.

The screenshot shows a web browser window displaying a Nagios Knowledge Base article. The browser tabs include 'AlienVault OSSIM [UNScos - 192...]', 'Apache HTTP Server Test Page p...', and 'NRPE - Return Code Of 127 Is Out...'. The address bar shows the URL: 'support.nagios.com/kb/article/nrpe-return-code-of-127-is-out-of-bounds-plugin-may-be-missing-613.html'. The article title is 'NRPE - Return Code Of 127 Is Out Of Bounds - Plugin May Be Missing'. Below the title, it shows 'Article Number: 613 | Rating: Unrated | Last Updated by tea on Fri, Jul 14, 2017 at 3:34 AM'. The 'Problem Description' section states: 'This KB article addresses the following NRPE error: Return Code Of 127 Is Out Of Bounds - Plugin May Be Missing'. The 'Assumed Knowledge' section explains that the article contains an explanation of how NRPE works and may need to be referenced to understand the problem and solution. The 'Troubleshooting The Error' section describes the error and provides a screenshot of a command configuration interface. The command view shows: '\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -t 30 -c \$ARG1\$ \$ARG2\$'. The 'Check command' dropdown is set to 'check_nrpe'. The 'ARG1\$' field contains 'check_foo' and the 'ARG2\$' field contains '-a "-w x -c y"'. Below the command view, it states: 'You can see the command is called: check_foo'.

Figura 80. Encontrando soporte a Error Critico encontrado por el Servidor OSSIM

Fuente: Propia

Cuando se apaga el Servidor Web o sucede algún percance en el, al ser uno de los activos determinados para ser monitoreado, en el sistema OSSIM inmediatamente se muestra las alertas en color rojo, para reflejar la situación actual y permitir al administrador del COS tomar las medidas correctivas apropiadas.

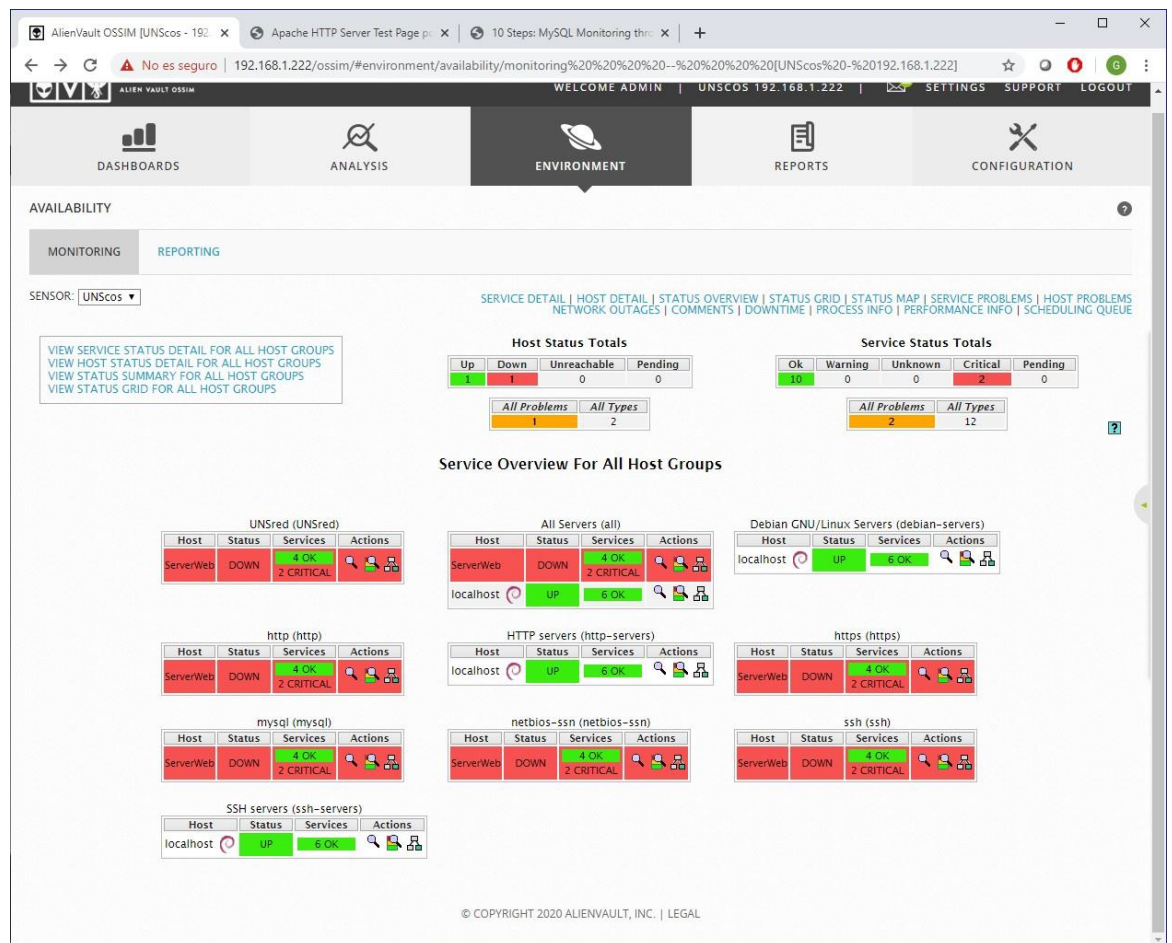


Figura 81. Visualizando alertas cuando sucede un problema en el Servidor Web

Fuente: Propia

Se pueden mostrar el detalle del status de los servicios en todos los hosts o servidores de la red informática.

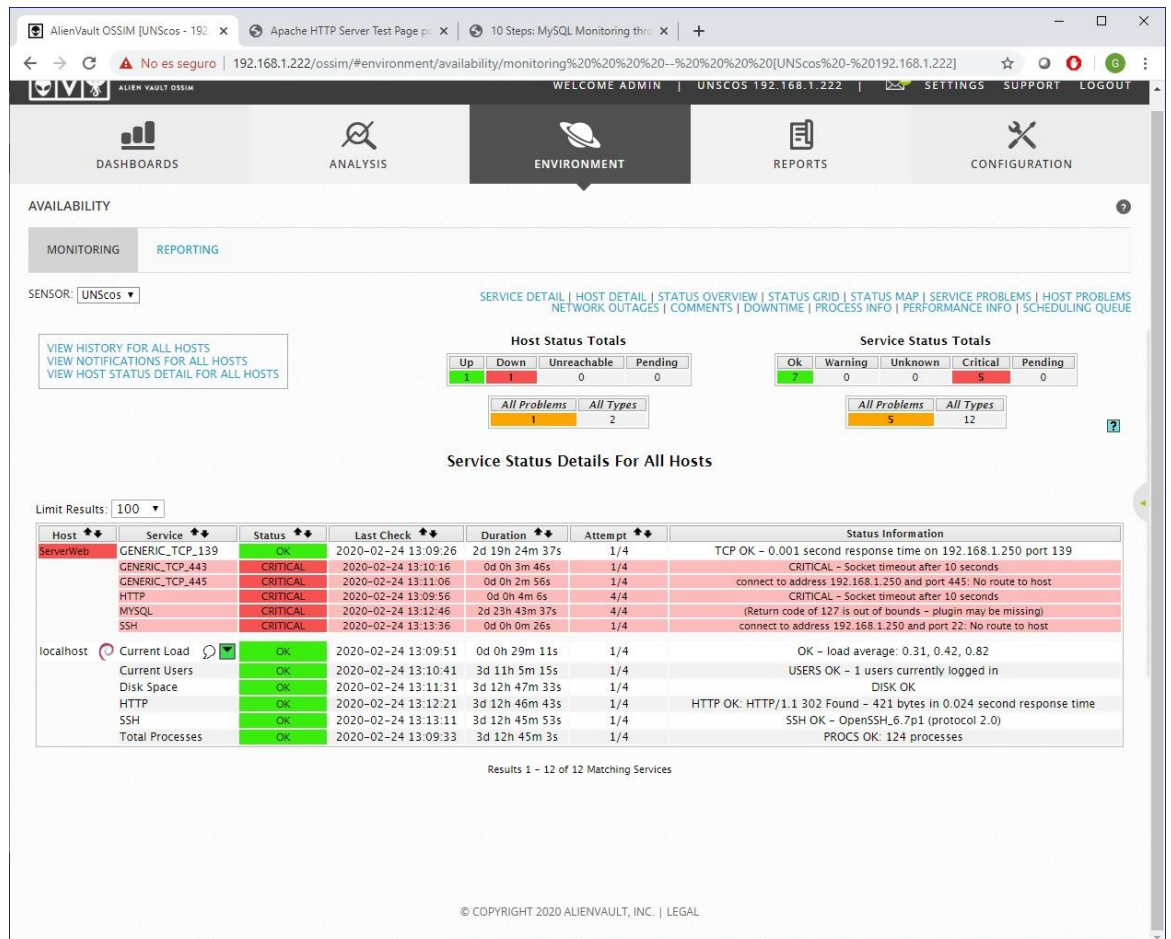


Figura 82. Mostrando el Detalle del Status de los Servicios en todos los Servidores

Fuente: Propia

También se puede mostrar el detalla del status de los servidores en la red informática. Aquí se muestra que el servidor Web esta caído o apagado, y el servidor local esta encendido o activo.

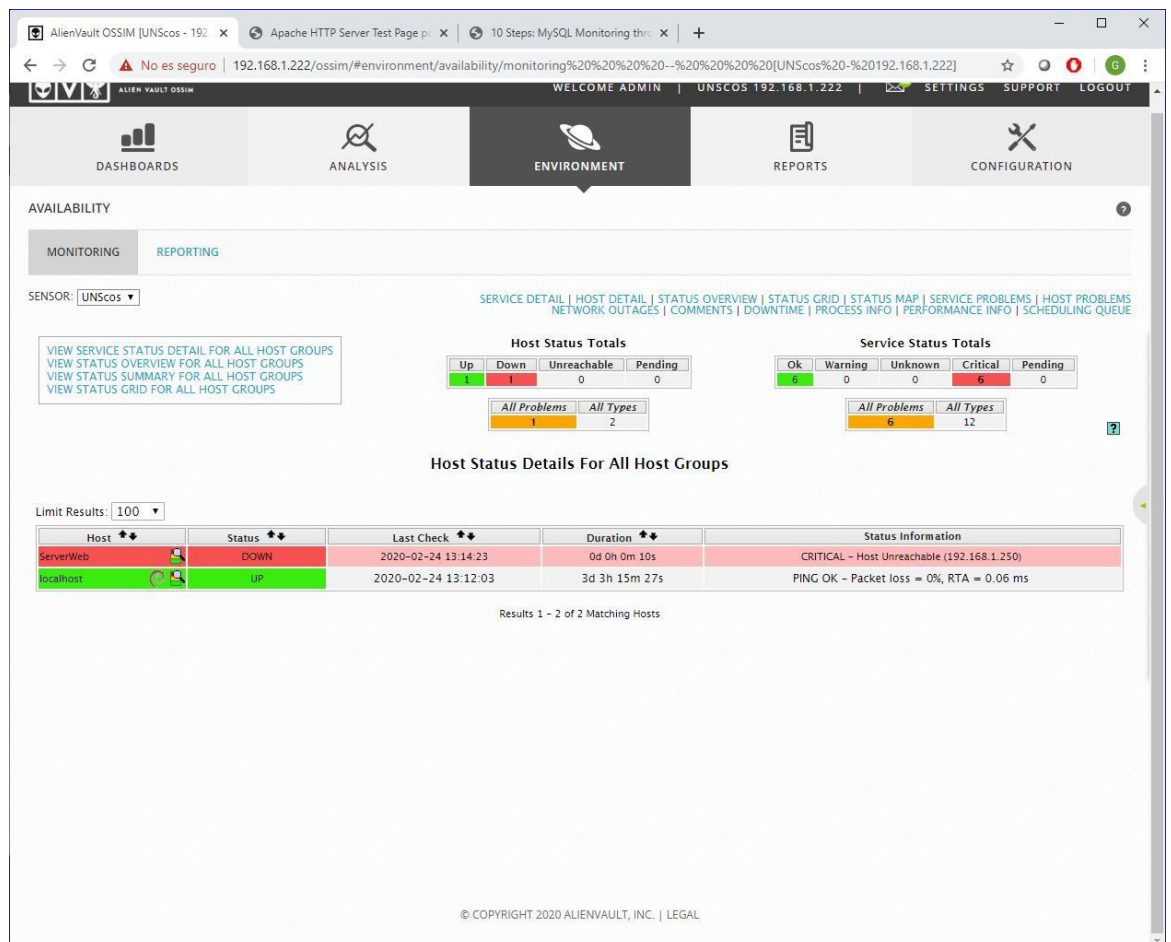


Figura 83. Visualizando el status de los hosts dentro de la Red Informática

Fuente: Propia

Teniendo en cuenta los resultados obtenidos en el monitoreo dentro de algún lapso de tiempo, se pueden realizar reportes de acuerdo a algunos parámetros.

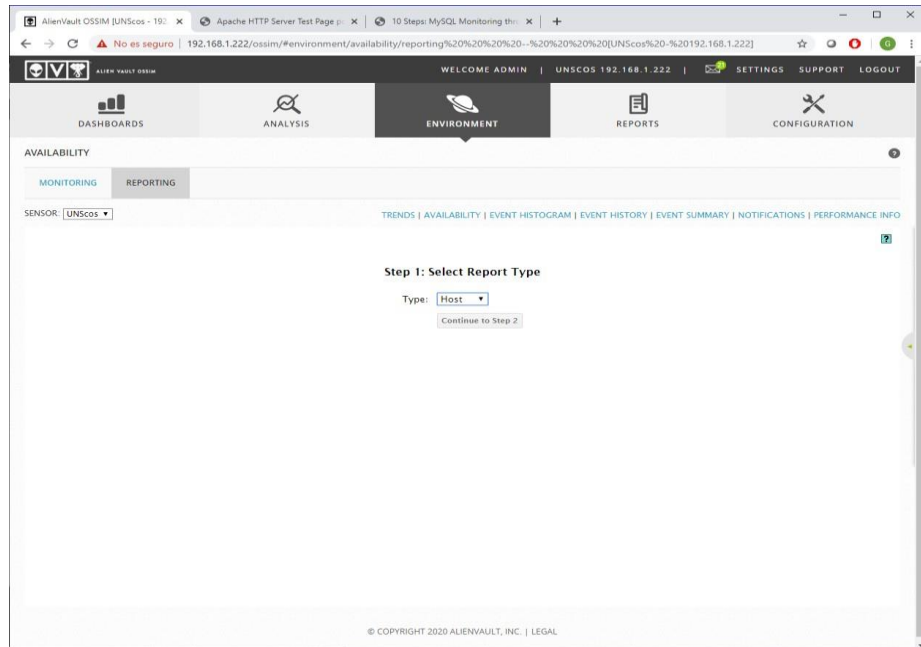


Figura 84. Configurando el Tipo de Reporte a Generar en el Servidor OSSIM

Fuente: Propia

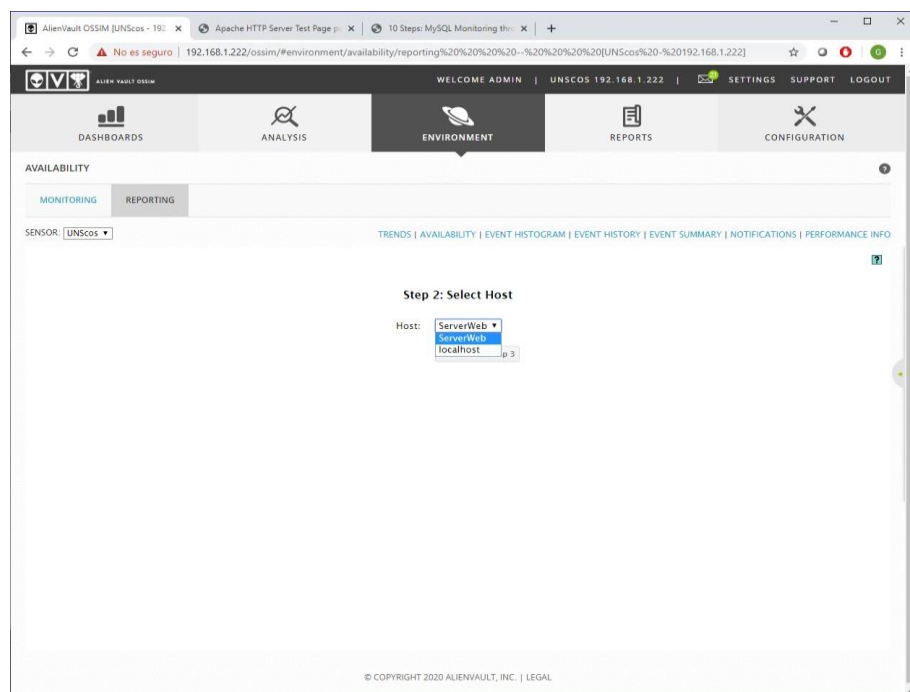


Figura 85. Seleccionando el Servidor del cual se hará el Reporte

Fuente: Propia

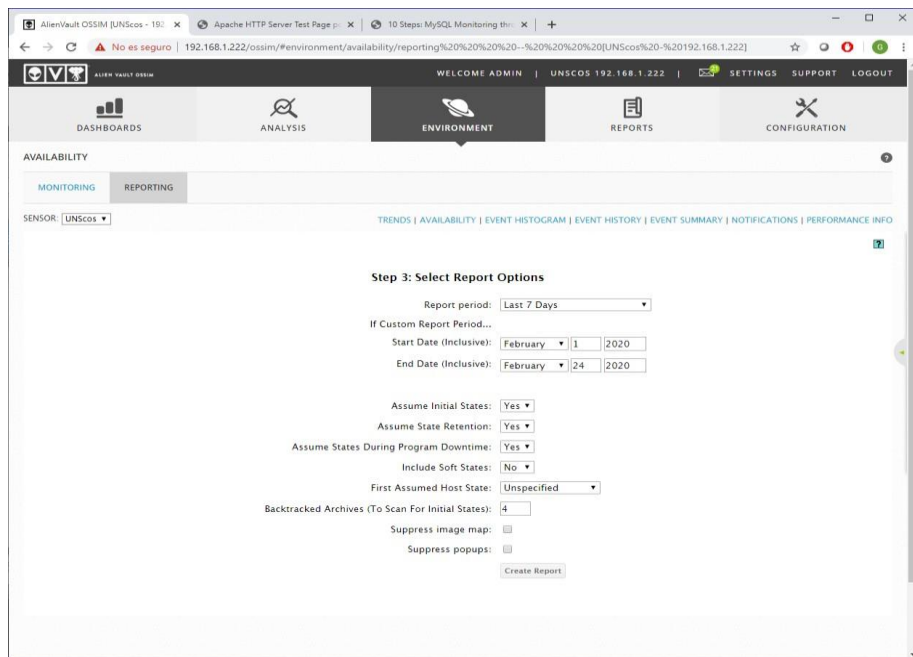


Figura 86. Configurar las Opciones del Reporte

Fuente: Propia

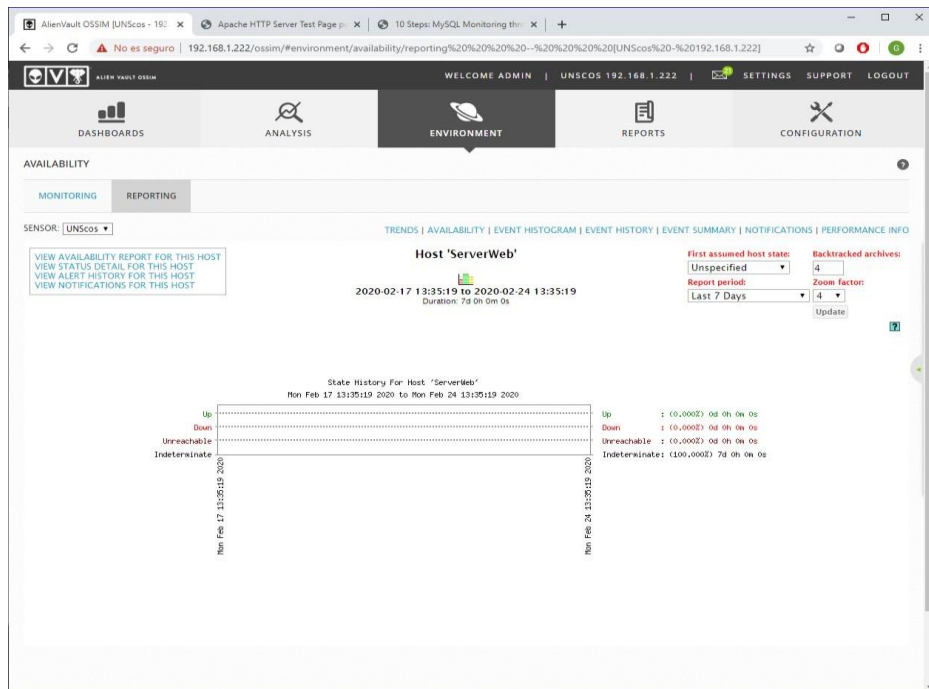


Figura 87. Visualizando el Reporte en un Lapso de Tiempo

Fuente: Propia

También se puede mostrar en el Reporte la historia de eventos sucedidos a través del tiempo, mostrándose picos donde ocurrió algún evento crítico.

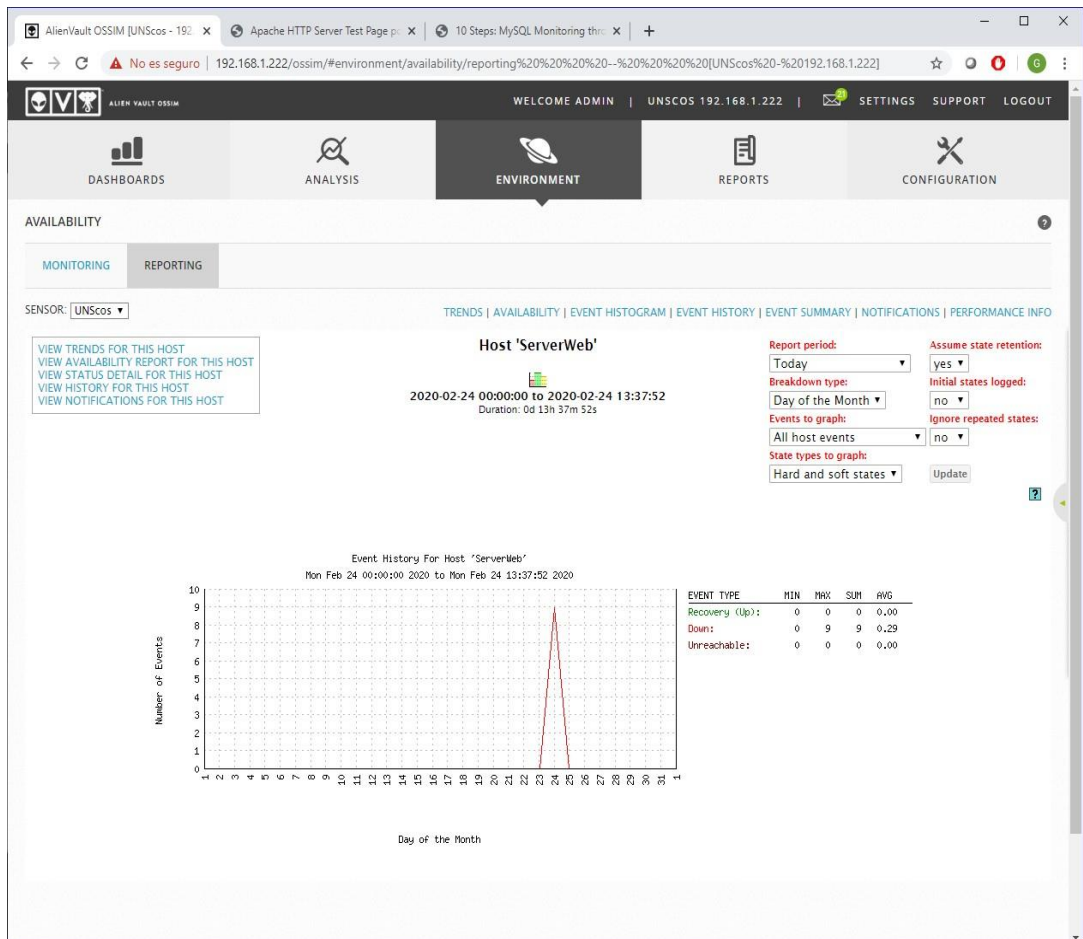


Figura 88. Visualizando un Histograma de Eventos

Fuente: Propia

Para establecer el mapa real de la institución, seleccionamos la opción Administración de Mapas, y dentro buscamos la opción Cargar un Nuevo Mapa.

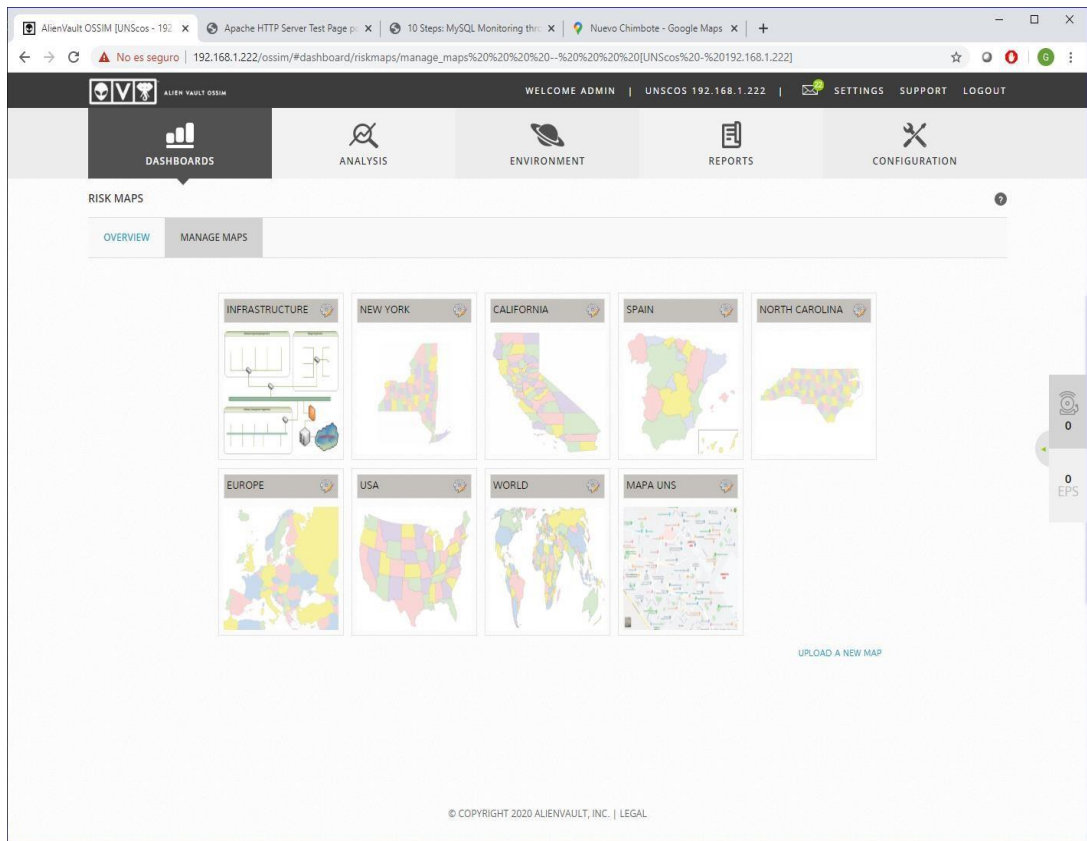


Figura 90. Configuración de Mapa Real de acuerdo a la Institución

Fuente: Propia

Se Selecciona el Mapa de Nuevo Chimbote, donde está ubicado la Universidad Nacional del Santa, tanto el Campus 1, Campus 2 y Rectorado.

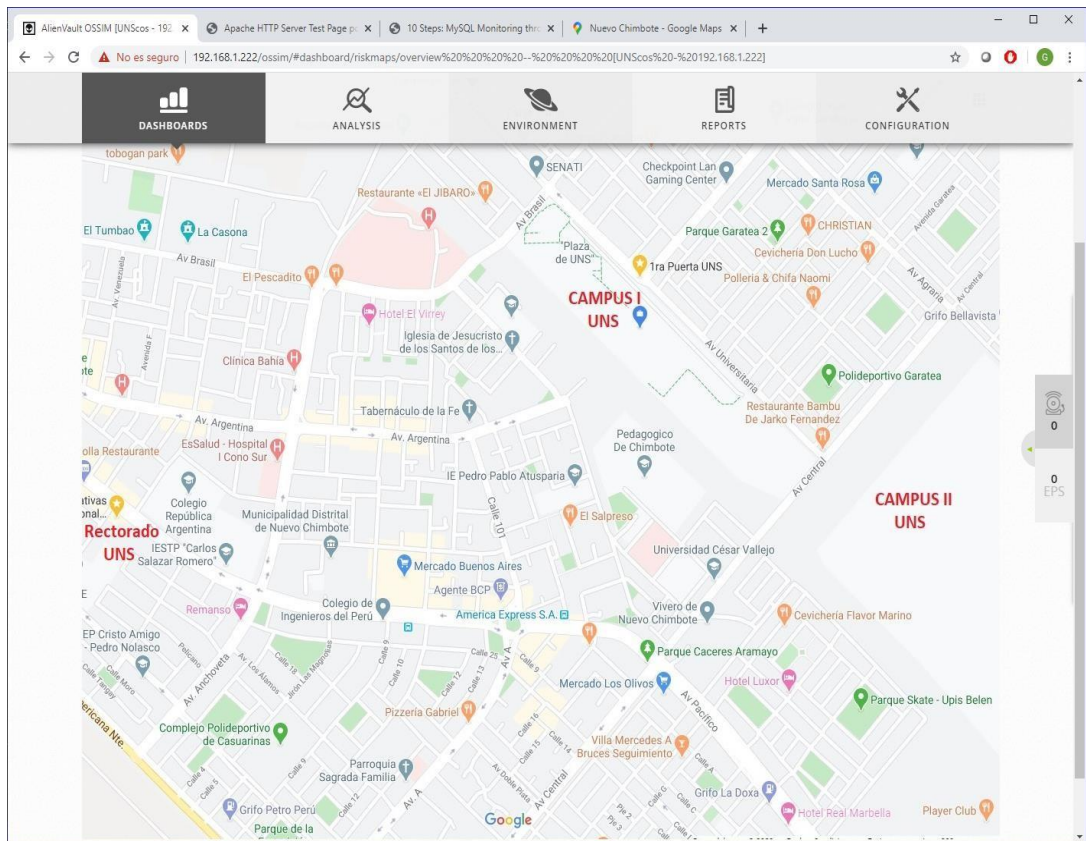


Figura 91. Cargando el Mapa de Nuevo Chimbote

Fuente: Propia

Eventos SIEM

También se puede realizar un análisis de los eventos ocurridos en la red informática, de acuerdo a los activos monitoreados.

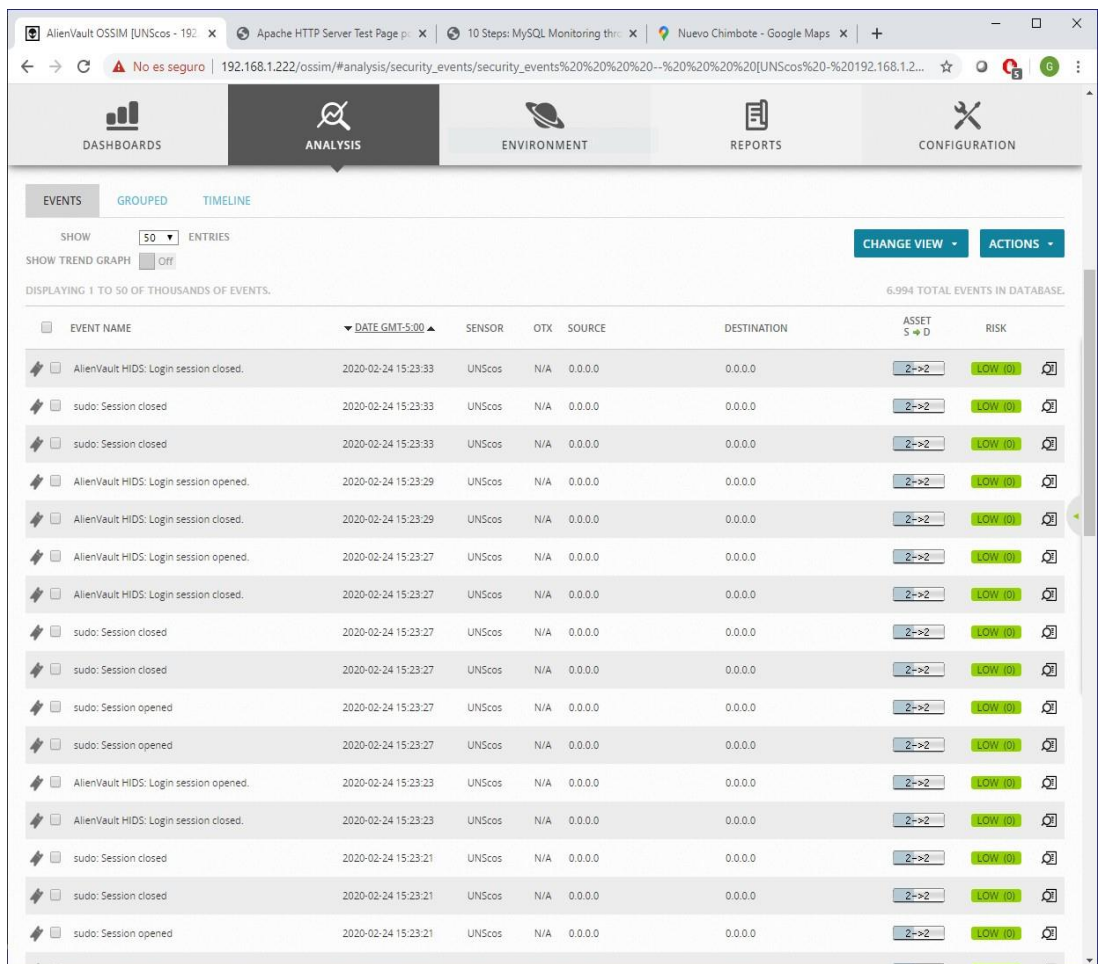
Se debe configurar de acuerdo a los parámetros dentro de un lapso de tiempo determinado.

The screenshot displays the AlienVault OSSIM web interface. The top navigation bar includes 'DASHBOARDS', 'ANALYSIS', 'ENVIRONMENT', 'REPORTS', and 'CONFIGURATION'. The main content area is titled 'SECURITY EVENTS (SIEM)' and features a search bar and several filter sections. The 'SHOW EVENTS' section has radio buttons for 'Last Day', 'Last Week', 'Last Month', and 'Date Range'. The 'DATA SOURCES', 'ASSET GROUPS', 'OTX IP REPUTATION', 'DATA SOURCE GROUPS', 'NETWORK GROUPS', 'OTX PULSE', 'SENSORS', and 'RISK' sections contain dropdown menus. A 'CLEAR FILTERS' button is visible. At the bottom, a table displays event data with columns for 'EVENT NAME', 'DATE GMT-5:00', 'SENSOR', 'OTX', 'SOURCE', 'DESTINATION', 'ASSET', and 'RISK'. The table shows one event: 'AlienVault HIDS: Login session closed.' with a risk level of 'LOW (0)'.

Figura 93. Configurando los Parámetros para mostrar Eventos SIEM

Fuente: Propia

Luego de ejecutar la consulta de acuerdo a los parámetros de configuración, se va a mostrar los eventos, ordenados por fecha y hora, tipo de sensor, el origen del evento, el destino del evento, nivel de riesgo.



The screenshot displays the AlienVault OSSIM web interface. The top navigation bar includes 'DASHBOARDS', 'ANALYSIS' (selected), 'ENVIRONMENT', 'REPORTS', and 'CONFIGURATION'. Below this, there are tabs for 'EVENTS', 'GROUPED', and 'TIMELINE'. The main content area shows a table of events with columns for 'EVENT NAME', 'DATE GMT-5:00', 'SENSOR', 'OTX', 'SOURCE', 'DESTINATION', 'ASSET S → D', and 'RISK'. The table lists various events such as 'AlienVault HIDS: Login session closed.', 'sudo: Session closed', and 'AlienVault HIDS: Login session opened.' Each row includes a risk level indicator (e.g., 'LOW (0)') and an action icon.

EVENT NAME	DATE GMT-5:00	SENSOR	OTX	SOURCE	DESTINATION	ASSET S → D	RISK
AlienVault HIDS: Login session closed.	2020-02-24 15:23:33	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
sudo: Session closed	2020-02-24 15:23:33	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
sudo: Session closed	2020-02-24 15:23:33	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: Login session opened.	2020-02-24 15:23:29	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: Login session closed.	2020-02-24 15:23:29	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: Login session opened.	2020-02-24 15:23:27	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: Login session closed.	2020-02-24 15:23:27	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
sudo: Session closed	2020-02-24 15:23:27	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
sudo: Session closed	2020-02-24 15:23:27	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
sudo: Session opened	2020-02-24 15:23:27	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
sudo: Session opened	2020-02-24 15:23:27	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: Login session opened.	2020-02-24 15:23:23	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: Login session closed.	2020-02-24 15:23:23	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
sudo: Session closed	2020-02-24 15:23:21	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
sudo: Session closed	2020-02-24 15:23:21	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
sudo: Session opened	2020-02-24 15:23:21	UNScos	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)

Figura 94. Visualizando los Eventos de la Red Informática

Fuente: Propia

Se puede también mostrar los eventos en tiempo real, conforme vayan sucediendo en la red informática.

Aquí se va mostrando todos los eventos que se están dando en todos los activos de toda la red informática.

DATE	EVENT NAME	RISK	DATA SOURCE	SENSOR	OTX	SOURCE IP	DEST IP
2020-02-24 15:26:49	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:49	sudo: Session closed	0	sudo	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:41	AlienVault HIDS: Login session opened.	0	AlienVault HIDS-authentication_success	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:41	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:40	sudo: Session closed	0	sudo	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:40	sudo: Session opened	0	sudo	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:39	AlienVault HIDS: Login session opened.	0	AlienVault HIDS-authentication_success	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:39	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:39	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:39	sudo: Session closed	0	sudo	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:39	sudo: Session closed	0	sudo	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:38	sudo: Session closed	0	sudo	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:38	sudo: Session opened	0	sudo	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:38	sudo: Session opened	0	sudo	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:26:38	sudo: Session opened	0	sudo	UNSCos	N/A	0.0.0.0	0.0.0.0

Figura 95. Visualizando los Eventos en Tiempo Real

Fuente: Propia

Se va a probar el acceso al servidor OSIMM con un usuario inexistente, desde un terminal SSH, utilizando el usuario jimmy@192.168.1.222 con una clave no valida.

El servidor va a denegar el acceso, por no existir el usuario.

Y el sistema OSSIM inmediatamente lo va a detectar y reportar, pues puede ser un posible agente invasor a la red informática.

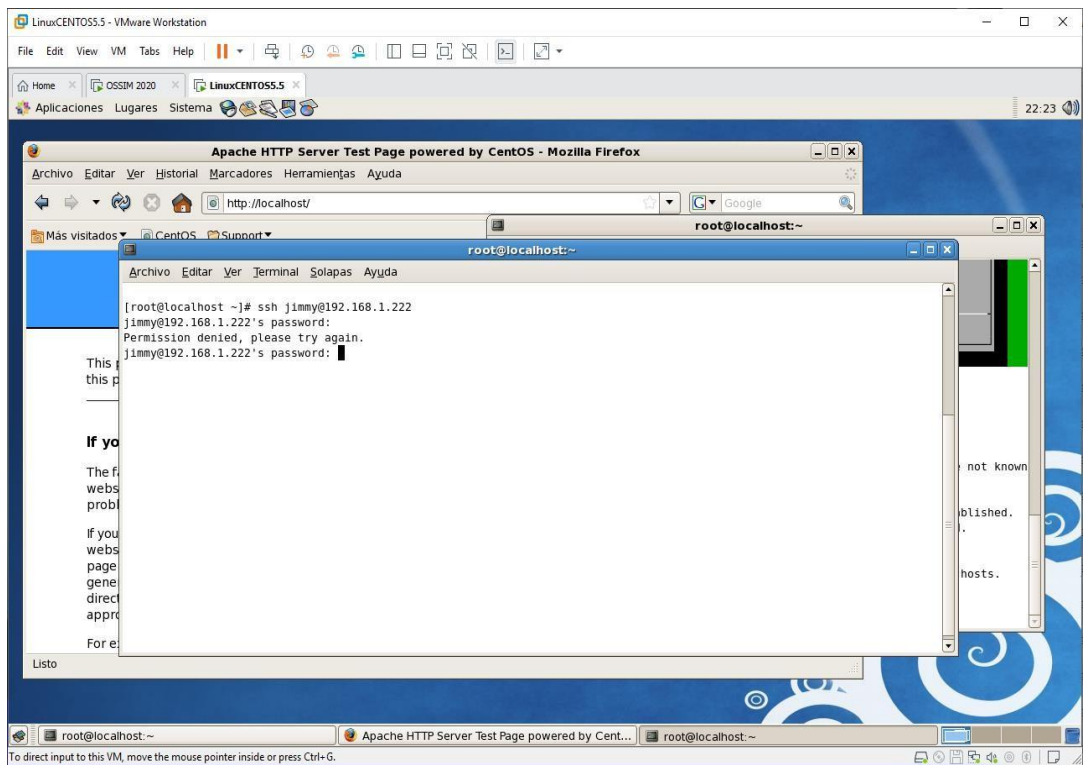
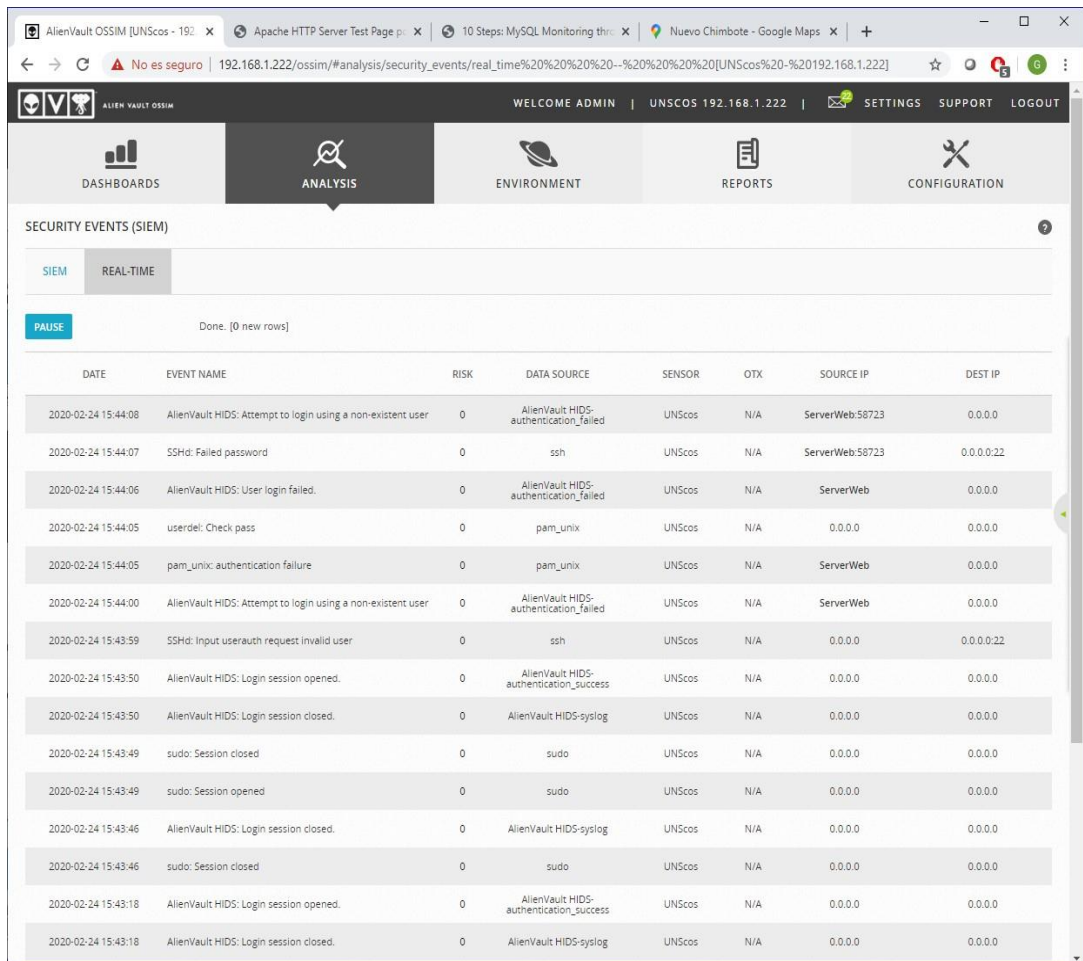


Figura 96. Tratando de acceder al Sistema OSSIM

Fuente: Propia

El Sistema OSSIM va a mostrar el evento ocurrido del intento fallido de acceso con un usuario inexistente.



The screenshot shows the AlienVault OSSIM interface. The top navigation bar includes 'WELCOME ADMIN', 'UNSCOS 192.168.1.222', and 'SETTINGS SUPPORT LOGOUT'. The main menu has 'DASHBOARDS', 'ANALYSIS', 'ENVIRONMENT', 'REPORTS', and 'CONFIGURATION'. The 'ANALYSIS' section is active, showing 'SECURITY EVENTS (SIEM)' with 'REAL-TIME' selected. A 'PAUSE' button and 'Done. [0 new rows]' are visible. The table below lists security events with columns for DATE, EVENT NAME, RISK, DATA SOURCE, SENSOR, OTX, SOURCE IP, and DEST IP.

DATE	EVENT NAME	RISK	DATA SOURCE	SENSOR	OTX	SOURCE IP	DEST IP
2020-02-24 15:44:08	AlienVault HIDS: Attempt to login using a non-existent user	0	AlienVault HIDS-authentication_failed	UNSCos	N/A	ServerWeb:58723	0.0.0.0
2020-02-24 15:44:07	SSHD: Failed password	0	ssh	UNSCos	N/A	ServerWeb:58723	0.0.0.22
2020-02-24 15:44:06	AlienVault HIDS: User login failed.	0	AlienVault HIDS-authentication_failed	UNSCos	N/A	ServerWeb	0.0.0.0
2020-02-24 15:44:05	userdel: Check pass	0	pam_unix	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:44:05	pam_unix authentication failure	0	pam_unix	UNSCos	N/A	ServerWeb	0.0.0.0
2020-02-24 15:44:00	AlienVault HIDS: Attempt to login using a non-existent user	0	AlienVault HIDS-authentication_failed	UNSCos	N/A	ServerWeb	0.0.0.0
2020-02-24 15:43:59	SSHD: Input userauth request invalid user	0	ssh	UNSCos	N/A	0.0.0.0	0.0.0.22
2020-02-24 15:43:50	AlienVault HIDS: Login session opened.	0	AlienVault HIDS-authentication_success	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:43:50	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:43:49	sudo: Session closed	0	sudo	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:43:49	sudo: Session opened	0	sudo	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:43:46	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:43:46	sudo: Session closed	0	sudo	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:43:18	AlienVault HIDS: Login session opened.	0	AlienVault HIDS-authentication_success	UNSCos	N/A	0.0.0.0	0.0.0.0
2020-02-24 15:43:18	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	UNSCos	N/A	0.0.0.0	0.0.0.0

Figura 97. Se muestra el evento donde notifica de intento de acceso con usuario inexistente

Fuente: Propia

Dando click al evento, se puede mostrar información detallada, como la fecha, el sensor utilizado, la dirección ip, el protocolo, categoría, el origen y destino.

EVENT DETAIL
AlienVault HIDS: Attempt to login using a non-existent user

DATE	2020-02-24 22:45:17 GMT-5:00	CATEGORY	Authentication
ALIENVAULT SENSOR	UNSCos [192.168.1.222]	SUB-CATEGORY	Failed
DEVICE IP	192.168.1.222 [eth0]	DATA SOURCE NAME	AlienVault HIDS-authentication_failed
EVENT TYPE ID	5710	DATA SOURCE ID	7010
UNIQUE EVENT ID#	578111ea-94ba-000c-297c-e0563d4716be	PRODUCT TYPE	Authentication and DHCP
PROTOCOL	TCP	ADDITIONAL INFO	N/A

PRIORITY	RELIABILITY	RISK	OTX INDICATORS
1	1	LOW (0)	0

SOURCE		DESTINATION	
ServerWeb [192.168.1.250]		0.0.0.0	
Hostname: ServerWeb	Location: N/A	Hostname: N/A	Location: N/A
MAC Address: 00:0C:29:7A:51:CC	Context: N/A	MAC Address: N/A	Context: N/A
Port: 48402	Asset Groups: UNSred	Port: 0	Asset Groups: N/A
Latest update: N/A	Networks: Pvt_192	Latest update: N/A	Networks: N/A
Username & Domain: N/A	Logged Users: N/A	Username & Domain: N/A	Logged Users: N/A
Asset Value: 2	OTX IP Reputation: No	Asset Value: 2	OTX IP Reputation: No

DATE	EVENT	RELIABILITY	PROTOCOL	SENSOR	RISK	OTX INDICATORS
2020-02-24 22:45:10	userdel: Check pass	0	pam_unix	UNSCos	N/A	0.0.0.0
2020-02-24 22:45:09	AlienVault HIDS: Attempt to login using a non-existent user	0	AlienVault HIDS-authentication_failed	UNSCos	N/A	ServerWeb:48402
2020-02-24 22:45:09	SSHd: Failed password	0	ssh	UNSCos	N/A	ServerWeb:48402
2020-02-24 22:45:07	AlienVault HIDS: User login failed.	0	AlienVault HIDS-authentication_failed	UNSCos	N/A	ServerWeb
2020-02-24 22:45:07	userdel: Check pass	0	pam_unix	UNSCos	N/A	0.0.0.0
2020-02-24 22:45:07	pam_unix: authentication failure	0	pam_unix	UNSCos	N/A	ServerWeb
2020-02-24 22:45:03	AlienVault HIDS: Attempt to login using a non-existent user	0	AlienVault HIDS-authentication_failed	UNSCos	N/A	ServerWeb

Figura 98. Información Detallada del Evento

Fuente: Propia

Asimismo, se puede mostrar información del evento en archivo log, el que se puede enviar a la central para soporte técnico.

The screenshot displays the AlienVault OSSIM web interface. A modal window titled "EVENT DETAIL" is open, showing information for a security event. The event source is "ServerWeb [192.168.1.250]" and the destination is "0.0.0.0". The event details include:

SOURCE	DESTINATION
Hostname: ServerWeb	Hostname: N/A
MAC Address: 00:0C:29:7A:51:CC	MAC Address: N/A
Port: 48402	Port: 0
Asset Groups: UNSred	Asset Groups: N/A
Latest update: N/A	Latest update: N/A
Username & Domain: N/A	Username & Domain: N/A
Asset Value: 2	Asset Value: 2
Location: N/A	Location: N/A
Context: N/A	Context: N/A
Networks: Pvt_192	Networks: N/A
Logged Users: N/A	Logged Users: N/A
OTX IP Reputation: No	OTX IP Reputation: No

Below the event details, there is a "RAW LOG" section showing the following log entry:

```
AV - Alert - "1582602317" --> RID: "5710"; RL: "5"; RG: "syslog,sshd,invalid_login,authentication_failed,"; RC: "Attempt to login using a non-existent user"; USER: "None"; SRCIP: "192.168.1.250"; HOSTNAME: "UNSCos"; LOCATION: "/var/log/auth.log"; EVENT: "[IN IT] Feb 24 22:45:16 UNSCos sshd[5173]: Failed password for invalid user jimmy from 192.168.1.250 port 48402 ssh2[END]";
```

The background shows a list of security events with columns for time, user, action, severity, and source/destination.

Figura 99. Información Detallada del Evento mostrado en modo log

Fuente: Propia

También se pueden mostrar los eventos agrupados, ordenados de acuerdo a su nombre, al origen, al destino, a la fecha, etc.

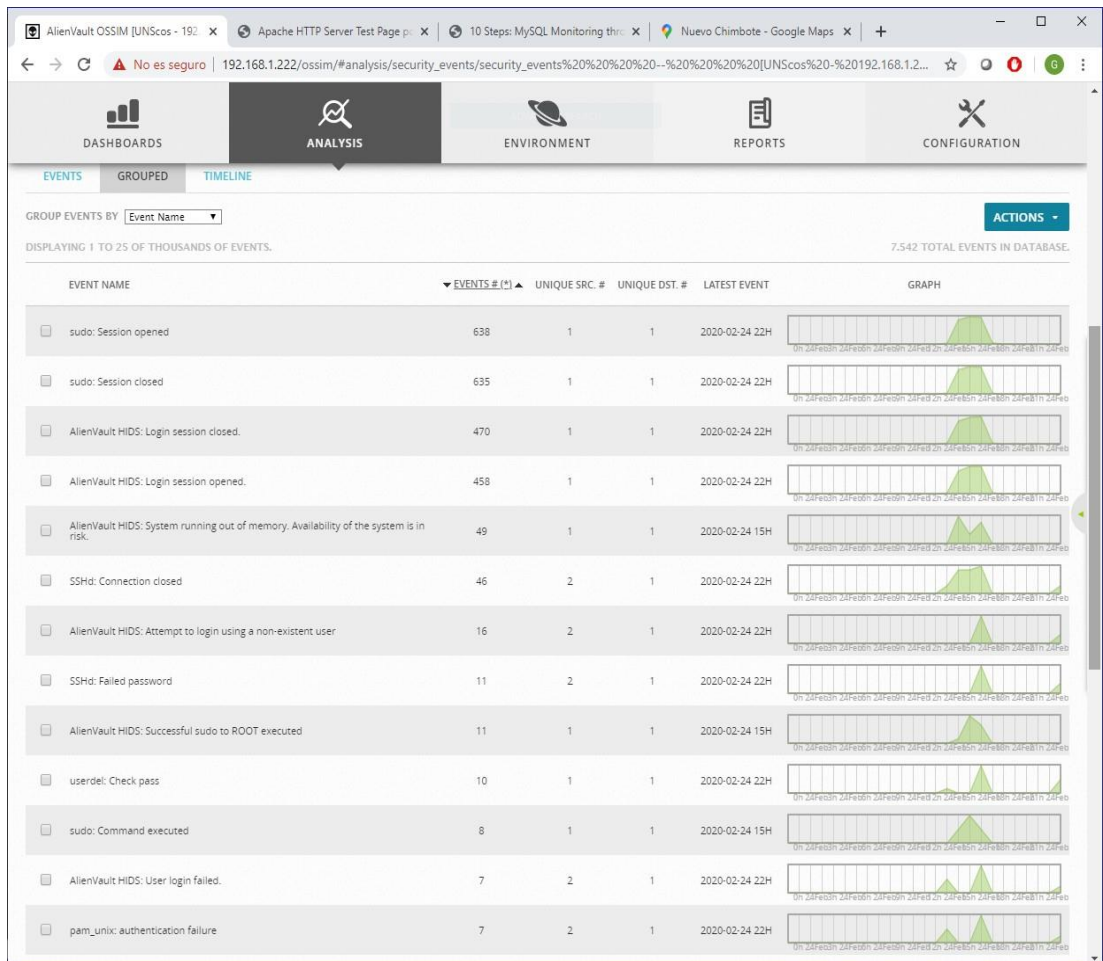


Figura 100. Visualizando los Eventos Agrupados

Fuente: Propia

Filtrando por Equipo 192.168.1.250

Ante tanta cantidad de eventos que se van generando en la red informática, se puede realizar un filtro por la dirección ip, para solo tenerlos los eventos ocurridos en un host o servidor determinado.

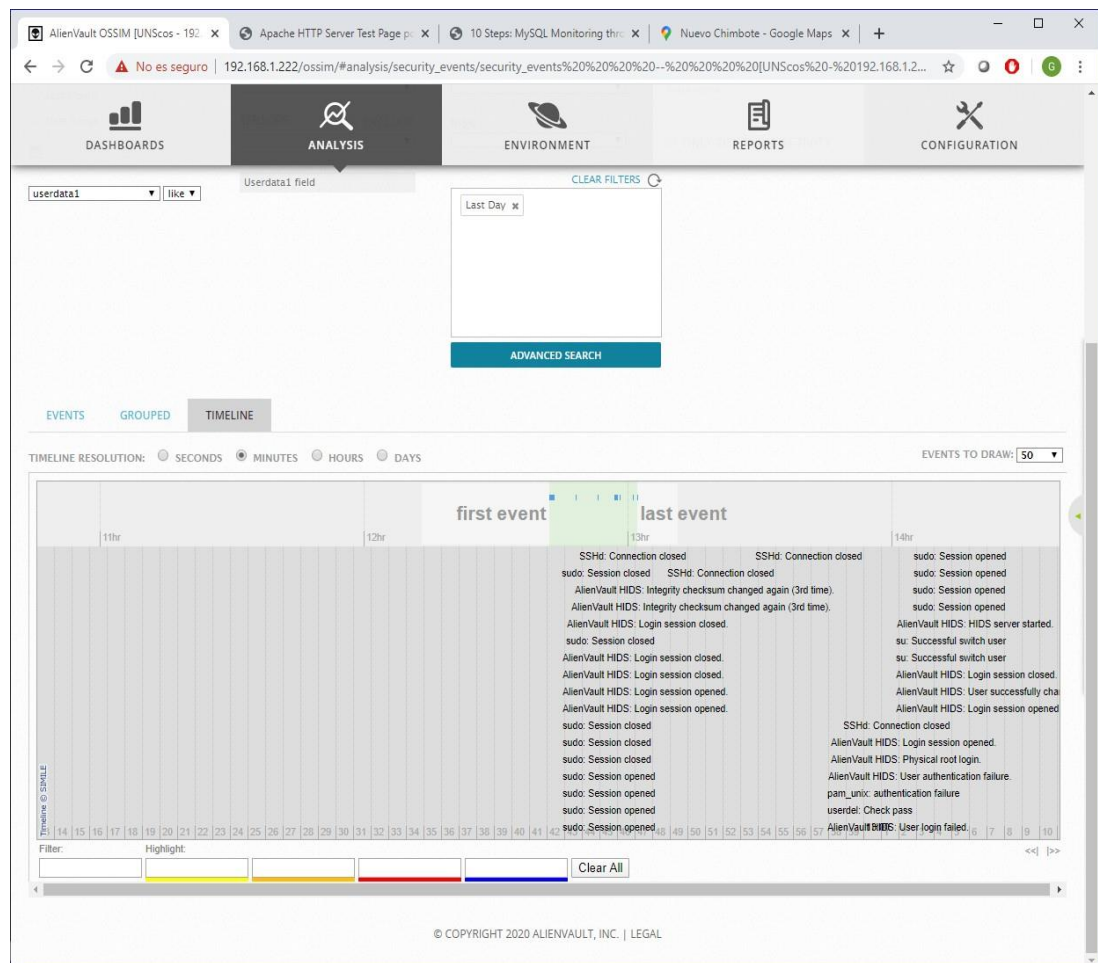


Figura 101. Configurando el Filtro de los Eventos

Fuente: Propia

Aquí se muestran los eventos ocurridos en el host 192.168.1.250 (Servidor Web), ordenados por la fecha y hora de ocurrencia.

EVENT NAME	DATE GMT-5:00	SENSOR	OTX	SOURCE	DESTINATION	ASSET ID	RISK
AlienVault HIDS: Attempt to login using a non-existent user	2020-02-24 22:45:17	UNScos	N/A	ServerWeb:48402	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: User missed the password more than one time	2020-02-24 22:45:17	UNScos	N/A	ServerWeb	0.0.0.0	2->2	LOW (0)
SSHd: Connection closed	2020-02-24 22:45:16	UNScos	N/A	ServerWeb	0.0.0.22	2->2	LOW (0)
pam_unix: X more authentication failures	2020-02-24 22:45:16	UNScos	N/A	ServerWeb	0.0.0.0	2->2	LOW (0)
SSHd: Failed password	2020-02-24 22:45:16	UNScos	N/A	ServerWeb:48402	0.0.0.22	2->2	LOW (0)
AlienVault HIDS: Attempt to login using a non-existent user	2020-02-24 22:45:13	UNScos	N/A	ServerWeb:48402	0.0.0.0	2->2	LOW (0)
SSHd: Failed password	2020-02-24 22:45:12	UNScos	N/A	ServerWeb:48402	0.0.0.22	2->2	LOW (0)
SSHd: Failed password	2020-02-24 22:45:09	UNScos	N/A	ServerWeb:48402	0.0.0.22	2->2	LOW (0)
AlienVault HIDS: Attempt to login using a non-existent user	2020-02-24 22:45:09	UNScos	N/A	ServerWeb:48402	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: User login failed.	2020-02-24 22:45:07	UNScos	N/A	ServerWeb	0.0.0.0	2->2	LOW (0)
pam_unix: authentication failure	2020-02-24 22:45:07	UNScos	N/A	ServerWeb	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: Attempt to login using a non-existent user	2020-02-24 22:45:03	UNScos	N/A	ServerWeb	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: SSHD authentication success.	2020-02-24 22:42:47	UNScos	N/A	ServerWeb:48400	0.0.0.0	2->2	LOW (0)
SSHd: Login successful, Accepted password	2020-02-24 22:42:46	UNScos	N/A	ServerWeb:48400	0.0.0.22	2->2	LOW (0)
AlienVault HIDS: User missed the password more than one time	2020-02-24 15:58:08	UNScos	N/A	ServerWeb	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: Attempt to login using a non-existent user	2020-02-24 15:58:08	UNScos	N/A	ServerWeb:57591	0.0.0.0	2->2	LOW (0)

Figura 102. Visualizando los Eventos Filtrados por el Host 192.168.1.250

Fuente: Propia

Las alertas de amenazas se dan a nivel mundial, por lo cual el Sistema OSSIM tiene una base de datos de eventos y amenazas dados a nivel mundial, al cual se puede acceder utilizando una cuenta OTX.

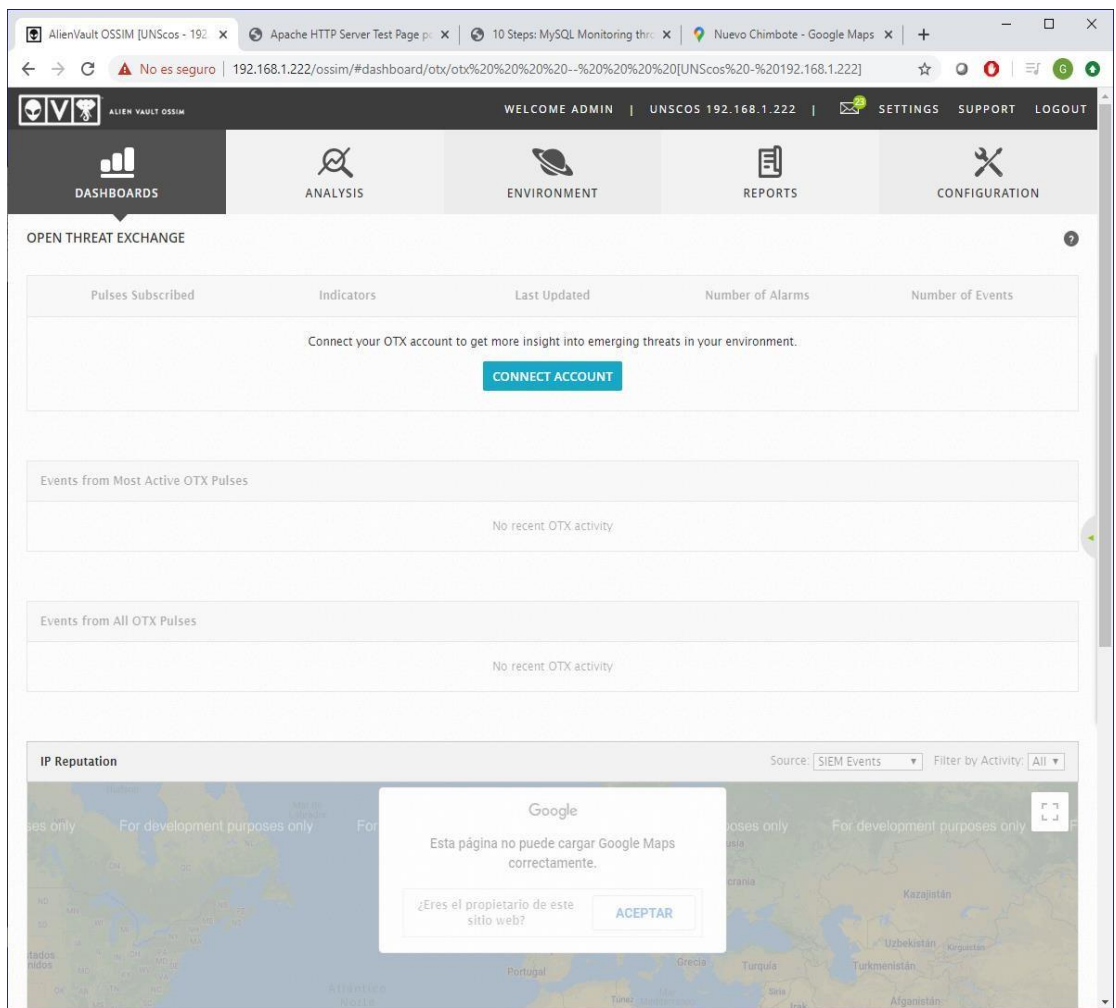


Figura 103. Ingresando a Visualizar Amenazas a nivel Mundial

Fuente: Propia

Se necesita una Cuenta OTX, que puede ser de prueba o una ya adquirida.

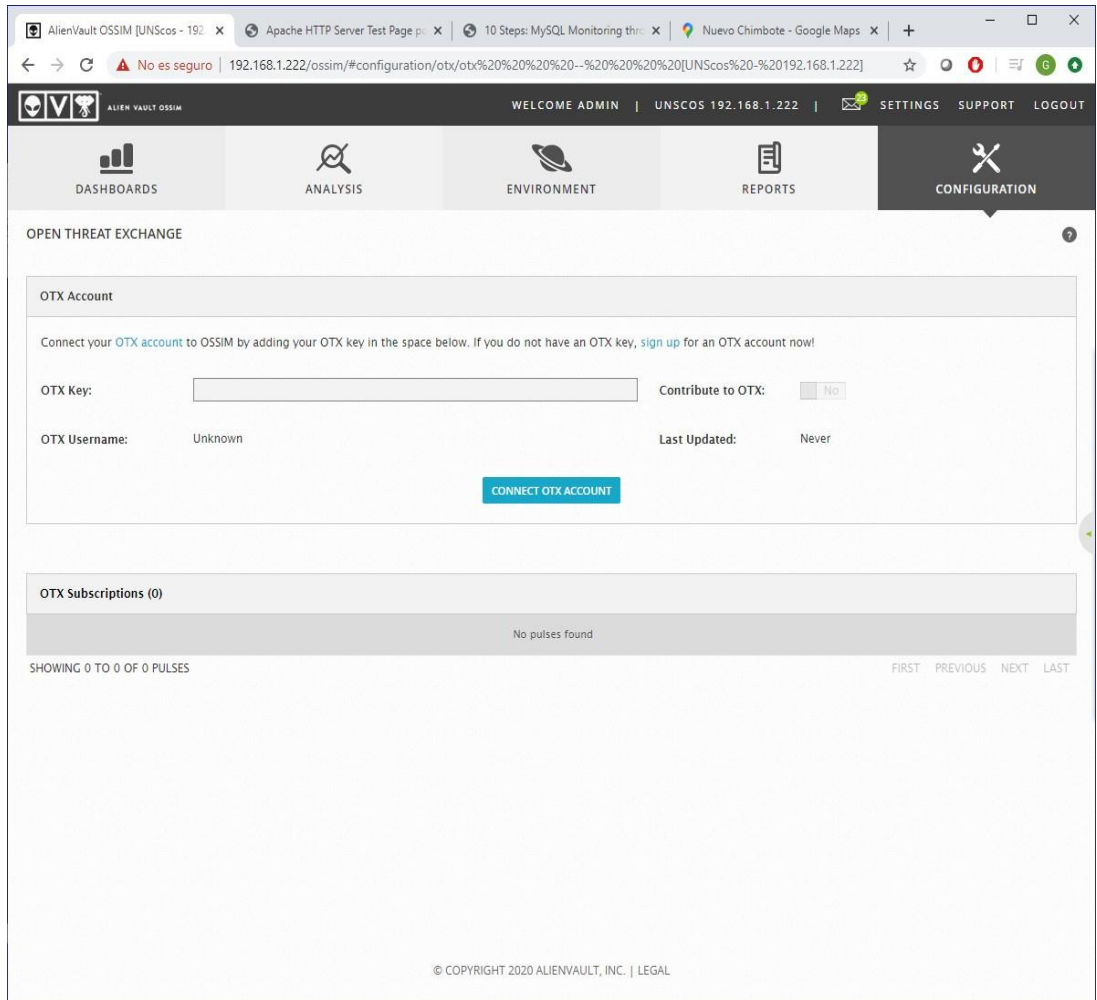


Figura 104. Ingresando la Cuenta OTX

Fuente: Propia

Se tiene acceso a las amenazas a nivel mundial por países, que nos sirve de referencia para conocer las amenazas que estamos recibiendo en nuestra red informática.

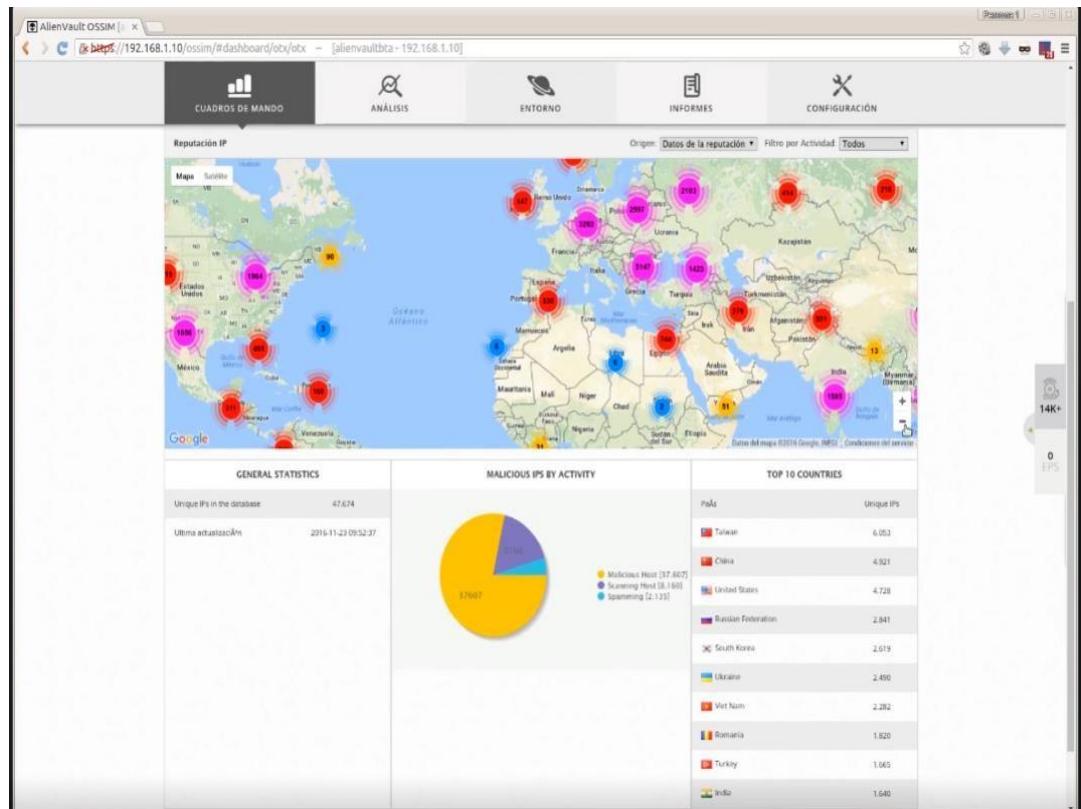


Figura 105. Visualizando las Amenazas a Nivel Mundial Registradas

Fuente: Propia

Alarmas

Se puede realizar un análisis de las alarmas activadas durante un lapso de tiempo, pudiendo ser: Sistema Comprometido, Explotación e Instalaciones, Entrega y Ataques, Reconocimientos y Pruebas.

The screenshot displays the AlienVault OSSIM interface for configuring alarms. The top navigation bar includes 'DASHBOARDS', 'ANALYSIS' (selected), 'ENVIRONMENT', 'REPORTS', and 'CONFIGURATION'. Below this, the 'ALARMS' section is active, showing 'LIST VIEW' and 'GROUP VIEW' tabs. A search and filter section is present, with fields for Sensor, Alarm Name / ID, Source IP Address, Destination IP Address, Date, Asset Group, Intent, Directive ID, Contains the Event Type, Number of events in alarms, Risk level in alarms, Label, and OTX Pulse. There are also checkboxes for 'Only OTX Pulse Activity', 'Do not resolve ip names', 'Hide closed alarms', and 'Beep on new alarm'. A 'SEARCH' button is located below the search and filter section. At the bottom, there is a calendar view showing a 31-day period from 10-02-20 to 20-02-26, with icons for System Compromise, Exploitation & Installation, Delivery & Attack, and Reconnaissance & Probing.

Figura 106. Configurando las Alarmas

Fuente: Propia

Se puede establecer ticket a las alertas, para luego ser evaluados y probados.

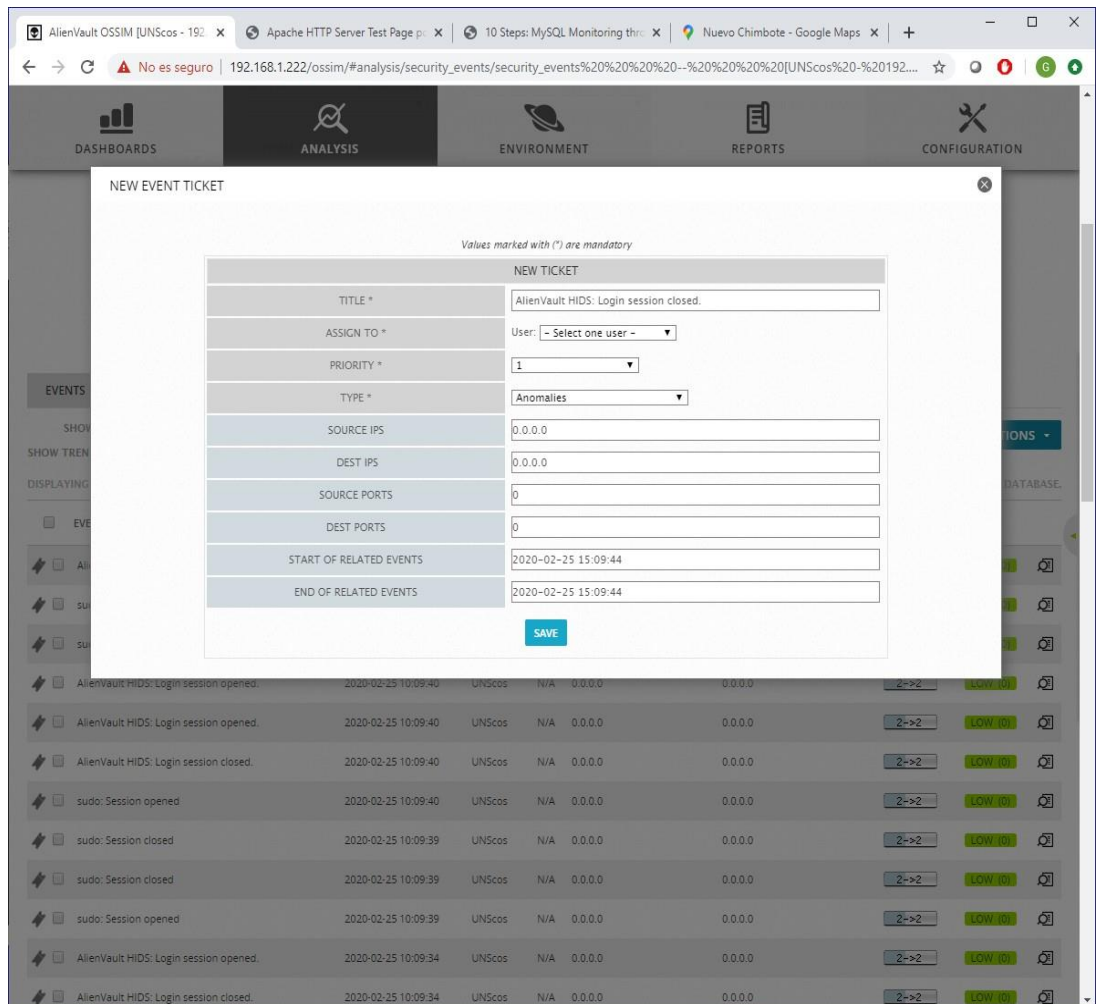


Figura 107. Asignando un Ticket a una Alerta

Fuente: Propia

Se puede visualizar todos los ticket generados, para una posterior revisión.

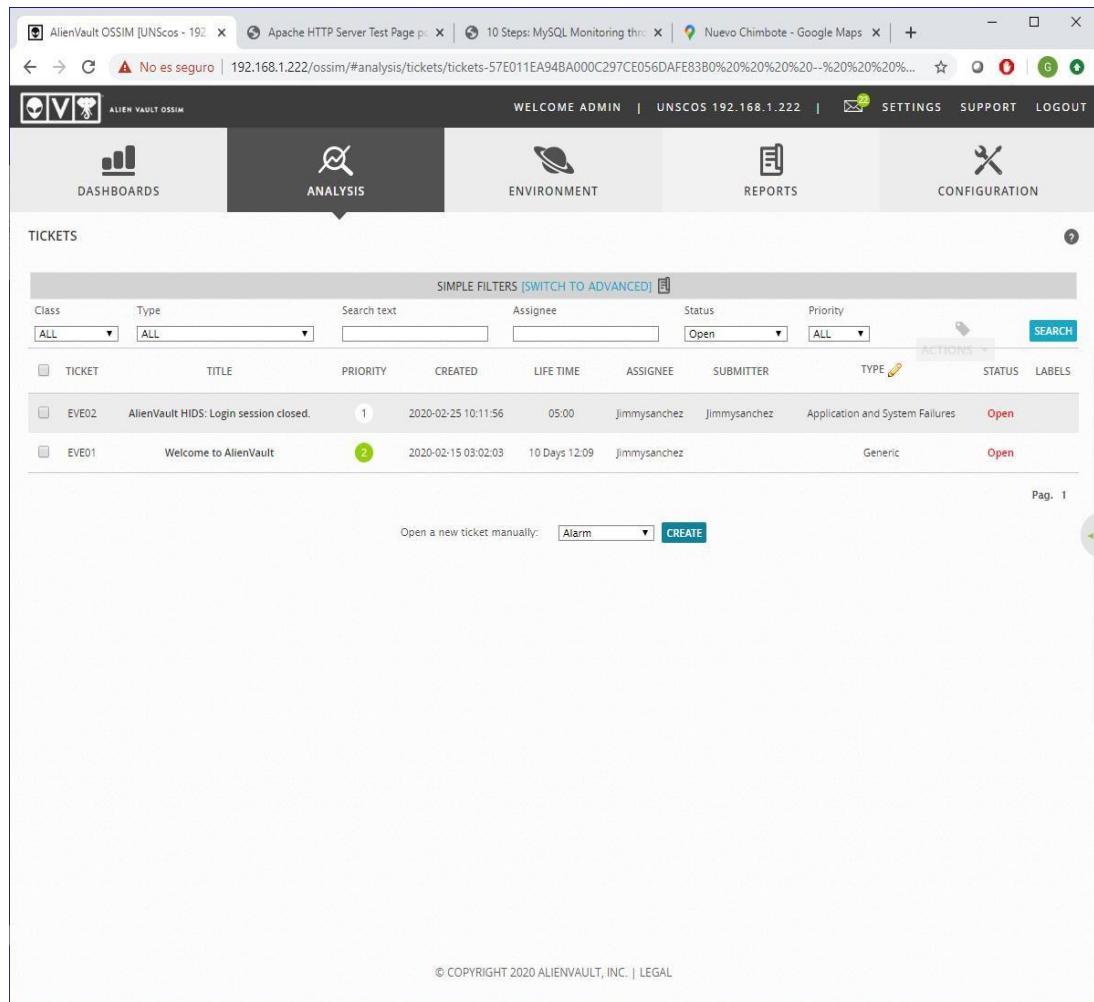


Figura 108. Listado de Tickets Generados en las Alertas

Fuente: Propia

5.6. LOGROS DEL CENTRO DE OPERACIONES DE SEGURIDAD

Luego de implementar el Centro de Operaciones de Seguridad basado en el software OSSIM, que se instaló en un servidor Virtual dentro de la Sala de Servidores y desde donde se realiza el monitoreo de la red informática, se pudo detectar los riesgos existentes en todos los activos, y asimismo se van mostrando los eventos y alertas durante el tiempo que dura el monitoreo.

De acuerdo a la información que se muestra en línea y en tiempo real, se puede tomar las medidas necesarias para corregirlos y mantener el servicio en la red informática de la UNS.

El Centro de Operaciones de Seguridad necesita contar con hardware independiente y un ambiente con personal a dedicación exclusiva, para responder en forma inmediata a los problemas de seguridad.

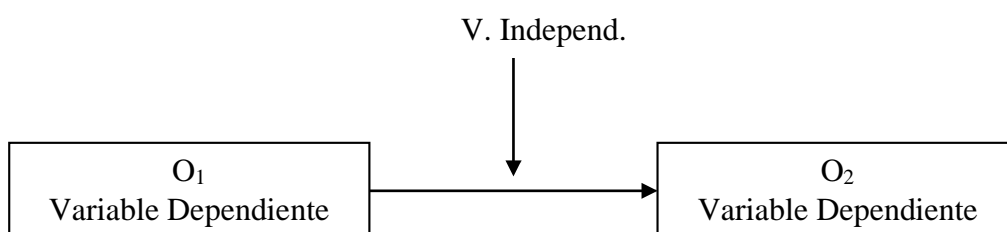
Cada día hay más amenazas en las redes, sobre todo si se está conectado a internet, por lo cual este sistema podrá darnos una respuesta rápida a los riesgos existentes.

CAPITULO VI

DISCUSIÓN

6.1. CONTRASTACIÓN DE LA HIPÓTESIS

Para efectos de la Contrastación de la hipótesis propuesta en la presente investigación se utilizó el modelo de sucesión en línea.



La implementación de un Centro de Operaciones de Seguridad (COS) Mejora la Seguridad en la Red Informática de la Universidad Nacional del Santa.

Dónde:

I = Implementación de un Centro de Operaciones de Seguridad (COS).

D = Seguridad en la Red Informática de la Universidad Nacional del Santa.

Estímulo = Tiempo de Respuesta, Fallas de Seguridad, Toma de Decisiones.

A través de esto se evaluó la variable dependiente, en este caso la Seguridad en la Red Informática de la UNS, en base a los efectos de la aplicación de la variable independiente, que está representada por la Implementación de un Centro de Operaciones de Seguridad (COS).

6.2. EVALUACIÓN DE INDICADORES

Para la evaluación de los efectos, en la variable dependiente con respecto a la variable independiente, usamos tres indicadores, como son:

- **Tiempo de Respuesta**
- **Fallas de Seguridad**
- **Tomas de Decisiones Oportunas**

A continuación, se muestran los resultados de la evaluación de los indicadores.

TIEMPO DE RESPUESTA: RANGO [10 mejor – 5 regular – 0 peor]

Indicadores	Tiempo de Respuesta	
	Sin la Solución	Con la Solución
Demora en reiniciar los servidores	2	9
Detección de Amenazas	2	9
Identificación de Riesgos en los servicios	3	9
Detección de Malware	2	9
Detección de brechas de seguridad	2	9
Promedio Final	11	45

Fuente: Datos de Pruebas realizadas en campo.

Interpretación

El resultado obtenido luego de las pruebas realizadas, nos permite apreciar que con el Centro de Operaciones de Seguridad se mejora el tiempo de respuesta

ante las amenazas y brechas de seguridad, ya que existe un existe un monitoreo en tiempo real.

FALLAS DE SEGURIDAD: RANGO [10 mejor – 0 peor]

Indicadores	Fallas de Seguridad	
	Sin Solución	Con Solución
Detección de Malware	4	8
Detección de Amenazas	3	8
Detección de Brechas de Seguridad	3	9
Detección de Ataques	2	8
Detección de Caídas de Servidores	3	9
Promedio Final	15	42

Fuente: Datos de Pruebas realizadas en campo.

Interpretación

El Centro de Operaciones de Seguridad (COS) permite detectar en tiempo real las fallas de seguridad como malware, brechas, amenazas, ataques y caídas de servidores; por lo cual su implementación permite reducir los fallos de seguridad en forma inmediata a través de la central. Esto es beneficioso para la red informática de la Universidad Nacional del Santa.

TOMA DE DECISIONES OPORTUNAS: RANGO [10 mejor – 0 peor]

Indicadores	Tomas de Decisiones Oportunas	
	Sin Solución	Con Solución
Eliminar Malware en la Red Informática	4	8
Reducir las Brechas/amenazas encontradas	3	8
Reiniciar los Servidores	4	8
Actualizar softwares en los Servidores	3	8
Repeler ataques informáticos	3	8
Promedio Final	17	40

Fuente: Datos de Pruebas realizadas en campo.

Interpretación

El uso del Centro de Operaciones de Seguridad (COS) permite tomar decisiones en forma oportuna ante los diferentes ataques o amenazas que afecten a los activos de la red informática. Esto es porque el monitoreo se realiza en tiempo real. El administrador podrá conocer los problemas en forma inmediata y determinar la mejor solución.

6.3. CONCLUSIÓN

Por los resultados de los tres indicadores de evaluación, se puede inducir y determinar que la implementación del Centro de Operaciones de Seguridad mejora la seguridad en la Red Informática de la Universidad Nacional del Santa.

CONCLUSIONES

1. Se implementó el Centro de Operaciones de Seguridad (COS) en la Red Informática de la Universidad Nacional del Santa, configurando un Servidor OSSIM en una máquina virtual, realizando el monitoreo de los activos de la red de acuerdo a la configuración planteada, logrando la detección en tiempo real de las amenazas y fallas de seguridad.
2. Se identificaron los riesgos existentes en la red informática de la Universidad Nacional del Santa, ubicándose los activos con que se cuenta y los servicios que ejecuta, configurándose su monitoreo en tiempo real para una detección inmediata.
3. Se analizó la red informática de la Universidad Nacional del Santa, estableciendo los requisitos que tendría el Centro de Operaciones de Seguridad, debiendo encontrarse enlazado en forma centralizada en la red y detectar los activos presentes en la red informática.
4. El Diseño del Centro de Operaciones de Seguridad establece que deberá implementarse en el Centro de Datos de la UNS, instalando el software OSSIM en una máquina virtual.
5. Se construyó el prototipo del Centro de Operaciones de Seguridad en una máquina virtual utilizando el software OSSIM, donde se configuró los activos y los servicios a ser monitoreados en la red informática de la UNS.

RECOMENDACIONES

1. Realizar capacitación al personal de la universidad del área de tecnologías de la información para la operación del Sistema OSSIM y de la tecnología de Centro de Operaciones de Seguridad.
2. Se debe adquirir equipos informáticos para dedicarlo en forma exclusiva para servidor OSSIM y pueda realizar el monitoreo y control de la carga de trabajo en la Red Informática de la UNS.
3. Realizar reportes periódicos sobre las detecciones realizadas y en base a eso realizar mantenimientos preventivos de los softwares instalados en los diferentes servidores y hosts de la red informática.

BIBLIOGRAFÍA

a) BIBLIOGRAFÍA BÁSICA

1. Hernandez R., Fernandez C. y Baptista P. (1991), Metodología de la Investigación, México, McGraw - Hill Interamericana de México.
2. Bernal Torres, Cesar Augusto. (2000) Metodología de la Investigación para Administración y Economía. Santa fe de Bogotá, Colombia. Pearson Educación de Colombia Ltda.
3. Rivas Galarreta, Enrique. (1995). Metodología de la Investigación Bibliográfica. Perú: Ed. Trujillo. 2da Edición.

b) BIBLIOGRAFÍA ESPECIALIZADA

1. Agesic. (8 de Diciembre de 2017). *agesic.gub.uy*. Obtenido de Agesic: <https://www.agesic.gub.uy/agesicweb/plantillas/imprimir.jsp?contentid=6672&channel=agesic&site=1>
2. Aguilera López, P. (2011). *Seguridad Informática*. Madrid, España: Editex.
3. Biggeri, P. H. (2018). *Centro de operaciones de seguridad. Estrategia, diseño y gestión*. Buenos Aires: Universidad de Buenos Aires.
4. Cisco. (06 de Mayo de 2019). *Cisco's Technology News Site*. Obtenido de The Network: <https://newsroom.cisco.com/overview>
5. Editorial CEP. (2017). *AUXILIAR DE LA FUNCIÓN ADMINISTRATIVA* (octubre 2017 ed., Vol. II). Madrid, España: CEP S.L.
6. EFE, E. (Dirección). (2014). *Securitas presenta en Sicur su nuevo Centro de Operaciones y Servicios (COS)* [Película].
7. ElevenPaths (Dirección). (2016). *SOC de Telefónica (Centro de Operaciones de Seguridad)* [Película].
8. España, I. (Dirección). (2018). *Simulador Virtual del Centro de Operaciones de Seguridad de IBM* [Película].

9. Ferro Veiga, José Manuel;. (2020). *Gestor en Seguridad Privada Integral*.
10. McAfee, C. (06 de Mayo de 2019). mcafee.com. Obtenido de McAfee:
<https://www.mcafee.com/es-mx/index.html>
11. Micro, T. (06 de Mayo de 2019). Trend Micro Inc. Obtenido de Trend Micro Inc: https://www.trendmicro.com/es_es/about.html
12. ORACLE. (s.f.). Oracle. Obtenido de <https://www.oracle.com>
13. Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzaty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades (Vol. 46 de Ingeniería y Tecnología)*. Ecuador: Area de Innovación y Desarrollo S.L 3Ciencias.
14. San Fernando, M. (Dirección). (2016). *Nuevo Centro de Operaciones de Seguridad [Película]*.
15. Symantec, C. (3 de Mayo de 2019). symantec.com. Obtenido de Symantec:
https://support.symantec.com/es_ES/article.HOWTO80985.html
16. UPADEC02. (29 de junio de 2012). scribd.com. Obtenido de <https://es.scribd.com/doc/18339909/Centro-de-Control-de-Seguridad>
17. Urbina Baca, G. (2016). *Introducción a la Seguridad Informática*. Mexico D.F.: Grupo Editorial Patria.

ANEXOS

ANEXO 01

ENCUESTA PARA EVALUAR EL CENTRO DE OPERACIONES DE SEGURIDAD EN SU IMPACTO EN LA SEGURIDAD INFORMÁTICA DE LA RED INFORMÁTICA DE LA UNS

COLOCAR UN VALOR DENTRO DEL RANGO: [10 mejor – 5 regular - 0 peor]

TIEMPO DE RESPUESTA

- 1) Tiempo de Reinicio de los Servidores:
- 2) Tiempo de Detección de Amenazas:
- 3) Tiempo de Identificación de Riesgos en los servicios:
- 4) Tiempo de Detección de Malware:
- 5) Tiempo de Detección de Brechas de Seguridad:

FALLAS DE SEGURIDAD

- 6) Detección de Malware:
- 7) Detección de Amenazas:
- 8) Detección de Brechas de Seguridad:
- 9) Detección de Ataques:
- 10) Detección de Caídas de Servidores:

TOMA DE DECISIONES OPORTUNAS

- 11) Eliminar Malwares detectados:
- 12) Reducir Brechas/Amenazas encontrados:
- 13) Reinicio de Servidores:
- 14) Actualizar software en los Servidores:
- 15) Repeler ataques informáticos:

METODOLOGIA OSSIM

1. Introducción.

Si lanzamos una mirada al pasado, podemos ver como poco a poco la capa tecnológica ha ido ocupando un espacio importante en las empresas y eso ha hecho que la tecnología evolucione de manera rápida y eficiente. Se puede ver como el campo de la seguridad informática ha evolucionado, desde los primeros cortafuegos hasta los más avanzados IDS (Sistemas de Detección de Intrusos).

Sin ninguna, duda hoy en día podemos encontrar en el mercado un amplio repertorio de aplicaciones de seguridad, cada una con un fin específico como son los cortafuegos, IDS, detectores de vulnerabilidades, programas de monitorización, detectores de anomalías, etc.

Sin embargo, esto tiene un coste que pocas empresas pueden soportar, porque no sólo requiere un gasto económico de software, sino que además se necesita de un personal técnico especializado, que emplee una gran cantidad de horas afrontando los miles de eventos que cada aplicación genera y que la mayoría de ellos son repetitivos o falsos positivos.

Las empresas que deciden realizar una inversión en proteger sus redes, adquieren numerosos dispositivos y pagan licencias con costes elevados. Y para su asombro, sedan cuenta que aun así se hace inviable gestionar la seguridad, ya que reciben miles de alertas, la mayoría de ellas falsos positivos y no saben cuál es el estado real de su red.

Mencionando las palabras de Julio Casal integrante en el diseño del sistema Ossim, haré

una clara descripción por el cual se ha creado este sistema: *“Nos sorprende que con el fuerte desarrollo tecnológico producido en los últimos años que nos ha provisto de herramientas con capacidades como la de los IDS, sea tan complejo desde el punto de vista de seguridad, obtener una foto de una red y obtener una información con un grado de abstracción que permita una revisión práctica y asumible”*. Estas necesidades fueron las causantes del proyecto Ossim.

Ossim no es una nueva aplicación de seguridad desarrollada, si no que han desarrollado una plataforma que integra las mejores aplicaciones de seguridad Open Source en una única interfaz, aprovechando lo mejor de cada una de ellas, e interrelacionándolas para obtener una información final mucho más fiable y detallada.

2. ¿Qué es Ossim?.

Ossim es la abreviatura de *Open Source Security Information Management System* (Sistema de gestión de la información de seguridad Open Source) desarrollado para gestionar la información de seguridad de una red. Es una distribución que integra más de 22 productos de seguridad todos ellos “Open Source” capaces de correlacionar entre ellos. Ossim es una plataforma compleja pero a su vez potente, ya que integra las soluciones de código libre de seguridad para la monitorización y detección de patrones de redes más conocidas (Snort, nessus, ntop, nmap, nagios, etc), integrándolas en una arquitectura abierta que se aprovechará de todas sus capacidades para aumentar la seguridad en las redes.

El objetivo de Ossim ha sido crear un framework capaz de recolectar toda la información de los diferentes plugins, para integrar e interrelacionar entre si y obtener una visualización única del estado de la red y con el mismo formato, con el objetivo de

aumentar la capacidad de detección de anomalías, priorizar los eventos según el contexto en el que se producen y mejorar la visibilidad de la monitorización del estado de la red actual.

El sistema Ossim se puede dividir en 3 capas:

El nivel mas bajo “*preprocesado*”, se compone por un número de detectores, monitores denominados preprocesadores, dispersados por la red, se encargan de realizar la detección y generación de alertas que posteriormente enviarán la información al sistema central para la colección y correlación de los diferentes eventos:

- IDS (detectores de patrones).
- Detectores de anomalías.
- Cortafuegos
- Varios tipos de Monitores

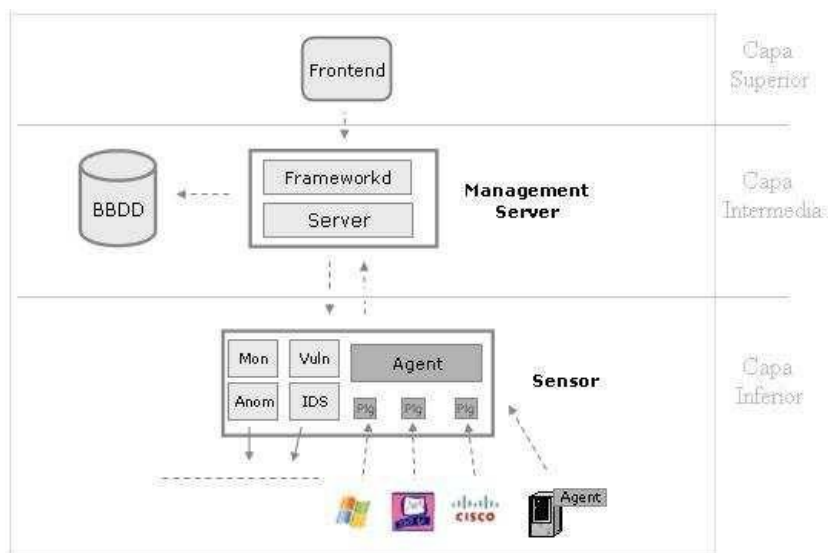
En el nivel intermedio se realiza el postprocesado, donde Ossim desarrolla un proceso de abstracción en el que millones de pequeños eventos incompresibles se convierten en singulares alarmas comprensibles, este proceso se lleva a cabo principalmente en el motor de correlación¹, donde el administrador crea directivas de correlación para unir diferentes eventos de bajo nivel en una única alarma de alto nivel, cuyo objetivo es aumentar la sensibilidad y la fiabilidad de la red.

- Normalización.
- Correlación.
- Priorización.
- Valoración de Riesgos.

Por último, en el nivel más alto “*Front-end*” se ubica una herramienta de gestión, capaz de configurar y visualizar tanto los módulos externos como los propios del framework,

mediante ella podremos crear la topología de la red, inventariar activos, crear las políticas de seguridad, definir las reglas de correlación y enlazar las diferentes herramientas integradas.

Representación Ossim 3 capas.



3. El proceso de detección.

El principal objetivo del proyecto Ossim, ha sido el de aumentar la capacidad de detección ofrecida por los productos hasta hoy en día desarrollados. En este punto introduciremos cual es el secreto, de este proceso que el sistema Ossim lleva a cabo para aumentar dicha capacidad de detección.

El proceso de detección se le llama al proceso global desarrollado por el SIM, incluyendo tanto los distintos detectores y monitores de la red como los realizados por el sistema para procesar la información.

Detectores.

Llamamos detector a cualquier aplicación capaz de escuchar en la red en tiempo real en busca de patrones y producir eventos de seguridad ante la localización de situaciones previamente definidas.

La capacidad e Incapacidad de la detección.

La capacidad de detección de un detector la podemos definir mediante dos sustantivos:

- *Sensibilidad*, definida como la capacidad de análisis en profundidad y complejidad, que posee el detector a la hora de localizar un posible ataque.
- *Fiabilidad*, definida como el grado de certeza que nos ofrece el detector ante el aviso de un posible ataque.

Por lo contrario, a pesar del gran desarrollo de estos detectores nos encontramos que están muy lejos de que su capacidad por si mismos sea aceptable. En la actualidad con la utilización de los detectores por separado para afrontar estas dos propiedades, nos encontramos con los dos principales problemas de la detección:

- *Falsos Positivos*, La falta de fiabilidad en los detectores es el causante de los falsos positivos, posibles ataques detectados que realmente no corresponden con ataques reales.
- *Falsos Negativos*, La incapacidad de detección implicaría que un ataque es pasado por alto “falta de sensibilidad”.

PostProceso.

Una vez realizado el preproceso por los diferentes detectores y haber enviado la información al sistema central para realizar la colección, El postproceso es un conjunto de mecanismos capaz de mejorar la sensibilidad y fiabilidad de la detección, disminuyendo los falsos positivos por descarte de estos, o descubrir patrones más complejos que los detectores han sobrepasado para disminuir los faltos negativos.

El postproceso se puede dividir en tres métodos:

- *Priorización*, Todas las alertas recibidas se priorizan mediante un proceso de contextualización desarrollado a través de la definición de una Política topológica de la red. De esta manera se consigue descartar falsos positivos.
- *Valoración de Riesgo*, Cada evento será valorado respecto del riesgo que implica, dependiendo del valor del activo al que el evento se aplica, la amenaza que representa el evento y la probabilidad de que este evento ocurra.
- *Correlación*, Donde se analizaran un conjunto de eventos relacionados para obtener una información de mayor valor. De esta manera aumentaremos la sensibilidad de la red.

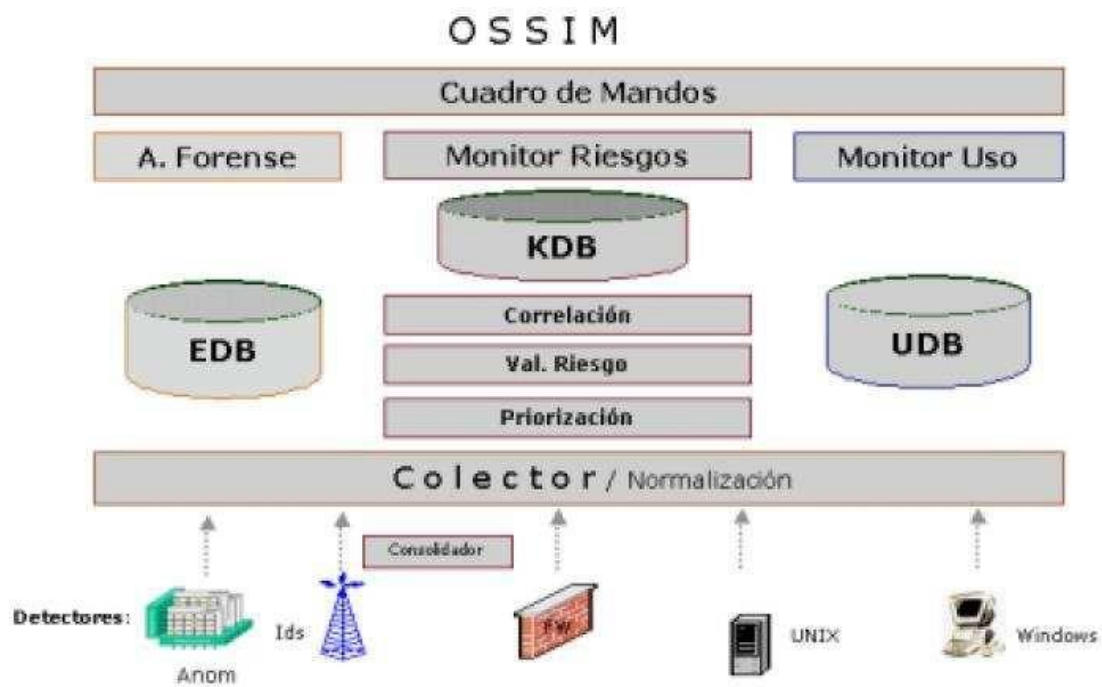
Tras el PostProceso se obtendrá como resultado las “Alarmas”, donde una alarma normalmente será el conjunto de varias alertas producidas. En este punto se habrá obtenido normalmente un mayor grado de sensibilidad, permitiendo localizar patrones más complejos y ofrecer un mayor grado de fiabilidad.

4. Arquitectura.

La arquitectura de Ossim se puede diferenciar en dos partes, una parte se realiza a través de una arquitectura distribuida y la otra sobre una arquitectura centralizada, en ellas se desarrolla los dos momentos diferentes del proceso:

- Preproceso: Que se realiza en los propios monitores y detectores distribuidos.
- Postproceso: Que se realiza en el servidor centralizado.

En el siguiente dibujo se representa de una forma detallada la funcionalidad de cada uno de los dos procesos.



2.

Ossim utiliza tres bases de datos heterogéneas para los distintos tipos de datos almacenados:

- EDB base de datos de eventos, la más voluminosa pues almacena todos los eventos recibidos desde los detectores y monitores.
- KDB base de datos del Framework, en la cual se almacena toda la información referente a la red y la definición de la política de seguridad.
- UDB base de datos de perfiles, almacena todos los datos aprendidos por el monitor de perfiles.

5. Funcionalidad.

En el siguiente punto se define cada una de las tres capas que compone Ossim. Cada una de ellas se descompone en varios niveles, formando nueve niveles que serán descritos uno a uno.

A continuación, se muestra una representación gráfica de las tres capas con sus nueve niveles intermedios:



Se empezará describiendo los niveles más bajos y se irá subiendo uno a uno hasta describir los nueve niveles que componen el sistema Ossim.

5.1 Detectores de Patrones.

Se les denomina a las aplicaciones capaces de escuchar el tráfico de la red, en busca de patrones malignos definidos a través de firmas o reglas, y producir eventos de seguridad.

Las aplicaciones más comunes son los sistemas de detección de intrusos “IDS”. Se basan en el análisis detallado de tráfico de la red, comparando el tráfico con las firmas de ataques conocidos o reglas de comportamientos sospechosos, como puede ser el escaneo de puertos. Los IDS analizan tanto el tipo de tráfico como el contenido y el comportamiento de los paquetes de la red.

Cualquier otro dispositivo de la red, como puede ser un router, firewall, o el mismo sistema operativo de los hosts, tienen la capacidad de detectar patrones en la red como puede ser un escaneo de puertos, intentos de spoofing, o posibles ataques por fragmentación, cada uno de ellos tiene su propio log de seguridad capaz de alertar de posibles problemas en la red, que podremos recolectar para su posterior tratamiento en los motores de correlación.

Detectores de patrones incluidos en Ossim.

Ossim integra varios detectores de patrones de código abierto. El detector más común en Ossim es el Snort (NIDS, Network Intrusión Detection System), incluye varios preprocesadores de detección de ataques y anomalías.

Otros detectores incluidos son Snare y Osiris (HIDS Host Intrusión Detection System), instalados en los sistemas monitorizados de la red.

5.2 Detectores de anomalías.

Los detectores de anomalías gozan de una capacidad de detección mucho más compleja e innovadora que la de los detectores de patrones. En este caso al sistema de detección no tenemos que especificarle mediante reglas que es un comportamiento bueno o malo, sino que es capaz de “aprender” por sí solo y alertar cuando un comportamiento difiere del comportamiento normal.

Esta técnica provee una solución para controlar el acceso de usuarios privilegiados y ataques internos, como puede ser un empleado desleal, o simplemente hacen un mal uso de los recursos y servicios de la empresa.

Casos en los que los detectores de anomalías son útiles:

- Nuevos ataques para el que aún no existen firmas, puede definir anomalías obvias para un detector de anomalías.
- Un gusano que puede haber sido introducido desde la red interna, malware, ataque de spam, pueden generar un número de conexiones anómalas que son fáciles de detectar.
- Uso de servicios con origen y destino anormales.
- Uso en horarios anormales.
- Exceso de tráfico o de conexiones (programas P2P).
- Cambios de sistemas operativos, ips, macs.

Estas aplicaciones pueden generar un número de nuevas alertas elevado, que podrían empeorar la visibilidad del estado de la red por si solas, pero si tomamos estas alertas como información que acompaña a resto de alertas, los niveles superiores realizarán unacorrelación más fiable y les permitirá detectar nuevas anomalías.

Detectores de anomalías incluidos en Ossim.

Ossim integra una amplia gama de detectores de anomalías:

- Spade detecta conexiones no usuales por puertos y destinos utilizados.
Usado para mejorar el reconocimiento sobre ataques sin firma.
- Aberrant Behaviour plugin para Ntop aprende el uso de parámetros y alerta cuando dichos parámetros se salen de los valores esperados.
- ArpWatch utilizado para detectar cambios de mac.
- Pof utilizado para detección de cambios de sistema operativo.
- Pads y Nmap Utilizado para detectar anomalías en los servicios de red.

5.3 Sistema de Colección y Normalización.

El proceso de colección y normalización se encarga de unificar todos los eventos de seguridad provenientes de cualquier sistema de la red en una única consola y formato.

La recolección de datos se puede hacer de dos formas distintas en el sensor. Se puede enviar los datos desde el equipo analizado usando protocolos nativos del equipo al gestor central, o instalando agentes en el equipo analizado que recopilan la información en el host y la envían seguidamente. Ossim normalmente no utiliza agentes y utiliza las formas de comunicación naturales de los sistemas.

La normalización implica la existencia de un “parser” o traductor que conozca los tipos de formatos de alertas de los diferentes detectores, capaz de homogeneizar el tratamiento y la visualización de todos estos eventos en una única base de datos “EDB”.

EDB, es la base de datos que Ossim utiliza para almacenar todos los eventos que colecciona, es la base de datos más voluminosa.

De esta forma se podrá visualizar en la misma pantalla y con el mismo formato los eventos de seguridad de un determinado momento, ya sean del Router, firewall, IDS o de cualquier host.

Al tener centralizado en la misma base de datos todos los eventos de la red se podrá desarrollar procesos a niveles superiores que permitan detectar patrones

más complejos y distribuidos.

5.4 Políticas de priorización.

La prioridad definida para una alerta será dependiente de la topología de la red, inventario de cada máquina y del rol que estas desempeñan en la organización. Si una alerta que se refiere a un ataque al servicio IIS de Microsoft, llega a una máquina con sistema operativo Unix y servidor Apache, la alerta debe de ser despriorizada. En cambio, si existe una conexión sospechosa de un usuario sobre un servidor, el sistema debe priorizar la alerta dependiendo de la ubicación del usuario y del uso de la conexión.

El proceso de priorización de alertas se realiza mediante contextualización, es decir la valoración de la importancia de una alerta depende del escenario de la red. Este escenario está descrito en una base de conocimientos sobre la red formada por:

- Inventario de Máquinas y Redes (ip, mac, sistema operativo, servicios, etc).
- Políticas de Acceso (desde donde a donde está permitido o prohibido).

Todos estos parámetros son alojados en la base de datos “KDB”, que es la base de datos que Ossim utiliza para parametrizar el framework. De esta forma el sistema conocerá la topología de la red, características de las máquinas y las políticas de seguridad definidas.

A través de la valoración de alertas se realizará una de las partes más importantes del filtrado de alertas recibidas por los detectores. Desde el framework del sistema

podremos configurar las siguientes características:

- Política de Seguridad
- Inventario de las máquinas de la red.
- Valoración de activos.
- Valoración de amenazas.
- Valoración de fiabilidad de cada alerta.
- Definición de alarmas.

Para que el proceso de priorización sea efectivo se debe realizar una continua y detallada especificación de la situación de la organización.

CASO FRECUENTE COS EN LA UNS

Uno de los casos más frecuentes en la UNS es la **propagación de malware**, para lo cual en el servidor OSSIM se debe configurar una alerta que nos permita detectar el virus en tiempo real. Esto se logra gracias a que el antivirus está conectado a la herramienta SIEM permitiéndonos así determinar si el malware fue eliminado, bloqueado o puesto en cuarentena. Esta alerta es enviada al equipo encargado del COS.

Durante una alerta de seguridad de este tipo (malware, archivos maliciosos), los especialistas encargados del COS son responsables de determinar si una alerta es válida o un falso positivo. El procedimiento a seguir para esta alerta es la siguiente:

1. **Recolección de datos:**

Durante este proceso, el especialista recopila de datos relevantes sobre la alerta. Esta información será utilizada para determinar si es un incidente o un falso positivo.

En este punto sucede dos acontecimientos:

- ❖ Dejar la alerta como falso positivo y dar cierre a esta alerta.
- ❖ Clasificar la alerta como un incidente.

2. **Identificar los afectados:**

En este punto se debe verificar si el equipo afectado corresponde a una estación de trabajo o un servidor.

- ❖ Si es una estación de trabajo, se debe aislar el equipo.
- ❖ Si es un servidor, se debe habilitar un servidor de respaldo y aislar el equipo afectado.

3. Investigación:

El propósito de este procedimiento es recopilar toda la información del método y archivo malicioso que ingreso a la red. Para eso se realiza lo siguiente:

- ❖ Análisis del antivirus al archivo.
- ❖ Análisis de la dirección IP de origen.
- ❖ Fecha de registro.
- ❖ Análisis del malware (Virus scanner, EDR).
- ❖ Búsqueda de otros equipos infectados, verificar los registros de red y los registros de puntos finales.
- ❖ Análisis de documentos (información de la familia de malware, vector de infección, mecanismos de persistencias, etc.).

4. Contención:

- ❖ Bloquear y registrar el trafico sospechoso en proxy y firewall.
- ❖ Identificar a través de la herramienta Antispam los destinatarios de algún mail malicioso.
- ❖ Escaneo por el antivirus en modo de bajo demanda (alta heurística).
- ❖ Análisis de exploración con antivirus y EDR.

5. Validar que se encuentre solucionado:

En este punto debemos validar que el malware se encuentre eliminado por completo y full Scan posterior a los dispositivos. En caso no se pueda eliminar por completo proceder a formatear o cambiar el equipo.

6. Concientizar a los usuarios:

Mediante capacitaciones o charlas informativas concientizar al personal y estudiantes sobre el uso adecuado de los equipos.

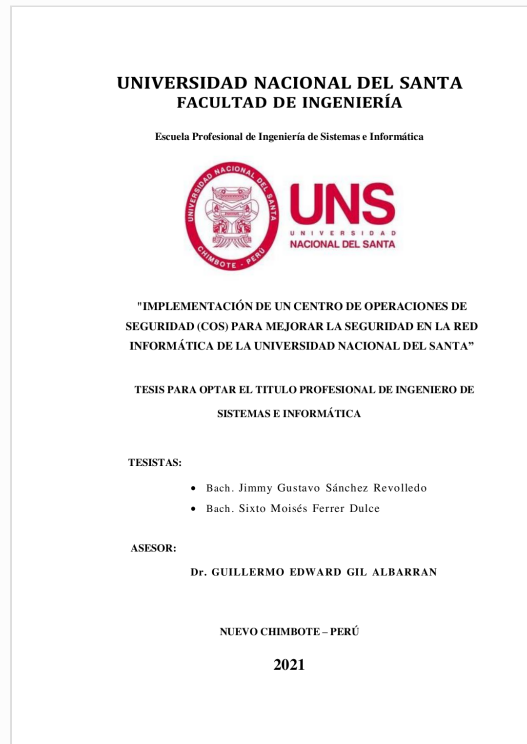


Recibo digital

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

La primera página de tus entregas se muestra abajo.

Autor de la entrega: Jimmy Gustavo Sánchez Revolledo Sixto Moisés Ferrer Dulce
Título del ejercicio: TESIS
Título de la entrega: "IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SE...
Nombre del archivo: INFORME_FINAL_DE_TESIS_2021.pdf
Tamaño del archivo: 11.61M
Total páginas: 179
Word count: 21,261
Total de caracteres: 128,338
Fecha de entrega: 09-feb.-2022 09:00a. m. (UTC-0500)
Identificador de la entre... 1758475428



"IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (COS) PARA MEJORAR LA SEGURIDAD EN LA RED INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DEL SANTA

por Jimmy Gustavo Sánchez Revollo Sixto Moisés Ferrer Dulce

Fecha de entrega: 09-feb-2022 09:00a.m. (UTC-0500)

Identificador de la entrega: 1758475428

Nombre del archivo: INFORME_FINAL_DE_TESIS_2021.pdf (11.61M)

Total de palabras: 21261

Total de caracteres: 128338

"IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (COS) PARA MEJORAR LA SEGURIDAD EN LA RED INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DEL SANTA

INFORME DE ORIGINALIDAD

29%

INDICE DE SIMILITUD

28%

FUENTES DE INTERNET

3%

PUBLICACIONES

19%

TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	nyulrdlr.blogspot.com Fuente de Internet	2%
2	pt.scribd.com Fuente de Internet	2%
3	es.slideshare.net Fuente de Internet	2%
4	www.ciset.es Fuente de Internet	2%
5	search.ndltd.org Fuente de Internet	2%
6	blog.cerounosoftware.com.mx Fuente de Internet	2%
7	Submitted to Universidad Nacional del Santa Trabajo del estudiante	1%
8	es.scribd.com Fuente de Internet	1%

9	es.wikipedia.org Fuente de Internet	1 %
10	www.coursehero.com Fuente de Internet	1 %
11	docplayer.es Fuente de Internet	1 %
12	repositorio.espe.edu.ec Fuente de Internet	1 %
13	www.scribd.com Fuente de Internet	1 %
14	Submitted to Universidad Catolica de Avila Trabajo del estudiante	1 %
15	Submitted to Universidad Catolica de Oriente Trabajo del estudiante	1 %
16	www.cybernuvol.com Fuente de Internet	1 %
17	repository.unad.edu.co Fuente de Internet	1 %
18	www.iperu.org Fuente de Internet	1 %
19	repositorio.une.edu.pe Fuente de Internet	1 %
20	lisainsurtech.com Fuente de Internet	1 %

21	www.microkeygroup.com Fuente de Internet	<1 %
22	www.dspace.uce.edu.ec Fuente de Internet	<1 %
23	dipsolutions.com.ar Fuente de Internet	<1 %
24	repositorio.ucv.edu.pe Fuente de Internet	<1 %
25	repositorio.upn.edu.pe Fuente de Internet	<1 %
26	www.ingeniaglobal.cl Fuente de Internet	<1 %
27	seguridadensistemas.wordpress.com Fuente de Internet	<1 %
28	repositorio.urp.edu.pe Fuente de Internet	<1 %
29	repositorio.udch.edu.pe Fuente de Internet	<1 %
30	www.piuraheraldo.net Fuente de Internet	<1 %
31	sertek.hn Fuente de Internet	<1 %
32	repositorio.unp.edu.pe Fuente de Internet	<1 %

33	Submitted to Fundación Universitaria Católica del Norte Trabajo del estudiante	<1 %
34	abcnoticias.pe Fuente de Internet	<1 %
35	blog.tecnologia5.com Fuente de Internet	<1 %
36	dspace.esPOCH.edu.ec Fuente de Internet	<1 %
37	cdn.nucom.at Fuente de Internet	<1 %
38	modelodecartaamonestacion.blogspot.com Fuente de Internet	<1 %
39	Submitted to UNIV DE LAS AMERICAS Trabajo del estudiante	<1 %
40	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1 %
41	Submitted to Universidad Privada Antenor Orrego Trabajo del estudiante	<1 %
42	www.telefonica.com Fuente de Internet	<1 %
43	repositorio.utn.ac.cr Fuente de Internet	<1 %

44	patrimoniocultural.defensa.gob.es Fuente de Internet	<1 %
45	repositorio.unprg.edu.pe:8080 Fuente de Internet	<1 %
46	yeranivanesa.blogspot.com Fuente de Internet	<1 %
47	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1 %
48	apps.contraloria.gob.pe Fuente de Internet	<1 %
49	repositorio.ucsg.edu.ec Fuente de Internet	<1 %
50	repositorio.udl.edu.pe Fuente de Internet	<1 %
51	hdl.handle.net Fuente de Internet	<1 %
52	renati.sunedu.gob.pe Fuente de Internet	<1 %
53	repositorio.usmp.edu.pe Fuente de Internet	<1 %
54	www.buenastareas.com Fuente de Internet	<1 %
55	revistas.udc.gal	

Fuente de Internet

<1 %

56

th-brilliant-innocence.blogspot.com

Fuente de Internet

<1 %

57

Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD

Trabajo del estudiante

<1 %

58

documentop.com

Fuente de Internet

<1 %

59

transparencia.rree.gob.pe

Fuente de Internet

<1 %

Excluir citas

Activo

Excluir coincidencias < 15 words

Excluir bibliografía

Activo