Diseño y transición inicial de un Centro de Operaciones de Seguridad (SOC) en la Unidad de Tecnologías de la Información de la Universidad de las Fuerzas Armadas ESPE, basado en Itil

Angos Cosíos, María José

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Sistemas e Informática

Trabajo de titulación, previo a la obtención del título de Ingeniera en Sistemas e Informática

Ing. Ron Egas Mario Bernabé

25 de febrero del 2022

Tesis SOC-María José Angos Final.pdf

Scanned on: 16:39 February 15, 2022 UTC

Overall Similarity Score | Results Found | Total Words in Text

Identical Words	319
Words with Minor Changes	108
Paraphrased Words	567
Ommited Words	2744

MARIO BERNA BE RON EGAS

Firmado digitalmente por MARIO BERNABE RON EGAS
Fecha: 2022.02.15 12:07:46 -05'00'

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

CARRERA DE INGENIERIA DE SISTEMAS E INFORMATICA

CERTIFICACIÓN

Certifico que el trabajo de titulación, **"Diseño y transición inicial de un Centro de Operaciones de Seguridad (SOC) en la Unidad de Tecnologías de la Información de la Universidad de las Fuerzas Armadas ESPE, basado en Itil"** fue realizado por la señora **Capt. de Com. Angos Cosios Maria Jose** el cual ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto, cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 25 de febrero de 2022

MARIO BERNABE RON EGAS

Firmado digitalmente por MARIO BERNABE RON EGAS
Fecha: 2022.02.21 15:19:18 -05'00'

Ing. MSc. Ron Egas Mario Bernabé MSc

C.C. 1704229747

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

CARRERA DE INGENIERIA DE SISTEMAS E INFORMATICA

RESPONSABILIDAD DE AUTORIA

Yo, **Capt. de Com. Angos Cosios, Maria Jose**, con cédula de ciudadanía N° 1720982873, declaro que el contenido, ideas y criterios del trabajo de titulación**: "Diseño y transición inicial de un Centro de Operaciones de Seguridad (SOC) en la Unidad de Tecnologías de la Información de la Universidad de las Fuerzas Armadas ESPE, basado en Itil"** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 25 de febrero de 2022

Angos Cosios Maria Jose

Capt. de Com.

C.C. 1720982873

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

CARRERA DE INGENIERIA DE SISTEMAS E INFORMATICA

AUTORIZACION DE PUBLICACION

Yo **Capt. de Com. Angos Cosios Maria Jose,** con cédula de ciudadanía N° 1720982873, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación "***Diseño y transición inicial de un Centro de Operaciones de Seguridad (SOC) en la Unidad de Tecnologías de la Información de la Universidad de las Fuerzas Armadas ESPE, basado en Itil***" en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 25 de febrero de 2022

Angos Cosios Maria Jose

Capt. de Com.

C.C. 1720982873

Dedicatoria

Primero quiero agradecer a Dios por darme la vida, la salud y la fortaleza para formar mi familia y orientarme en cada etapa profesional.

A mi familia, Jorge mi esposo, Paula, Isabella y Caleb mis hijos que han sido la base fundamentan de cada elección y testigos del camino recorrido, pero sobre todo por la comprensión y el amor en todo momento, que son sus consejos y abrazos nunca me dejaron derrotar por las adversidades y dificultades.

A mis queridos padres Hugo y Luz que me formaron para llegar a ser el gran humano que soy hoy y que siempre me han apoya en cada etapa de mi vida profesional.

A mis hermanos que siempre han estado a mi lado en todo momento apoyándome a culminar mi meta.

Y a todas aquellas personas que me brindaron su sincera amistad y me brindaron una mano.

Agradecimientos

Agradezco principalmente a Dios por bendecir mi camino y estar conmigo en todas las áreas de mi vida, sobre todo en la profesional.

A mis hijos Paula, Isabella y Caleb, a mi esposo, mis padres, mis hermanos que han sido mi apoyo y guía en todo este proceso y siempre fueron la motivación para alcanzar mis metas.

A mi director de tesis el Ing. Mario Bernabé Ron Egas por confiar en mí y ayudarme en este largo camino.

A mis compañeros cercanos y amigos que han sido motivación para culminar esta etapa.

A la Universidad de las Fuerzas Armadas que me ha formado como profesional en sus aulas.

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

La ciberseguridad intenta proteger datos, dispositivos, identidad y sistemas contra amenazas cibernéticas para el bienestar personal, académico, estatal o militar; hay que recordar que en la actualidad toda institución maneja datos, y en la mayoría hacen un uso continuo del internet y vincular sus sistemas con ellos. Existen instituciones médicas, financieras, educativas o del gobierno, que optan por el uso del internet para funcionar de una manera más óptima y eficaz.

De acuerdo con la problemática actual de la ESPE, no posee un Centro de Operaciones de Seguridad de la Información propio, formalmente establecido que permita actuar, monitorear y dar seguimientos a las alertas o amenazas informáticas presentadas.

El siguiente trabajo de titulación busca como objetivo poner en marcha inicial un Centro de Operaciones de Seguridad (SOC) dentro de la Universidad de las Fuerzas Armadas ESPE en la unidad de Tecnologías de la Información (UTIC) ,a través de un análisis preliminar de la situación actual de la universidad que nos permitirá escoger las herramientas más optimas de seguridad de la información para así levantar un nuevo servicio cuyo objetivo principal sea detectar amenazas y mitigar riesgos para garantizar la seguridad de las conexiones y sus dispositivos en el desarrollo de las actividades diarias de la comunidad universitaria de la ESPE.

Palabras clave:

- **EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA**
- **SOC**
- **ITIL V4**
- **HERRAMIENTAS DE CIBERSEGURIDAD**

Abstract

Cybersecurity attempts to protect data, devices, identity, and systems against cyber threats to personal, academic, state, or military well-being; It must be remembered that at present every institution handles data, and most of them make continuous use of the Internet and link their systems with it. There are medical, financial, educational or government institutions that choose to use the Internet to function in a more optimal and efficient way.

In accordance with the current problems of the ESPE, it does not have its own Information Security Operations Center, formally established that allows it to act, monitor and follow up on the alerts or computer threats presented.

The following degree work seeks as an objective to start up a Security Operations Center (SOC) within the University of the Armed Forces ESPE in the Information Technology unit (UTIC), through a preliminary analysis of the current situation of the university that will allow us to choose the most optimal information security tools in order to build a new service whose main objective is to detect threats and mitigate risks to guarantee the security of connections and their devices in the development of daily activities of the ESPE university community.

Key words:

- **COMPUTER SECURITY INCIDENT RESPONSE TEAM**
- **CSIRT**
- **ITIL V4**
- **CYBERSECURITY TOOLS**

Capítulo I

Introducción

Generalidades

El presente capitulo tiene como como finalidad revisar y verificar la situación actual del proyecto previo a la realización del tema propuesto, en la cual tendremos presente desde los antecedentes del proyecto hasta el alcance que se espera alcanzar con sus objetivos. Con este capítulo iniciamos el proyecto de titulación para poder entender la problemática y hacia dónde queremos llegar con nuestro proyecto de titulación. Dentro de este capítulo veremos la importancia de implementar un SOC propio dentro de las UTICS, juntamente con las expectativas a ser alcanzadas para el éxito de dicho proyecto; estas servirán para comprobar con las conclusiones y recomendaciones que se verá en el capítulo V.

Antecedentes

La red de información electrónica se volcó en los últimos años hacer parte primordial del diario vivir de las personas. Actualmente, gracias a una sociedad globalizada por medio del internet, todo tipo de organización sean médicas, educativas, financieras o gubernamentales utilizan la red para funcionar de una manera óptima. Esta información es utilizada para almacenar, procesar y compartir grandes cantidades de datos digitales aumentando la importancia de la misma siendo este un activo muy importante el cual se lo debe cuidar para evitar poner en peligro la seguridad de la organización (Minchev, 2018).

Todas las empresas, con el avance de tecnología deben ver como una inversión la protección de su activo más importante: la información; ya sea de sus clientes o de su empresa. Debido a que esta información ahora es el objetivo principal para los ataques a la seguridad informática por la cantidad enorme de datos confidenciales y estratégicos que manejan al interior de cada organización, con gran crecimiento por la situación actual

que estamos atravesando el mundo la Pandemia mundial por el virus COVID 19 (García-Peñalvo, 2020)

Siempre tomando en cuenta que se debe manejar protocolos de seguridad para su manejo dentro de la empresa, los ciberataques son cada vez más sofisticados y complejos, motivo por cual la ciberseguridad ya no es una necesidad sino una obligación (Academy, 2020).

La ciberseguridad se refiere a la protección de todos los sistemas digitales, en contra del uso no autorizado y de todas las amenazas que pongan en riesgo a la información digital. Una de las prácticas que tratan de mitigar y proteger a la información es la consolidación de un SOC (Centro de Operaciones de Seguridad) que se encarga de ejecutar muchas acciones de protección para el seguimiento y el análisis de la actividad en redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web y otros sistemas, indagando actividades anómalas que nos indican los diferentes procesos que se ejecutan sobre la seguridad de la información de la empresa resultando como un incidente (Mendoza, 2015).

Definición de la problemática

La Universidad de las Fuerzas Armadas ESPE cuenta con la comunidad universitaria conformada por el personal administrativo, docente, y alumnos que son los principales beneficiarios de los servicios que provee en cuanto a su estructura física y tecnológica. La universidad tiene la mayoría de sus procesos y operaciones con un alto uso de herramientas en red para lograr su adecuado funcionamiento y proveer de mejor manera sus servicios. El gran avance tecnológico ha hecho que la universidad se adapte a los cambios en tecnología, principalmente de la internet, donde, debido a su gran crecimiento también ha aumentado los riesgos ante amenazas informáticas siendo un peligro inminente las amenazas cibernéticas, para la operación normal de la institución.

De acuerdo con la problemática actual de la Universidad, no se posee un Centro de Operaciones de Seguridad de la Información propio de la universidad, formalmente establecido que permita actuar, monitorear y dar seguimientos a las alertas o amenazas informáticas presentadas, dando como consecuencia la vulnerabilidad de la red ante ataques cibernéticos internos o externos, sin dar el tratamiento adecuado a los incidentes de seguridad de la información.

Dada la situación actual de la ESPE y su déficit en cuanto a seguridad informática, es primordial la creación de un SOC propio que monitoree la red de la institución y permita ejecutar acciones preventivas y correctivas ante un incidente de seguridad, disminuyendo el riesgo y las consecuencias dadas por un ataque cibernético. Es de suma importancia la operación de un SOC ya que este nos ayuda a mitigar los potenciales incidentes de seguridad logrando que se identifiquen, analicen, defiendan e investiguen y se informe al área encargada siento su finalidad la de prestar servicios la ciberseguridad.

Justificación

En evaluaciones realizadas al Sistema de Información de la ESPE, se ha determinado que no existe un Centro de Operaciones de Seguridad actualmente en la universidad, a pesar de que las disposiciones normativas requieren de su implementación y que las amenazas actuales han aumentado en el ciberespacio, la universidad no cuenta con dicha área.

Las amenazas cada vez se han vuelto más preocupantes en la región, por lo que existen estadísticas alarmantes de ataques a instalaciones tanto públicas como privadas, de las que no se encuentra libre la universidad, sabemos que los datos y la infraestructura TI es importante en cualquier establecimiento para entregar sus servicios con calidad y oportunamente, entendiendo que la disponibilidad, integridad y

confidencialidad de información debería ser un activo prioritario para el crecimiento de toda institución.

Hay varios riesgos a los que está expuesta la Universidad y que deben ser mitigados mediante una estrategia eficaz y eficiente con el SOC, en ese sentido Mendoza (2015) menciona lo siguiente:

- Infección de computadores dentro de una red.
- Infección de servidores.
- Conexión con servidores externos maliciosos.
- Se omite de control en el manejo de la estructura de TI dentro de la institución.
- No autorizar el acceso a datos.
- Falta de control a los usuarios en los diferentes sistemas dentro de la institución.
- Falta de preservación de evidencia ante un incidente.
- Poca capacidad reactiva ante un evento de seguridad indeseado.
- Explotación de vulnerabilidades.
- Datos de estudiantes, profesores y personal administrativo vulnerables ante un ataque.

El presente proyecto intenta mitigar estos riesgos en la Universidad de las Fuerzas Armadas ESPE, diseñando un SOC funcional que se encuentre en capacidad de monitorear las áreas críticas de la institución y brindar servicios relacionados con la ciberseguridad, además de permitir la formación y capacitación de personal docente y estudiantes en esta importante área de la informática, fomentando buenas prácticas de seguridad y promoviendo a la investigación activa.

Objetivos

Objetivo General

Realizar el Diseño y transición inicial de un Centro de Operaciones de Seguridad (SOC) en la Unidad de Tecnologías de la Información de la Universidad de las Fuerzas Armadas ESPE, utilizando el marco referencial de ITIL V4 asegurar el control de amenazas y mitigar el riesgo dentro los sistemas de información de la institución.

Objetivos Específicos

- Realizar una revisión sistemática de literatura, revisando los proyectos y la documentación existente para la instalación de un SOC dentro de una universidad.
- Realizar el Diseño del SOC utilizando ITIL.
- Realizar la Transición inicial del SOC-ESPE de acuerdo a las buenas prácticas de ITIL.
- Evaluar la Transición inicial del SOC –ESPE.

Alcance

El presente proyecto plantea como solución a los problemas de seguridad presentados actualmente en la Universidad de las Fuerzas Armadas, la implementación de un SOC, utilizando ITIL V4, específicamente considerando sus componentes y dentro de ésta se llegará hasta el diseño y transición hasta el punto de obtener y construir la solución inicial.

Capítulo II

Fundamentación Teórica y Estado del Arte

Fundamentación teórica

En este capítulo se detalla la importancia de la ciberseguridad en nuestro entorno actual y el valor que tienen los datos dentro de todo tipo de organización y ahora con más énfasis en la seguridad de dichos datos por la pandemia mundial que estamos atravesando, además del estudio de las diferentes vulnerabilidades informáticas que tienen actualmente las instituciones académicas siendo estas un riesgo prominente a ser víctimas de un ciberataque. Aquí detallaremos aspectos importantes como la definición de la seguridad informática, la importancia y el comportamiento que tiene ciberdelincuente para cometer varios delitos informáticos, veremos la importancia de estar seguros y por qué la Universidad de las Fuerzas Armadas ESPE debe contar con un SOC que le permita tomar acciones ante alguna acción maliciosa o ante un ataque cibernético.

Al elaborar el presente proyecto se tomó en cuenta investigaciones pasadas del diseño y la estrategia para la implementación de un SOC; estos servirán para tener en cuenta en el inicio al desarrollo del este proyecto; se estudiará las propuestas de los anteriores investigadores que servirán como base para que el actual proyecto sea un éxito y cumpla con los aspectos más importantes de un SOC.

Se ha tomado como indicador el marco de referencia de ITIL para la elaboración del proyecto, en este capítulo veremos por qué ITIL es un marco de referencia que tiene lo apropiado para este tipo de propuestas, tomando en cuenta sus fases de desarrollo y sus procesos para que dicho proyecto sea un éxito. Hay que tomar en cuenta que este trabajo de titulación se realizara la fase I y fase II. Se verá también las herramientas necesarias para la elaboración del proyecto, con base en el hardware y software indispensable para operación exitosa del SOC de la ESPE, así como el espacio físico, la

metodología de implementación y la descripción de cada una de las herramientas seleccionadas.

Seguridad de la información

Concepto

La red de comunicación interconectados entre sí (internet) se ha hecho parte fundamental del uso cotidiano de todas las personas. Según (Simon, 2021) en su reporte digital del 2021 nos cuenta que más de 4.66 billones de personas usan internet, donde 4.2 billones de estas usan redes sociales, es decir alrededor del 54% de la población mundial. Según (Simon, 2021) el crecimiento del uso del internet tomando en cuenta al del año pasado, es de 4.66 mil millones, es decir un aumento del 1%, debido que el año 2021 subió un 7% con relación al 2019 por la pandemia mundial que estamos atravesando aún. En cuestión de las redes sociales, esta ha crecido un 9,5 % desde el año 2019 y finalmente el uso de dispositivos móviles ha crecido a 5.22 billones de usuarios en el presente año.

Figura 1

Datos del Uso del Internet del 2021

Nota. *Tomado del We are Social por Kemp Simon, 2021.*

A continuación, observaremos el crecimiento de internet en base a enero del 2021

Figura 2

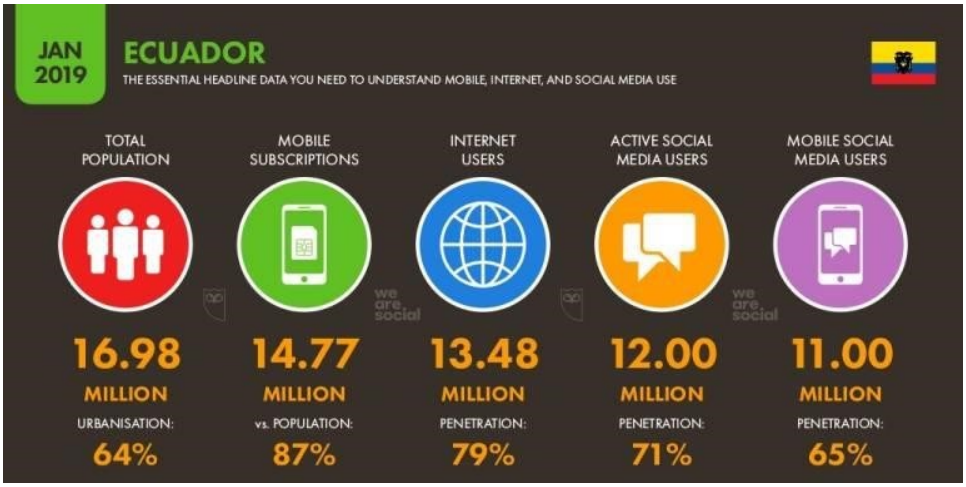
Crecimiento del Internet en el 2021

Nota. *Tomado del We are Social por Kemp Simón, 2021.*

Como podemos observar el mundo tiende al crecimiento en el uso del internet con respecto al 2019 bastante amplio, pero con respecto al 2020 no fue tanto el crecimiento debido a que la gente ya se acoplo a la nueva normalidad, estamos en una era digital en la cual la mayoría de dispositivos tienen una conexión a internet. En el caso de Ecuador según un estudio que hizo (Kemp, s.f.) del 16.98 millones de habitantes el 13.48 millones usan internet, es decir hablamos del 79% de personas en el país, en la cual 12 millones usan redes sociales es decir el 71% y 11 millones usan un dispositivo móvil para conectarse a internet. En la siguiente figura observamos los datos estadísticos del uso de internet en Ecuador.

Figura 3

Uso de Internet en Ecuador 2019

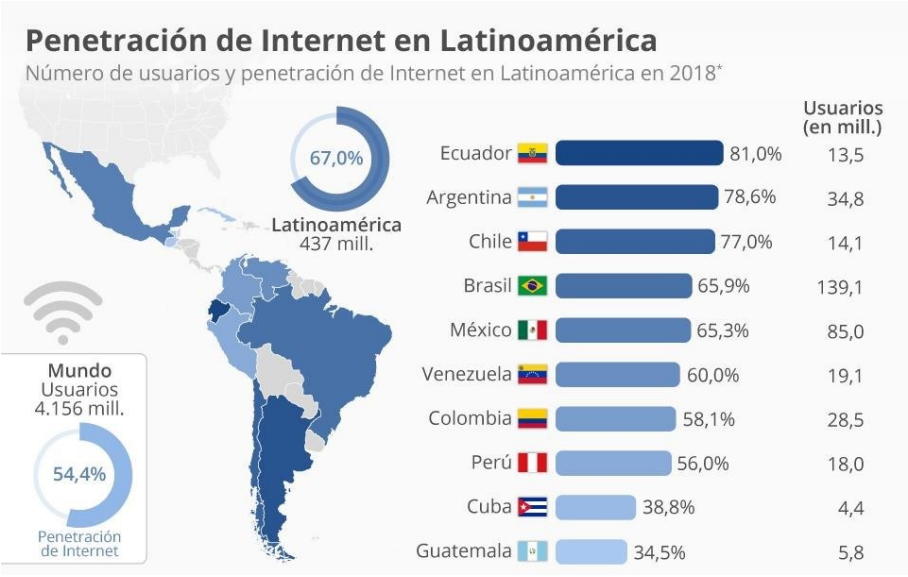


Nota. *Tomado* de We Are Social *por Kemp Simón, 2019*

Según cifras (Starts, 2018) Ecuador alcanzo en el 2018 el índice mayor de penetración de internet en América Latina, con un 81.0% Ecuador se ubica en el primer lugar seguido por Argentina con un 78.6% y Chile con el 77%.

Figura 4

Ingreso Paulatino del internet en Latinoamérica



Nota. *Tomado de* Internet World Stats *por Internet World Stats, 2018.*

En referencia a la figura anterior, podemos observar que el internet se ha convertido en una parte cotidiana para los ecuatorianos, y a pesar de ser un país pequeño también ha optado por el consumo masivo de dispositivos con conexión a la red mundial el internet. Dados estos datos estadísticos, hay que tomar en cuenta un factor importante, que es el de la seguridad informática; en donde el país cuenta con un alto consumo de internet diario, y las instituciones deberían dar la garantía de una navegación segura y confiable para los usuarios, y es cuando comenzaron a aparecer las estafas informáticas porque no se garantizó esta navegación segura.

Se define a la seguridad informática o ciberseguridad como un esfuerzo continuo de proteger todos los sistemas, sean de red o de datos, contra usuarios sin autorización. Es decir, la ciberseguridad intenta proteger datos, dispositivos, identidad y sistemas contra amenazas cibernéticas para el bienestar personal, académico, estatal, militar, etc. Hay que recordar que en la actualidad toda institución maneja datos, y en la mayoría hacen uso continuo del internet para acceder a ellos, o vincular sus sistemas con ellos. Existen instituciones médicas, financieras, educativas o del gobierno, que optan por el uso de esta red para funcionar de una manera óptima y eficaz.

En conclusión, la ciberseguridad como un conjunto de procesos y herramientas que tienen como objetivo la defensa de la información, sabiendo que la seguridad informática es un proceso en el cual participan diversas personas, sistemas y herramientas, tratando de crear conciencia de su importancia antes de ser atacados por una amenaza critica.

Características

Confidencialidad

La confidencialidad reside en lograr que toda la información sea ininteligible para todo el personal que no este o necesite participar en dicha información.

Integridad

La integridad es la verificación de los datos comprobando que no han sido modificados durante la emisión (ya sea accidental o intencionalmente).

Disponibilidad

La disponibilidad es asegurar el acceso en cualquier momento y circunstancia de un servicio o recurso.

No repudio

El repudio de la información es la garantía de que las partes involucradas en un futuro nieguen que las operaciones fueron realizadas

Elementos Fundamentales

Dentro de los elementos fundamentales que debemos tomar en cuenta al momento de la seguridad de la información tenemos los siguientes:

Un navegador seguro

Para todos los que usamos el internet hoy en día, el navegador web es prácticamente la ventada al internet siendo este nuestro medio de acceso a la información con todo el contenido para trabajar, realizar investigaciones, entretenernos, muchas veces organizar nuestras finanzas y realizar pagos en línea; con la pandemia quedo muy demostrado que todo se puede hacer en línea; siendo lo más importante la seguridad.

Felizmente, un 90% de los navegadores que están en línea son aceptablemente seguros, como por ejemplo Firefox, Edge, Chrome, Safari o incluso Opera, tomando en cuenta que sus funciones de seguridad se adaptan perfectamente a nuestras necesidades básicas, no debemos olvidar que un navegador seguro es solo aquellos que están actualizados.

No obstante, cada navegador es seguro según sus creadores, pero no lo son sus extensiones. En su mayoría las extensiones infecciosas normalmente están asociadas al

fraude que pueden dañar tu equipo. El navegador es redireccionado o enviado a un sitio publicitario que utiliza el «pago por clic» para generar dinero para la persona que creo este sitio. Iniciando el 2018, los investigadores encontraron cuatro de estas extensiones para Chrome que las habían ubicado dentro de sus máquinas alrededor de 500 000 usuarios. No obstante, este tipo de técnicas nos muestran un gran avance en la red local.

En octubre del 2018, Google estableció medidas nuevas en contra de la instalación de extensiones maliciosas para Chrome, motivo por el cual se ocasiono una caída del 89 % en ese año. Sin embargo, es fundamental ser cauteloso a la hora de instalar extensiones. Pese a ello siempre es aconsejable verificar en la red si se ha informado sobre algún problema con una instalación antes de hacerla.

No debemos esperar demasiado de la seguridad instalada en nuestro navegador, debido a que una reciente una investigación indico que 177,4 miles de sitios web han sido infectados con malware, y aproximadamente el 16% de estos se encuentran en la lista negra del motor de búsqueda.

Bloqueador de publicidad

A simple vista, tener un bloqueador de publicidad puede ser útil para nuestra ciberseguridad. Todos esos pop-ups, pop-unders y banners se vuelven muy irritantes, y al momento de cerrarlos se convierte en una mejor experiencia para la navegación. Siento así, desde las normas de seguridad aplicadas a nuestra navegación por internet es imperioso limitar la cantidad de anuncios. La publicidad ha sido un gran aliado para los malware y ciberataques como un ejemplo tenemos a PayLeak, que engaño a sus usuarios indicándoles que era un anuncio legítimo y termino siendo un ataque contra los Wallet de Apple Pay.

El Malvertising son ataques como un anuncio simple que nos redirecciona a un sitio infeccioso e intenta introducir en nuestro sistema varias cosas como Spyware hasta un Ransomware.

En esta última década, el problema más fuerte han sido los anuncios en la web que ha tenido un crecimiento acelerado. Tanto así que ya nos hemos acostumbrados a esta publicidad personalizada donde siempre se nos ofrece lo que creen que necesitamos. Todo esto se trata de la famosa ingeniería social en donde por medio de los anuncios no solo buscan influenciar en nuestras compras sino también en nuestra intención al voto cuando es tiempo de elecciones.

Motivo por el cual se han creado complementos de bloqueo de publicidad gratuitos en la mayoría de navegadores y con buena calificación; un ejemplo de estos es Secure Browser de Avast. Debemos recordar que al emplear estos bloqueadores de anuncios tomaremos en cuenta la elaboración de la lista blanca en donde ubicaremos los sitios web de confianza para que se mantenga la publicidad legitima.

Antimalware

Con todo este crecimiento de la publicidad maliciosa se duplicaron los ciberataques para robar identidad o infectarnos con malware y para poder tener más seguridad en nuestros equipos debemos tener un ANTIMALWARE, por medio del cual si llega a ingresar a nuestro sistema inmediatamente se ponga en cuarentena o se elimine.

Varios de los sistemas operativos han incorporado herramientas propias para la eliminación de los malware con el nombre de “Herramienta de eliminación de software malintencionado de Windows”, también debemos tener una solución antivirus gratuita como Avast Free para poner en cuarentena los archivos maliciosos que ingresen a nuestros equipos si las posibilidades económicas no permiten pagar un antivirus.

Por lo cual, siempre se recomienda en tener un antivirus pagado y este nos va a proteger mucho mejor de los archivos maliciosos ya que esos se están continuamente actualizando de acuerdo a cómo van saliendo nuevas amenazas.

Administrador y generador de contraseñas

La contraseña es la norma de seguridad más básica que siempre debemos implementar en todos nuestros sistemas, usando una contraseña fuerte que contenga letras y números; pero es realmente la norma más ignorada. En 2019, un estudio del National Cyber Security Center encontró que alrededor de veintitrés millones de usuarios mundiales utilizan: «123456». Una buena contraseña es exclusiva de sus dueños y muy complicada de descifrar. La entropía de una contraseña crece al mezclar símbolos, letras y caracteres. Una contraseña realmente fuerte es cuando ningún software logra descifrar en un corto periodo de tiempo.

Potencialmente nosotros estamos conscientes del gran problema que causa la seguridad de nuestras contraseñas. Se debe deducir que todos tenemos contraseñas diferentes para sitio web que utilizamos continuamente, siendo así que cada contraseña es diferente, complicada y larga. Tomando en consideración que es un gran error tener apuntado nuestras contraseñas ya que si alguien tiene acceso a este documento ya sea físico o digital podrá acceder a toda nuestra información (Bancaria y personal).

Es recomendable tener un administrador confiable de contraseñas nos ayudará solventando el problema de complejidad y singularidad permitiendo una mayor comodidad al introducir nuestras diferentes contraseñas.

Una VPN

Su traducción al español nos dice que son las redes privadas virtuales y se han especializado recientemente. No obstante, cada año crecen las preocupaciones de la privacidad en línea, los anuncios cada vez son más intrusos a nuestras necesidades y muchas personas buscan tener un anonimato en línea para sus navegaciones.

Las VPN trabajan siendo un puente entre el tráfico de Internet hacia un servidor de red centralizado antes de dirigirse con los requerimientos hacia su destino final. Haciendo que se interponga una nueva dirección IP anónima entre su máquina y los sitios

web a navegar. Lo que nos quiere decir es que las cookies que nos realizan el seguimiento para atacar nuestra información solo podrán ser rastreadas hasta el servidor VPN.

Siempre tratemos de ser cuidadosos al elegir al proveedor de VPN, utilizando solo conocidos y de confianza comprobada. Debemos siempre buscar servicios VPN que tengas buenos comentarios o reputación para así no ser vulnerables. Si el tráfico no será monitoreado y registrado por los sitios que utilicemos, el servicio del proveedor de VPN podrá guardar su propio registro, cayendo en una falta de seguridad grande ya que los dueños propietarios de los servicios que nos proveen la VPN , podrán vender toda esta información personal a grandes ciber atacantes.

Copia de seguridad de datos

Existe muchos motivos por lo que nuestros dispositivos se averían y corremos el riesgo de perder el acceso a nuestra información más sensible. Actualmente tenemos varias formas de realizar una copia de seguridad para los datos personales. Una de las conocidas es la opción de emplear un almacenamiento externo, como un disco duro extraíble o de estado sólido los mismos que nos permiten tener una copia a largo plazo sin embargo las actualizaciones nos podrían ocasionar pérdidas de tiempo, pero debemos tomar en cuenta que estos dispositivos también están expuestos a daños físicos y degradación, lo que puede traducirse en gastos fuertes para la recuperación o pérdida total de nuestros datos.

Igualmente disponemos en la actualidad de la opción de almacenamiento en la nube para realizar una copia de seguridad de todos nuestros datos. Tenemos varios proveedores de este servicio como: Dropbox, iCloud drive, OneDrive o Amazon S3, los mismos que nos proporcionan almacenamiento gratuito limitado para nuestras necesidades básicas. No obstante, varios de estos servicios básicos en línea pueden ser vulnerables y es fácil configurarlos para que pierdan su seguridad. Un estudio del año pasado nos mostró que alrededor 1500 millones de registros, que incluían información

confidencial, quedaron sin seguridad debido a la mala configuración. Desde este año, se han descubierto más falencias en la seguridad: siendo el más reciente, en mayo del 2020, fue la filtración de información de contacto en Instagram de miles de influencers o personas conocidas.

Los servicios gratuitos como dijimos anteriormente pueden ser suficientes para utilizarlos de manera personal, pero ya para las micro empresas se debe tomar en consideración la contratación de un servicio especializado en copia de seguridad y recuperación. Tomando el factor tiempo como algo primordial un buen servicio mantendrá todos los archivos actualizados de manera automática.

Cifrado de datos

El cifrado de datos no es una norma de seguridad muy conocida siendo así que pasa desapercibido; y al momento de registrar una contraseña para utilizar un servicio en línea, este sitio web debe guardarla (o así debería ser) en formatos sal y hash, evitando puedan leer fácilmente nuestras credenciales creadas e ingresar a la base de datos del sitio web. Las diferentes leyes sobre la seguridad de la información imponen regulaciones y buenas prácticas a las empresas para cifrar toda la información confidencial de los clientes, siendo así que de cierta forma ya estamos utilizando el cifrado de datos. No obstante, para nuestra seguridad personal deberíamos pensar en un cifrado de datos propio.

Al momento de realizar las copias de seguridad de nuestra información también debemos hacerlo con los servicios de la nube que cifran automáticamente esta información, pero para cifrar nuestros datos de forma local requiere una solución especializada.

Para poder mantener nuestro equipo cifrado podríamos utilizar las VPN las mismas que nos ayudan con el cifrado para la salida al tráfico de internet; y finalmente se

puede utilizar el cifrado de nuestra red de personal de WI-FI consultado con nuestro proveedor de internet.

Concluyendo el cifrado personal, por varias actividades que se realizan en casa ahora por la pandemia es muy común que varias personas compartan el mismo dispositivo entonces es mejor mantener cifrada cierta información para mantener la seguridad de nuestros datos.

Una sana paranoia

El Octavo fundamento sobre seguridad a mi criterio personal es el más importante y se trata de la paranoia, efectivamente es el que más funciona; en donde de lo que se trata es de mantener una correcta actitud sobre seguridad siendo la más económica y accesible pero la menos utilizada. Las palabras «saludable» y «paranoia» no combinan bien en otras especialidades, no obstante, para continuar seguro en línea, la paranoia potencialmente es la actitud más saludable.

Tenemos que ser sensatos de que cualquier dirección de correo electrónico o cualquier persona puede ser suplantada simplemente porque algo que nos pareció conocido o de confianza le dimos un clic y nos robó la información, y nos vale desconfiar de cualquier cosa en línea como: un correo electrónico, un sitio web, una página web, redes sociales donde nos pidan información personal(credenciales de ingresos a cuentas números de tarjetas, identificación) , como ocurre muy frecuentemente con correos enviados supuestamente del banco del pichincha diciendo que se tiene la cuenta bloqueada o suspendida y que se clic en cierto enlace.

Tomemos en cuenta que las organizaciones financieras jamás te solicitan datos reservados como números completos de tarjetas de crédito, fechas de caducidad de tarjetas, por medio de un correo electrónico, redes sociales o llamada telefónica.

En resumen, pongamos en práctica la frase «comprueba, pero confía», para mantener la seguridad en línea.

Gestión de riesgo de la información

La gestión de riesgo ejecutará un proceso para la cuantificación de las perdidas principales y secundarias que se producen de los diferentes desastres, trabajando de la mano con acciones reductivas, preventivas y correctivas.

La gestión de riesgo es un procedimiento continuo y disciplinado para la identificación y resolución del problema en cuestión; sin embargo, todo este proceso tiene una organización, planificación y presupuesto, en base a lo nombrado anteriormente la sorpresa se disminuirá ya que la gestión se convertirá en proactiva y ya no reactiva.

El riesgo cuenta con dos variables: la amenaza y la vulnerabilidad.

Amenaza

En el área de seguridad informática el término “Amenaza" es usualmente utilizado para para cualquier incidente (accidental o intencionado) que ocurre dentro de la institución y que se derive en un daño (material o inmaterial) provocando un funcionamiento defectuoso de los servicios y procesos, incidiendo en perdidas reputacionales, materiales y monetarias.

Teniendo como base el estándar internacional ISO/IEC 17799, la amenaza es el posible origen de un incidente, el cual puede ocasionar daño a una organización o sistema (ISO/IEC, 2005).

Las clasificaciones de las amenazas son de varios tipos como origen, grado de intencionalidad y efecto provocado.

1. Amenazas por el Origen: dentro de esta lista tenemos las amenazas de origen natural, internas y externas:

- Amenazas Naturales: Estas son las amenazas que controla la naturaleza y no puede saber el ser humano cuando van a ocurrir pueden ser :erupciones volcánicas, aluviones, terremotos, tsunamis, etc.

- Amenazas Internas: Son las amenazas que caen directamente sobre el personal que trabaja directamente dentro de la institución como, por ejemplo: uso indebido de herramientas informáticas, negligencia al gestionar y/o procesar toda la información de la institución, empleados insatisfechos, entre otros.
- Amenazas Externas: dentro de estas amenazas se toma en cuenta a todo el personal externo a la institución o desde redes externas como virus informáticos, ataques de DoS, robos de información, ciber ataques, etc.

2. Amenaza por el Grado de Intencionalidad: Dentro de estas listas tenemos a las amenazas de acuerdo con el nivel de intencionalidad:

- Amenazas Accidentales: son las causadas de manera no intencional es decir muchas veces sin darse cuenta del daño causado tenemos varios ejemplos: averías de hardware, fallos en software, dentro de esta amenaza se puede tomar en cuenta las amenazas naturales.
- Amenazas por Errores: este tipo de amenazas se causan por errores al momento de la ejecución, procesamiento, uso de herramientas tecnológicas y procesos propios de la institución. Normalmente estas amenazas ocurren por el desconocimiento del individuo.
- Amenazas Mal Intencionadas: dentro de estas amenazas tenemos a las realizadas con el fin de causar incidentes graves dentro de la institución.

3. Amenaza por el Efecto Causado: Dentro de este tipo de amenaza son las que causan efecto a la víctima, varios ejemplos: robo de información informática, información personal, destrucción de datos personales, etc.

Al momento de identificar los tipos de amenazas tomando como parámetros una escala definida por la institución como, por ejemplo: Baja, Media, Alta, etc. (Vieites, 2014).

Vulnerabilidades

La palabra vulnerabilidad es una debilidad que se le pueda encontrar a los recursos de la organización el mismo que va a permitir que esta se materialice y causa perdidas y daños a la institución. Como lo expone el estándar ISO/IEC 17799, vulnerabilidad es la debilidad de un grupo de activos o un activo solo, que puede convertirse en una amenaza (ISO/ICE, 2005).

La actualización de varios procedimientos propios de las instituciones no solo en la seguridad sino también en la capacitación de su personal son las mayores vulnerabilidades.

Al momento de identificar los tipos de vulnerabilidades tomando como parámetros una escala definida por la institución como, por ejemplo: Alta, Media o Baja (Vieites, 2014).

Definición de Incidentes de Seguridad

Un incidente de seguridad es la materialización de una amenaza, siendo un evento que produce la interrupción del desarrollo normal de los servicios tecnológicos que utiliza la institución mismo evento que puede llevar a perdidas, daños materiales y financieros.

Un incidente de seguridad de la información se desarrolla por una serie de eventos o evento inesperado el mismo que tiene la gran opción de perjudicar el negocio e ir en contra de la seguridad de la información (ISO/ICE, 2005).

SOC

Un Security Operation Center (SOC) es básicamente el encargado de toda la vigilancia, el rastreo y apartamiento de todos los incidentes, y la dirección de los productos de seguridad, dispositivos de red, dispositivos de usuarios finales y sistemas de las instituciones (Security M. I., 2016) El funcionamiento es fijo del SOC y se debe concentrar en toda la comunidad involucrada en las tareas de ciberseguridad (Security M. I., 2016).

Objetivos de un SOC

- Ampliar la capacidad de detección y vigilancia de las amenazas.
- Examinar las posibles amenazas y ataques.
- Recobrar toda la información perdida o dañada que la institución haya perdido por los incidentes de seguridad.
- Perfeccionar la capacidad de respuesta ante incidentes o ataques.

Organización de un SOC

Para la organización de un SOC, lo vamos a dividir por grados de especialización:

1. En el nivel 1, Nivel en que él se encuentran los analistas siempre alertas, realizan un monitoreo constante. Los analistas revisan y estiman las alertas que ingresan y si sobrepasan su capacidad de resolución lo escalan al siguiente nivel.
2. Los analistas de nivel 2, Dentro de este nivel se toma en cuenta que sistema y que datos han sido afectados y se recomendara una solución.
3. Por último, el nivel 3 Dentro de este nivel se encuentras los analistas más capacitados quienes se encargarán de resolver los incidentes de los demás niveles y buscarán prevenir los incidentes futuros.

El personal que trabaja en SOC tendrá 2 equipos unos técnicos y otros a analistas especializados en varias y diferentes áreas; y experimentados diferenciándose de un departamento tradicional del TI. Siendo esto una gran ventaja ya que mientras más variado el conocimiento será una gran ayuda en los diferentes incidentes a resolver.

Actividades principales de un SOC

El SOC utilizara procesos y metodologías estratégicas para poder mantener y construir una excelente ciber seguridad mediante la vigilancia y el análisis constante.

Monitorización continua y proactiva

Siempre el SOC ejecutará medidas intencionales fuera del normal desenvolvimiento de los sistemas para poder llegar a detectar actividades sospechosas antes de que se ejecuten.

Clasificación de alertas

Dentro de las funciones principales de un SOC es realizar la clasificación de las alertas conforme van ingresando al sistema.

Ajuste de las defensas

La prevención es lo más importante para evitar las violaciones de seguridad siendo que la gestión de vulnerabilidades y la concienciación sobre las amenazas son los pilares fundamentales para este fin.

Abarcando la vigilancia permanente del perímetro y las operaciones de la institución es donde eventualmente se producen brechas.

Comprobación del cumplimiento

Dentro de la esencia de un SOC es el cumplimiento de los reglamentos y normas nacionales e internacionales.

Un SOC trabajara diariamente para mantener la protección de la información, siempre estando un paso más adelante evitando daños y perdidas a la empresa.

Herramientas del SOC

Tenemos varias herramientas que un SOC posee:

Herramientas de análisis de malware

Para la detección de un nuevo malware, este sistema le permite al analista del SOC ejecutar y poder observar con seguridad como funciona este malware sin involucrar a los sistemas de la institución (Cisco, 2019).

Sistemas de detección de intrusiones

Este sistema nos permite realizar una inspección y monitoreo del tráfico que existe en la reden en tiempo real, si existe algún evento en este monitoreo se actuara de acuerdo a las reglas establecidas por el SOC (Cisco, 2019).

Elementos de un SOC

Para poder llegar a una protección sobre las amenazas actuales debemos tener un enfoque estructural y disciplinado (Cisco, 2019). Los SOC tiene un gran abanico de servicios que van desde el seguimiento y la gestión hasta las posibles soluciones en contra de amenazas y seguridad que podemos encontrar dentro del sistema los mismos que se van a personalizar de acuerdo a las necesidades de la cada institución. Normalmente tenemos los siguientes elementos principales de un SOC:

- Las personas.
- Los procesos.

Servidor de antivirus

Dentro de la protección anti-malware en tiempo real que ofrece este antivirus tenemos: protege frente a amenazas nuevas y emergentes. Gracias a la experiencia que tiene en el mercado este antivirus le permite la conjugación de tecnologías antimalware tradicionales y proactivas que se pueden manejar desde la nube.

Kaspersky Antivirus es el antivirus que utilizar la Espe y promete protección en tiempo real ya que constantemente se ejecutan las actualizaciones contra las diferentes amenazas de la red como podemos ver a continuación:

Protección antivirus

Este software antivirus de Kaspersky protege nuestros equipos de todos los softwares maliciosos (Troyanos, bots, virus).

Tecnología con asistencia en la nube que permite la protección en tiempo real

Constamente los ciber criminales lanzan nuevos malware, todos los proveedores de seguridad se tardan un poco en actualizar sus bases de datos y así poder ofrecer la protección en línea a sus clientes. Tomando en cuenta este antecedente la compañía Kaspersky maneja una tecnología de asistencia en la nube que les permite garantizar la protección el tiempo que se demoran sus servidores en la creación de la nueva firma contra el malware.

El servicio de Kaspersky Security Network (KSN) trabaja en el Cloud computing y contantemente recibe información sobre las nuevas amenazas que salen en la red a miles de usuarios.

Normas y buenas Prácticas para crear un SOC

Conforme continuamos en la creación de un SOC para su organización, es esencial estar atento a lo que depara el futuro en la ciberseguridad.

Las mejores prácticas de SOC incluyen:

La ampliación del enfoque de la seguridad de la información

Cuando la tecnología empezó a manejarse a través de la nube y con esto se crearon miles de procesos que se desarrollan en este sitio, entre ellos el crecimiento de la infraestructura virtual, también debemos tomar en cuenta que dentro de los avances tecnológicos más importantes esta IOT internet de las cosas siendo la conexión lo más importante. No obstante, también estamos más vulnerables a los ataques ya que se abren más puertos para todas las conexiones que estamos usando actualmente. Con el avance en la creación del SOC, es decisivo extender el alcance de la seguridad de información para continuar ofreciendo el servicio de seguridad a todos los procesos que se desarrollan dentro de la institución.

Expansión del ingreso de datos

Un aporte muy valioso es la recopilación de datos ya que por medio de estos nos permite saber cuáles son los problemas más comunes en la red, logrando ubicar estos problemas en posibles incidentes para nuestra institución y de donde viene la amenaza.

Análisis de datos mejorado

La compilación de datos es valioso solo si se hace un buen análisis de los mismos, ya que así nos permitirá colocar los posibles incidentes que existan. Siendo el caso, dentro de las buenas prácticas para el SOC será implementar un análisis profundo y completo de los datos actualizados. Centrarse en un mejor análisis de la seguridad de los datos permitirá a su equipo de SOC tomar decisiones más acertadas.

Aproveche la automatización de la seguridad

Debido al avance tecnológico la ciberseguridad se vuelve automática de forma obligatoria. De esta forma permite a los equipos ocupar su tiempo y energía en áreas más complicadas, siendo la obligación del SOC aprovechar los beneficios de la automatización de todos los sistemas.

Funciones y responsabilidades del Centro de Operaciones de Seguridad

Un centro de operaciones de seguridad está formado por varios miembros individuales del equipo. Cada miembro del equipo tiene deberes únicos. Los miembros del equipo específico que conforman el equipo de respuesta a incidentes pueden variar. Las posiciones comunes, junto con sus roles y responsabilidades, que encontrará en un equipo de seguridad incluyen:

Gerente SOC

El gerente es el jefe del equipo. Es el responsable de administrar el equipo, establecer presupuestos, agendas, y reportar a los gerentes ejecutivos dentro de la organización.

Analista de seguridad

Un analista de seguridad es responsable de organizar e interpretar los datos de seguridad del informe o auditoría de SOC. Además, la administración de riesgo en tiempo real, la valorización de vulnerabilidades y la inteligencia de seguridad brindarán información sobre el estado de preparación de la organización.

Investigador forense

En el caso de un incidente, el investigador forense es el responsable de analizar el incidente para recopilar datos, pruebas y análisis de comportamiento.

Servicio de respuesta a incidentes

El equipo de respuesta a incidentes son los primeros en recibir las notificaciones cuando se producen alertas de seguridad. Luego son responsables de realizar una evaluación inicial y una evaluación de la amenaza de la alerta.

Auditor de cumplimiento

El auditor de cumplimiento es responsable de garantizar que todos los procesos llevados a cabo por el equipo se realicen de manera que cumplan con las normas reglamentarias.

ITIL V4

ITIL en ingles se define como Information Technology Infraestructura Library que en español significa Biblioteca de Infraestructura de Tecnologías de Información donde (Merino, 2016) es un estándar para la dirección de servicios en tecnologías de la información que se proyecta en base a la ISO 20000 y a COBIT, en la cual pretende entregar una guía documentada para saber cómo planificar, proveer y dar soporte para los servicios en las tecnologías de la información.

Según (De la Torre Moscoso H.M. & Parra Rosero, 2018; Andrade, 2013)define a ITIL como un marco de referencia que contiene buenos procesos o prácticas para la

administración de sus servicios dentro de las tecnologías de la información. (Rios, 2017)Se refiere a ITIL como un grupo de publicaciones que explica de una forma sistemática el grupo de buenas prácticas que permita gestionar la infraestructura tecnológica de una organización con el objetivo de ayudar a los objetivos generales de negocio.

ITIL a lo largo de los años ha demostrado ser una guía completa, muy útil para cualquier organización, según (Rios, 2017) ITIL fue creado para empresas públicas británicas en la década de los 80´s , pero a lo largo del tiempo ha demostrado su eficiencia y ha sido adoptado por empresas privadas adaptándose a sus necesidades y objetivos de negocio. En ese contexto (Delgado, 2017) describe que la guía resulto ser tan útil que a lo largo de los años se ha adaptado en el sector de la seguridad de la información ya que sus buenas prácticas ayudan a gestionar mejor los niveles de servicio, amplía el panorama de negocios y gestiona de manera óptima los activos software y hardware.

Por otro lado, (Merino, 2016) resalta la importancia de ITIL al ser este un marco de referencia que intenta garantizar todos los servicios y procesos tecnológicos dentro de la institución y que estén alineados con las necesidades de la empresa y sus clientes. No obstante, todos los servicios de TI son utilizados por las empresas para tener éxito y crecimiento constante.

Según (Rios, 2017) ITIL es un gran referente en el sector de la ciberseguridad ya que para proveer servicios de seguridad se requiere de una gestión total del servicio, esto por la importancia de información que se maneja dentro del área de seguridad informática donde se solicita buenas prácticas para la administración. Hay que tomar en cuenta que un área de seguridad informática cuenta con información confidencial y una infraestructura diseñada para gestionar la red de la empresa, es decir dicha área es un proceso que debe contar con la guía correcta para su funcionamiento.

El presente proyecto ha tomado la guía de ITIL por las siguientes características que permiten la integración de un nuevo servicio TI en la Universidad de las Fuerzas Armadas ESPE:

- Conecta las tecnologías de la información con las diferentes áreas de negocio.
- Se adapte las metas y los objetivos de la organización.
- Se enfoca en cada uno de los procesos de la organización.
- Es sencilla de aplicar y adaptar en la organización.
- Perfeccionar la comunicación entre todos los usuarios externos e internos.
- Impulsar la efectividad y eficiencia del servicio logrando un impacto positivo dentro de los recursos financieros de la institución.
- Ser la guía práctica para el mejoramiento continuo del servicio.
- Cuenta con las buenas prácticas necesarias para el levantamiento de nuevos servicios TI.

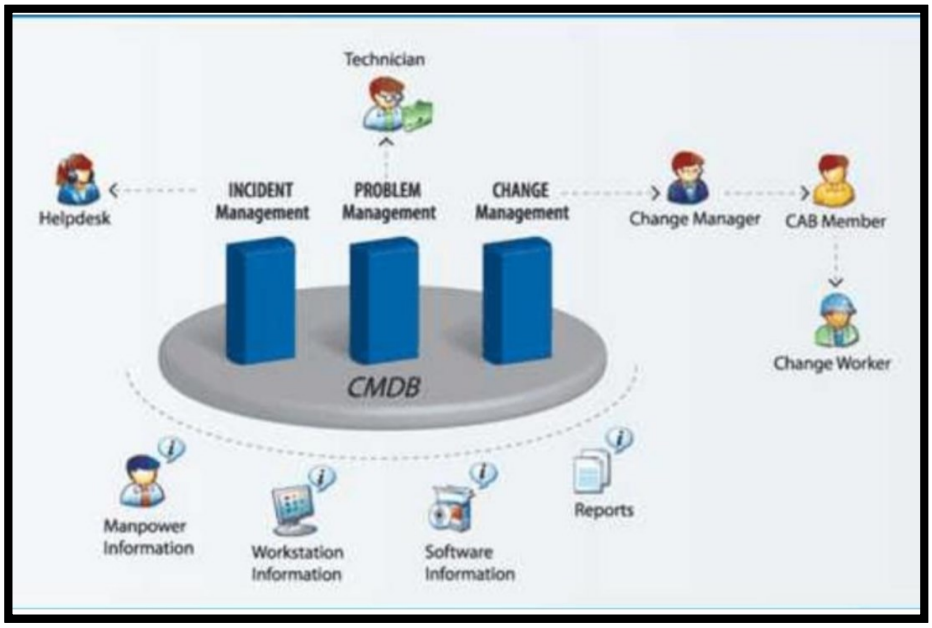
Comenzando un poco la historia de ITIL empieza en la década de los 80´s por la Central Computer and Telecommunication (CCTA) del Reino Unido y creado para el sector público y en la actualidad se ha convertido en el estándar de TI para la gestión de servicios tanto en el área privada como publica, siendo su propietario AXELOS.

La Biblioteca de Infraestructura de Tecnología de la Información (ITIL) es la base de las mejores prácticas para poder dirigir los servicios y las operaciones de TI establecidos en la década de los 80´s por el Gobierno de Reino Unido. Como objetivo principal de ITIL se busca orientar el negocio junto con la tecnología de la información, teniendo el control de lo que realmente necesita el negocio.

Dentro del primer módulo llamado Soporte de servicios de ITIL se promete las mejores prácticas para que todos los servicios estén totalmente habilitados.

Figura 5

Diagrama Global de Itil 4



Nota. Diagrama de cómo se responde a un incidente según Itil, tomado de Axelos, 2019.

Es importante entender porque ITIL ha tenido un enfoque y crecimiento en la industria de TI por esto vamos hacer el siguiente énfasis: “ITIL por muchos años ha estado a la cabeza de la industria para la Gestión de Servicios de TI (ITSM) creando programas para la orientación, formación y certificación por aproximadamente 30 años. ITIL 4 se actualizo reformulando la mayor parte de las todas las prácticas ya determinadas por el ITSM dentro de este contexto se amplió para mejorar de sus clientes su experiencia pero sobre todo la transformación digital.

ITIL V4, reformula las mejores estrategias de ITIL V3, las optimiza y se crea marcos de trabajo enfocados directamente en brindar soluciones especializadas a cada organización. En versiones anteriores de ITIL se proponía al profesional seguir de manera tasita creando un vacío al momento de surgir los problemas ya que no estaban

contemplados dentro de las normativas planteadas. Motivo por el cual ITIL V4 es más pragmática.

ITIL 4 invita a los profesionales a implementar procesos más prácticos ofreciendo soluciones mucho personalizadas para cada organización mediante prácticas que están compuestas por dos unidades que son el modelo de cuatro dimensiones y el sistema de valor del servicio de ITIL.

Para poder entender de mejor manera a ITIL V4 lo hemos dividido en cuatro partes:

- Las cuatro dimensiones de la gestión de servicios
- El sistema de valor del servicio ITIL
- Prácticas para el uso de ITIL V4
- Certificación ITIL V4

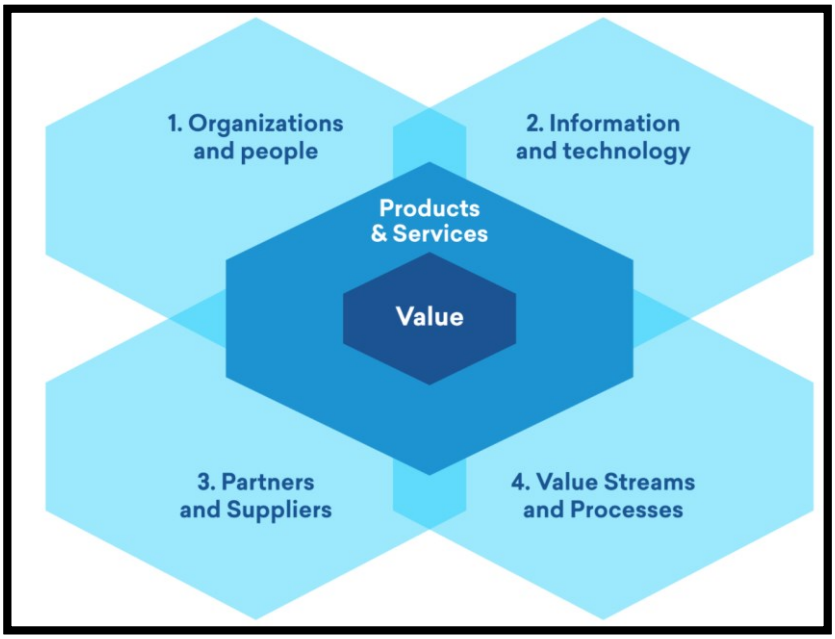
Las cuatro dimensiones de la gestión de servicios

Una administración de servicios de las Tecnologías de la Información es más importante que solo administrar la tecnología, esta administración contiene la organización estructural de la empresa y los individuos involucrados, las relaciones de los proveedores, y finalmente los procesos y las tecnologías usadas dentro de la empresa.

ITIL 4 define cuatro dimensiones bases para la creación del valor a los clientes y lo representamos a continuación:

Figura 6

Dimensiones de gestión de Servicios



Nota. Diagrama de sobre los cuatro servicios que se ha planteado en itil, tomado de Axelos, 2019.

Organizaciones y personas

La jerarquía no solo aplica para el ejército sino para toda empresa que desea que todos sus empleados cumplan a cabalidad sus funciones y se ofrezca un servicio eficiente y oportuno; esto se logra ejecutado jerarquías claras con sus roles y responsabilidad perfectamente definidas.

Lo que más afecta a una empresa es la forma en que se presta el servicio o el producto a sus clientes, como se lograr este servicio excelente, pues colocando a cada empleado en categorías como técnicos, no técnicos, administrativos, seguridad, informática, etc. Operando todos en un solo conjunto siendo que sus empleados son el activo más importante para desenvolvimiento de la empresa.

Hacer un correcto seleccionamiento del personal que va a trabajar en cada área identificando sus habilidades y debilidades llevará a la empresa al éxito. El factor humano es lo más importante para la empresa.

Información y tecnología

Para ITIL V4 se tomará en cuenta la tecnología que permita administrar los servicios, los sistemas de administración del flujo de trabajo, bases de conocimiento, inventarios, herramientas analíticas junto con el sistema de comunicación interno de la empresa. Sin olvidar la información generada, almacenada, gestionada y ocupada por la empresa durante su funcionamiento.

En la actualidad toda empresa debe establecer políticas para el manejo adecuado de grandes cantidades de información tomando en cuenta que ahora se trabaja con inteligencia artificial, aprendizaje automático y el famoso internet de las cosas.

Socios y proveedores

La gestión de servicios cuentas con dos grandes componentes los socios y los proveedores; en donde unos dependen de otros hasta cierto punto para lograr cumplir con el servicio ofrecido al cliente; en ITIL 4 se ha incorporado las relaciones de la organización con todos los involucrados en el proceso de la prestación de servicio (Diseño, desarrollo y soporte).

Toda organización depende de sus socios a diferentes niveles, unos más que otros y otro menos que otros; en cualquiera de estos casos los socios y proveedores cumplen con valores fundamentales para poder cumplir con los objetivos que busca la empresa y así garantizar la prestación de servicio de manera eficiente y oportuna .

Fuentes y procesos de valor

Dentro de ITIL 4 esta fase es donde definimos las actividades a realizar, los flujos del trabajo, junto con los procesos y procedimientos óptimos para cumplir con los objetivos estratégicos propuestos por la empresa verificando como los demás componentes de la empresa trabajan juntos para ofrecer un producto o servicio excelente al cliente.

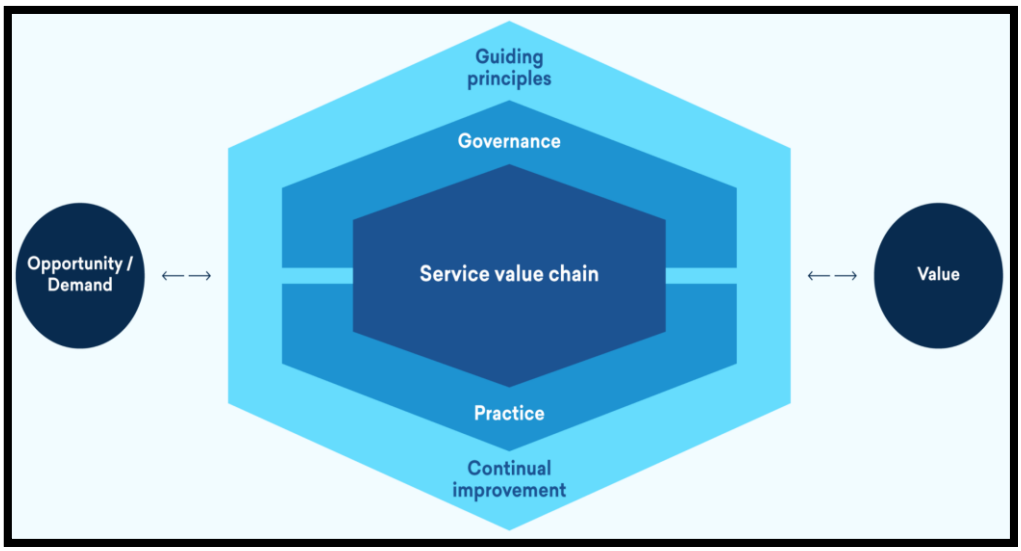
Tomando la definición que se plantea en ITIL 4 una fuente de valor es un conjunto de pasos que ejecuta la empresa para crear y finalmente entregar servicios o productos a sus clientes, dentro de esta definición logramos plantear el modelo para la entrega de servicios y así poder identificar los procesos que no aportan nada al negocio.

El sistema de valor del servicio ITIL V4

El SVS conocido como el sistema de valor del servicio relata de manera jerárquica cada entrada al sistema, tomando en cuenta los diferentes elementos que están inmiscuidos en la creación del valor y todas las salidas, es decir cumplir con los objetivos empresariales.

Figura 7

Sistema de valor del servicio



Nota. Diagrama de del sistema de valor según Itil, tomado de Axelos, 2019.

Oportunidad/demanda

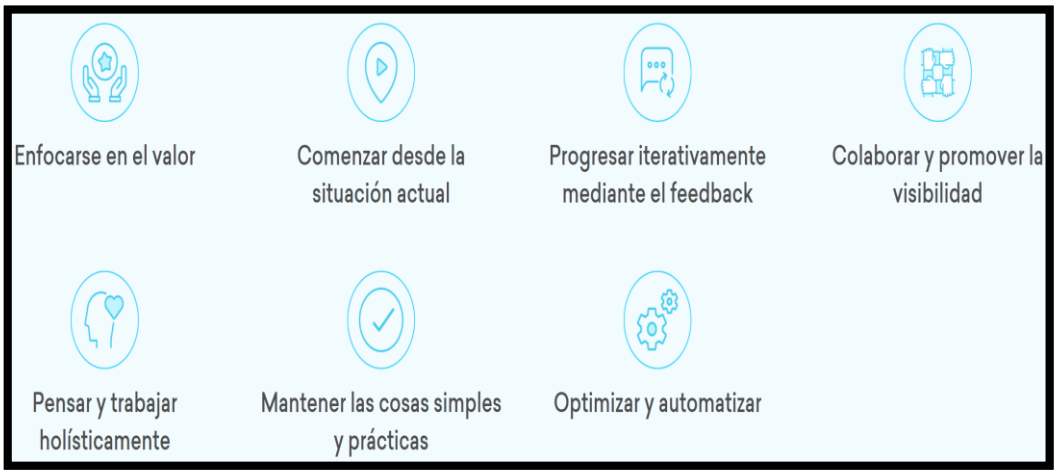
La demanda es creada por la necesidad del cliente de nuestros productos o servicios y la oportunidad personifica la habilidad de crear valor para los clientes; estas son entradas importantes para que la empresa aproveche y satisfaga sus demandas, pero no siempre son aprovechadas por la empresa.

Principios rectores

Son recomendaciones propuestas por ITIL 4 para que las empresas se orienten a través de un ciclo de vida de administración de servicios, sin que cambie al momento de cambiar objetivos o estrategias de la organización, se establecen 7 principios:

Figura 8

7 principios Rectores



Nota. Sobre los siete principios básicos o rectores según Itil, tomado de Axelos, 2019.

Gobernanza

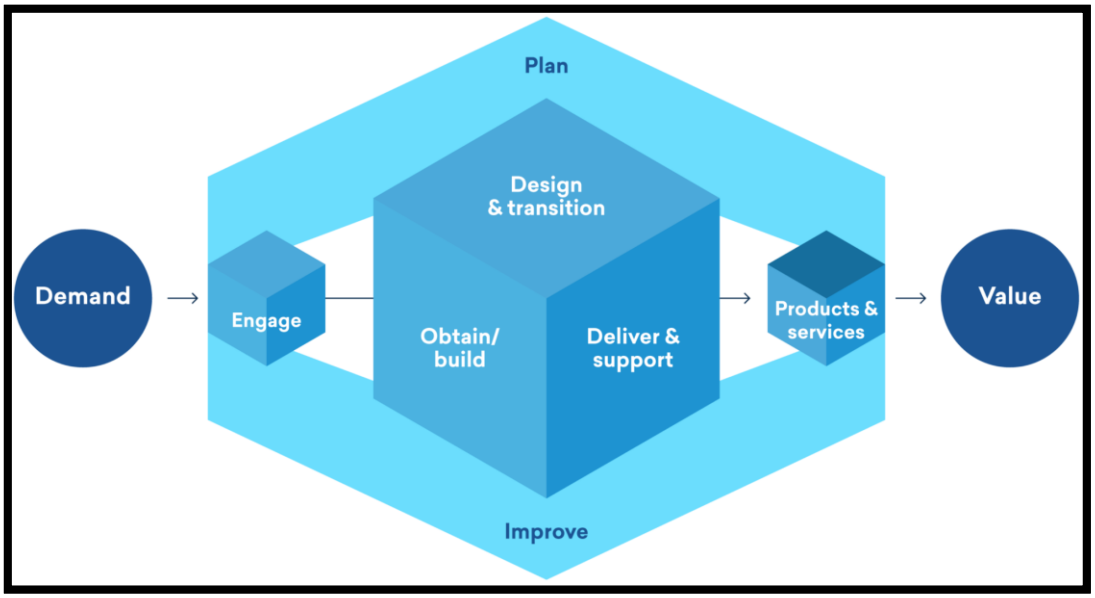
Este punto trata sobre la evaluación, dirección y monitorización de todas las actividades llegando al objetivo estratégico que es asegurar la cadena de valor del servicio o producto ofrecido por la empresa alineados perfectamente a los objetivos estratégicos.

La cadena de valor del servicio ITIL

Dentro de esta cadena de valor planteada por ITIL 4 se conjugan seis actividades que se encuentran interconectada y reciben apoyo interno como externo y las detallamos a continuación :

Figura 9

Cadena de valor Itil 4



Nota. Diagrama sobre la cadena de valor que se aplica en el plan según Itil, tomado de Axelos, 2019.

- Planificar: Consta de la creación de políticas, estándares y planes para la dirección correcta de la cadena de valor.
- Mejorar: Se asegura el mejoramiento continuo de productos y servicios.
- Interactuar: Se asegura siempre tener excelentes relaciones con todas las partes involucradas en el proceso.
- Diseño y transición: Asegurar que siempre los productos y servicios brindados a los clientes cumplan con todas sus expectativas.
- Obtener/crear: Tener siempre disponible todas las partes que conforman el servicio.
- Ofrecer soporte: Se asegura que todos los servicios sean entregados de manera oportuna y exista un seguimiento para cumplir con todas las expectativas al 100 %.

Mejora continua

El principal objetivo de la mejora continua es que continuamente se indaguen oportunidades para poder mejorar constantemente los servicios de la empresa

Prácticas para el uso de ITIL V4

(AXELOS, 2019) Una práctica es un grupo de recursos organizacionales que se desarrollan para la ejecución de todos los trabajos o para cumplir con el objetivo propuesto.

Tabla 1

Prácticas para el uso de Itil 4

GENERAL MANAGEMENT PRACTICES	SERVICE MANAGEMENT PRACTICES	TECHNICAL MANAGEMENT PRACTICES
Architecture management	Availability management	Deployment management
Continual improvement	Business Analysis	Infrastructure and platform management
Information security management	Capacity and performance management	Software development and management
Knowledge management	Change control	
Measurement and reporting	Incident management	
Organizational change management	IT asset management	
Portfolio management	Monitoring and event management	
Project management	Problem management	
Relationship management	Release management	
Risk management	Service catalogue management	
Service financial management	Service configuration management	
Strategy management	Service continuity management	
Supplier management	Service design	
Workforce and talent management	Service level management	
	Service request management	
	Service validation and testing	

Nota. Tabla sobre los usos para cada servicio según ITIL, tomado de Axelos, 2019.

Prácticas de gestión general

- Administración de la arquitectura: Nos explica detalladamente como cada elemento de la empresa se relacionan y logran cumplir con el objetivo estratégico.

- Mejora continua: Es la búsqueda de mejorar los productos o servicios mediante las necesidades cambiantes del mundo actual.
- Administración de la seguridad de la información: Establece las políticas de seguridad dentro de la empresa conforme los estándares internacionales y nacionales de cada país, ejecutando planes de seguridad interna de todos los sistemas y sus usuarios.

Prácticas de gestión de servicios

- Administración de disponibilidad: Esta práctica es la administración de disponibilidad 24 / 7 es decir asegurar que el servicio de TI este todo el tiempo disponible.
- Análisis del negocio: Esta práctica nos facilita el análisis del negocio y permite identificar problemas y sus posibles soluciones.
- Gestión de capacidad y rendimiento: Es la administración de los servicios de manera eficaz es decir que se deben cumplir con los rendimientos estimados junto con los objetivos planteados.

Prácticas de gestión técnica

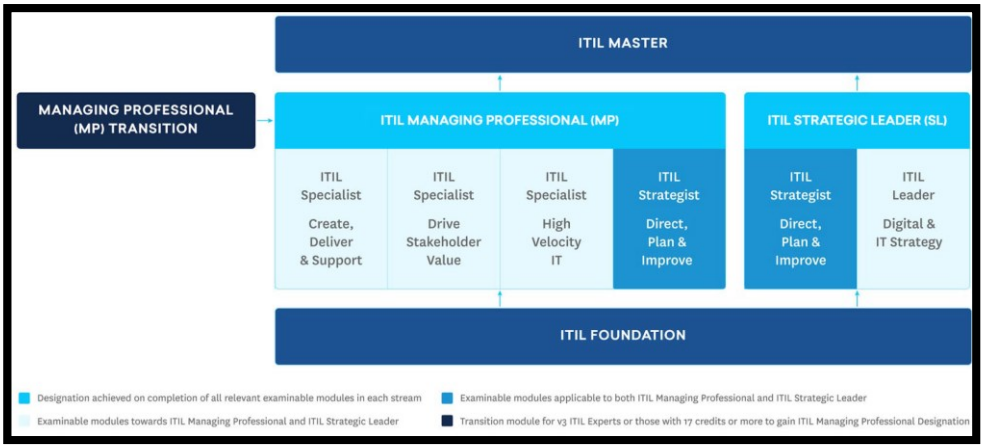
- Administración de despliegue: En esta práctica se realizar la configuración de todos los sistemas y procesadores para que funcionen de acuerdo al requerimiento solicitado.
- Administración de infraestructuras y plataformas: En esta práctica lo más importante es la correcta administración de los recursos tecnológicos físicos y virtuales, adicional la solicitud de la mejora continua de esta infraestructura.
- Desarrollo y gestión de software: El desarrollo de las aplicaciones de software propias de la empresa son importantes ya que así se permitirá tener un tratamiento único en los procesos que maneja la empresa, sin olvidar el correcto manejo de los datos.

Certificación ITIL V4

En la siguiente figura podemos observar cómo se maneja la certificación de ITIL V4.

Figura 10

Esquema de certificación de Itil V4



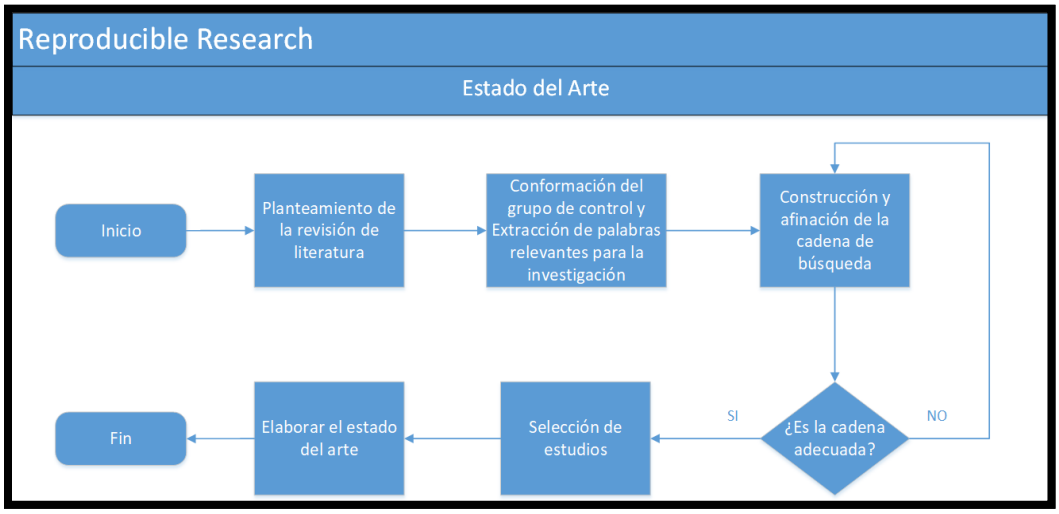
Nota. Diagrama sobre el esquema que se debe seguir para sacar la certificación según Itil, tomado de Axelos, 2019.

Estado del Arte

Para examinar el estado del arte en la investigación acerca de un SOC y la búsqueda de datos con rapidez y precisión se realizó una verificación de revisión de literatura preliminar. Su ejecución se detalla en la siguiente ilustración.

Figura 11

Método de elaboración del estado del arte



Nota. Diagrama de cómo elaborar el estado del arte, tomado de Documentos Espe, 2017.

Planteamiento de la revisión de literatura

Basándonos en las características proporcionadas en los apartados previos al Estado del arte, se realizó una descripción breve del problema de investigación para ofrecer un marco completo para la búsqueda de estudios científicos; también se definieron objetivos de búsqueda y preguntas de investigación en relación con el problema definido que permitirán alinear nuestra búsqueda relacionada con el problema descrito.

Conformación del grupo de control (GC) y extracción de palabras relevantes para la investigación

La participación en esta investigación fue realizada por una sola persona. Luego se realizó una validación de todos los estudios encontrados y se estableció cuatro estudios como los más transcendentales y detallo en la siguiente tabla:

Tabla 2

Investigaciones realizadas sobre el SOC

Título	Cita	Palabras clave
The Development of Information System Security Operation Centre (SOC): Case Study of Auto Repair Company	Muharman Lubis; Chandra Wardana; Adityas Widjajarto (2020).	Temperature sensors, Temperature measurement, Companies, Maintenance engineering, Logic gates, Control systems, Security
Analysis of the Functionalities of a Shared ICS Security Operations Center	Willian Dimitrov; Svetlana Syarova (2019).	Cyber, security, Operation, center, ics, scada, functionality
Developing and Analysis of Cyber Security Models for Security Operation Center in Myanmar	Wai Phyo Aung; Htar Lwin; Kyaw Lin (2020).	Blue team, Incident Handling, SOC, Cyber Security Model, Vulnerabilities, Threats, Attack.
Intelligent SOC Chatbot for Security Operation Center	Vihanga Heshan Perera; Amila Nuwan Senarathne; Lakmal Rupasinghe (2019).	ChatOps, SIEM, SOC, IPS, IDS, Cryptography
Security Operations Center: A Systematic Study and Open Challenges	Manfred Vielberth; Fabian Böhm; Ines Fichtinger; Günther Pernul (2020).	Security management, security operations center, security operations, SOC

Con las investigaciones presentadas se seleccionaron los términos: Security management, security operations center, security operations, SOC.

Construcción y afinación de la cadena de búsqueda

Para la afinación de la búsqueda, se tomó en cuenta los buscadores más importantes en cuanto a documentos, papers, tesis, etc, para la realización de la cadena de búsqueda. Estos buscadores son: Springerlink, IEEE Xplore y Google Académico. Al usar todos los términos seleccionados previamente, en SpringerLink se mostraron 21 resultados de los cuales como más relevantes tomamos los más votados

internacionalmente, que servirá para tener una mayor visión para la elaboración del presente trabajo de titulación.

Cadena de búsqueda: security + operations center + early alerts + vulnerability

Selección de estudios

En relación a los resultados entregados por la cadena de búsqueda. Se han seleccionado aquellos estudios que están más relacionados con fines educativos enfocados a sectores académicos, algunos ya presentados anteriormente en relación a la problemática propuesta, los cuales serán revisados a continuación

Resultados

El artículo científico presentado por (Lubis, Wardana, & Widjajarto, 2020) titulado "The Development of Information System Security Operation Centre (SOC): Case Study of Auto Repair Company" habla de su objetivo final que es brindar el mejor servicio y los mejores estándares de calidad a los clientes mediante la ejecución de los procesos de respuesta adecuados, que conduzcan a una mayor satisfacción del cliente. Es importante destacar que toda empresa requiere un sistema y un mecanismo de seguridad como un esfuerzo para proteger y superar los problemas asociados a la privacidad de los datos, las transacciones y la comunicación. Este estudio explora el problema y los desafíos que enfrenta la respetada empresa para generar una matriz de control de acceso para los activos lógicos y físicos, así como el procedimiento de operación del servicio. Y es así que toma como enfoque principal del desarrollo de Security Operation Center (SOC) como la puerta de entrada de la empresa para ofrecer diversos servicios a los clientes. SOC es un habilitador clave para los operadores que aspiran a diferenciarse en función de la experiencia y la demanda del cliente. Una aplicación de SOC exitosa puede ayudar a los operadores a reducir la presión y mejorar la eficiencia operativa.

El articulo Científico planteado por (Dimitrov & Syarova, 2019) titulada "Analysis of the Functionalities of a Shared ICS Security Operations Center" menciona que el paso

básico en el diseño de un centro de operaciones de seguridad (SOC) es identificar las funciones necesarias que se debe realizar. El artículo ofrece un análisis de las funcionalidades de ICS SOC y está enfocado a crear una parte del concepto de operaciones antes del diseño real de Shared ICS SOC. Se muestran las funcionalidades de Shared ICS SOC y se analiza su efectividad. Realiza una encuesta que se basa en una revisión del marco legal, los incidentes de seguridad de ICS, la investigación sobre las brechas entre los productos de ciberseguridad y las necesidades reales de la comunidad de ICS y SCADA. Shared SOC desempeña el papel de centro de servicios comunitarios con experiencia integrada, proporcionando servicios de seguridad para múltiples ICS. Al subcontratar estos servicios, una empresa puede reducir el personal de seguridad y concentrarse en su negocio principal.

Aung et al. (2020) proponen un estudio para contrarrestar la creciente amenaza del terrorismo cibernético, se necesita seriamente el modelado de los modelos predictivos para estimar la incidencia de ataques cibernéticos para la red empresarial en Myanmar. Se utilizan modelos predictivos a pesar de que no hay registro de ataques, indefensos, resultados y amenazas. El objetivo principal es determinar si el administrador del SOC (Security Operation Center) utiliza el modelo de seguridad cibernética mediante el uso de cifras de resultados de SOC para preparar un plan adicional de ciberdefensa y respuesta a incidentes. El objetivo de este estudio se logró mediante la realización de experimentos sobre diversos ciberataques ocurridos en el centro de operaciones de seguridad del Sistema de Control Industrial (ICS).

Perera et al. (2019) Propone en su artículo científico “Intelligent SOC Chatbot for Security Operation Center” dice que los analistas de seguridad de la información se enfrentan actualmente a muchos desafíos: tanto ocultos como visibles frente a registros de ataques únicos. Los patrones de rápido aumento de las herramientas de investigación y monitoreo de seguridad (ya que se ha utilizado un promedio de 20 soluciones de

seguridad por empresa) conducen a cambios frecuentes entre pantallas, fatiga de alertas, mantenimiento de registros inconexos y un mayor tiempo de investigación. Utilizan un chat Bot y este puede sugerir el flujo de investigación y los comandos relevantes que ayudarán a obtener los resultados que deben resolverse en el incidente. Automatizar la creación de tickets de incidentes es uno de los principales logros de esta investigación. Los analistas de seguridad también reciben mensajes de alertas de seguridad de las instancias alojadas en AWS. También acota en este estudio que los analistas de seguridad continúan trabajando en sus subtareas, bastante sobrecargados con sus tareas principales para participar en investigaciones colaborativas e intercambio de conocimientos. Los Chat-Ops ayudan a vencer y enfrentar esos desafíos. Los procesos, los flujos de trabajo automatizados, el chatbot, las herramientas de seguridad y los seres humanos existen en la misma ventana de chat que alimentan los datos y los comandos en un ciclo digno. Dará lugar a grandes cambios en todo, desde los tiempos de remediación y la profundidad de la investigación hasta el aprendizaje futuro y la administración del conocimiento. Diferentes analistas impulsarán la investigación de diferentes maneras. La mayoría de las veces, los analistas perderán las partes y técnicas más importantes, pero esas partes podrían ser muy valiosas para el resultado. El flujo de investigación y los comandos sugerirán basados en investigaciones y comandos anteriores que se utilizaron analistas anteriores.

(Vielberth, Böhm, Fichtinger, & Pernul, 2020) En su artículo científico evalúa que desde la introducción de los Centros de Operaciones de Seguridad (SOC) hace unos 15 años, su importancia ha crecido significativamente, especialmente en los últimos cinco años. Esto se debe principalmente a la necesidad primordial de prevenir incidentes cibernéticos importantes y la consiguiente adopción de operaciones de seguridad centralizadas en las empresas. A pesar de su popularidad, el trabajo académico existente sobre el tema carece de una visión generalmente aceptada y se enfoca principalmente

en fragmentos en lugar de mirarlos de manera integral. Estas deficiencias impiden una mayor innovación. En este documento, se realiza una encuesta exhaustiva de la literatura para recopilar diferentes puntos de vista. La literatura descubierta se utiliza luego para determinar el estado actual de la técnica de los SOC y derivar los bloques de construcción primarios. Se identifican y resumen los desafíos actuales dentro de un SOC. Una deficiencia notable de la investigación académica es su enfoque en los aspectos humanos y tecnológicos de un SOC mientras descuida la conexión de estas dos áreas por procesos específicos (especialmente por procesos no técnicos). Sin embargo, esta área es esencial para aprovechar todo el potencial de un SOC en el futuro.

Capítulo III

Diseño del servicio Basado en Itil

Situación Actual de la Espe

La Universidad Politécnica del Ejército ESPE que es su nombre original y con el transcurso de los años se cambió a Universidad de las Fuerzas Armadas desde su fundación hace 100 años en 1922, siempre se la considerado una de las universidades más innovadoras y que da un gran aporte de excelentes profesionales al país, desde el pregrado, postgrado.

A partir del 2014 que se empezó a calificar a las universidades según varias normas internacionales la ESPE fue clasificada dentro del Ranking Mundial de Universidades QS dentro de las 250 más destacadas de América del Sur y en nuestro país como la Cuarta mejor.

La ESPE se encuentra amparada bajo la Ley Orgánica de Educación Superior y por la Constitución del Ecuador, luego de la firma del Estatuto para su creación el 26 de Junio del 2013 por las CES (Consejo de Educación Superior)

La Universidad cuenta con el Plan estratégico de Tecnologías de la Información y comunicación (ESPE, Reglamento Organico del Gestion Organizacional por procesos de la ESPE, 2015) de la cual se desprenden los siguientes incisos.

Misión

“Formar profesionales e investigadores de excelencia, creativos, humanistas, con capacidad de liderazgo, pensamiento crítico y alta conciencia ciudadana; generar y aplicar el conocimiento científico; y transferir tecnología, en el ámbito de sus dominios académicos, para contribuir con el desarrollo nacional y atender las necesidades de la sociedad y de las Fuerzas Armadas” (ESPE, Plan Estratégico de Desarrollo Institucional, 2018).

Visión

"La Universidad de las Fuerzas Armadas- ESPE es reconocida, como un referente a nivel nacional y regional por su contribución en el ámbito de sus dominios académicos, al fortalecimiento de la Seguridad y la Defensa, bajo un marco de valores éticos, cívicos y de servicio a la comunidad" (ESPE, Plan Estratégico de Desarrollo Institucional, 2018).

Valores Institucionales

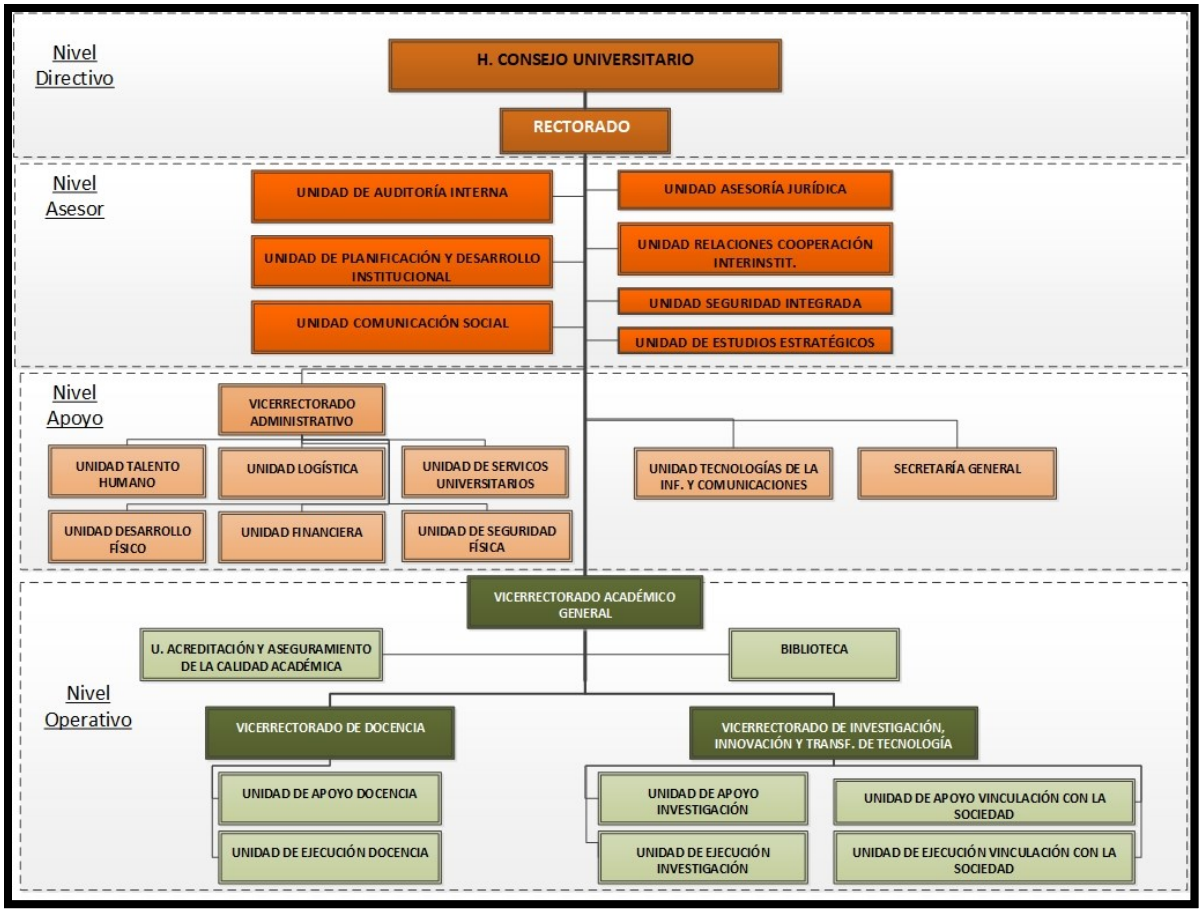
- Civismo
- Compromiso institucional
- Responsabilidad social
- Disciplina
- Identidad
- Respeto por la dignidad humana (ESPE, 2018).

Estructura Organizacional

En la Figura que tenemos a continuación esta la estructura organizacional por procesos de las unidades administrativas.

Figura 12

Estructura Organizacional de la ESPE



Nota. Diagrama de cómo se encuentra organizada la ESPE, tomado de Pagina web ESPE, 2021.

Sedes y Estudiantes

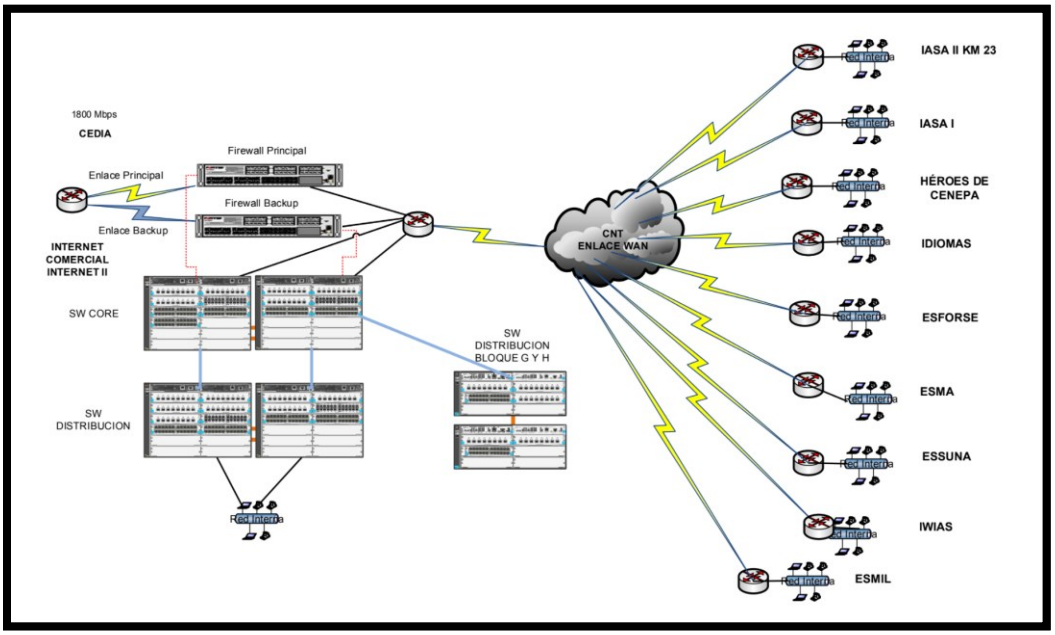
La Espe es parte del Sistema de Educación Superior del Ecuador, y está conformada por 4 sedes: la matriz en Sangolquí, las sedes Latacunga y Santo Domingo de los Tsáchilas, así como las Unidades Académicas Especiales y el Instituto de Idiomas; entre los cuales se dispone de 20.000 estudiantes entre civiles y militares.

Infraestructura

En diagrama que tenemos a continuación podemos observar el sistema de redes y comunicaciones de la universidad, el enlace al internet y varios equipos de seguridad que posee la universidad.

Figura 13

Diagrama de Red

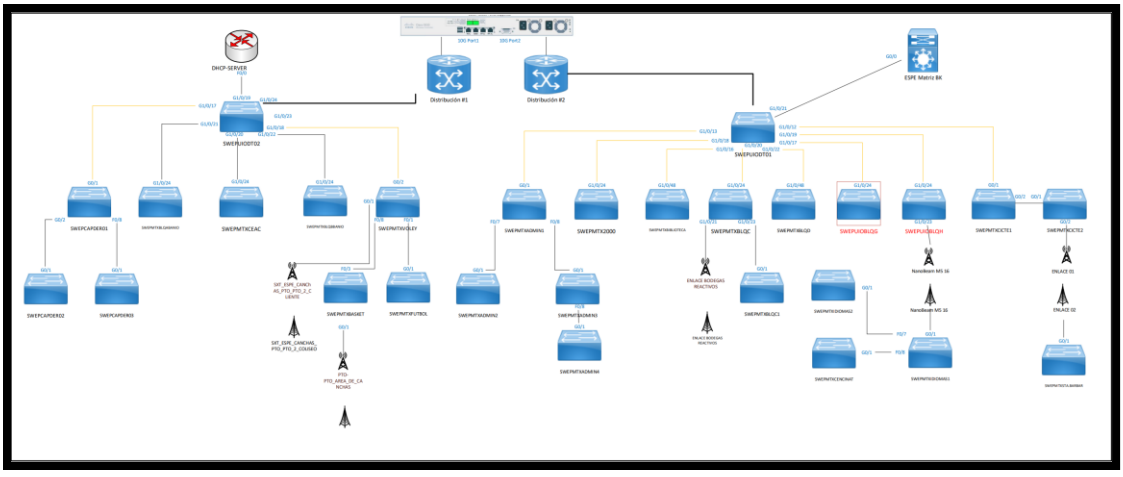


Nota. Esta Figura fue tomada de los archivos de las UTICS.

El servicio de internet ofrecido dentro la universidad funciona de forma inalámbrica y por cableado estructurado, el mismo servicio es ofrecido tanto en la matriz como en las demás sedes.

Figura 14

Diagrama de red inalámbrica de la Espe



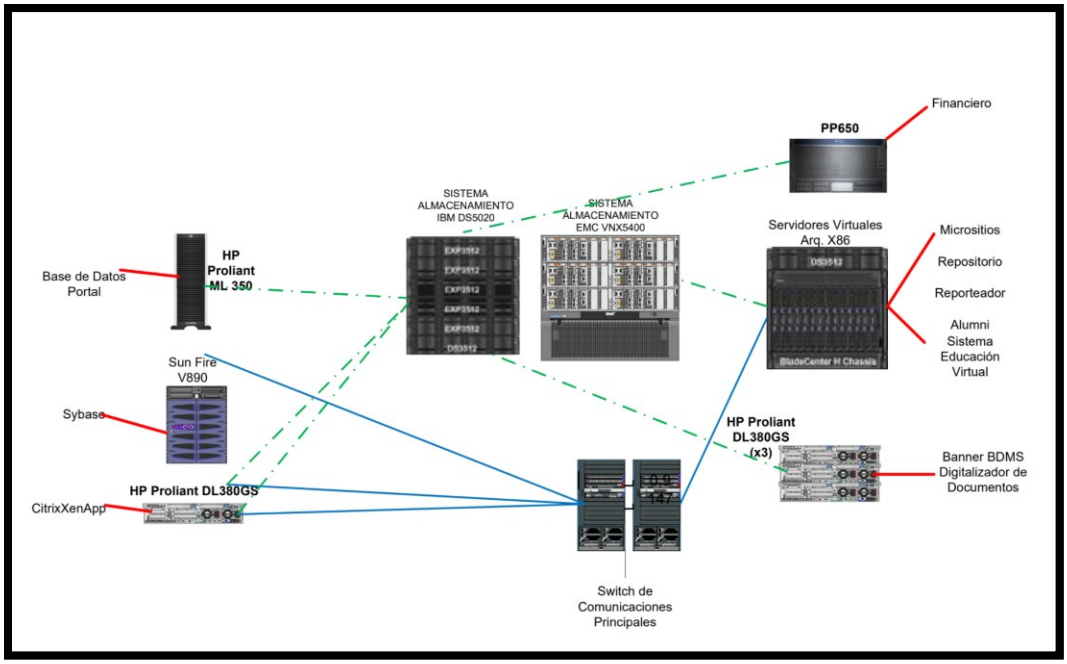
Nota. Esta Figura fue tomada de los archivos de las UTICS.

Servidores

Los servidores que se utilizan por UTIC para brindar todos las aplicaciones y servicios de tecnologías las mismas que se encuentran instalados en todos los servidores virtuales y físicos.

Figura 15

Distribución de las aplicaciones en los servidores físicos ESPE



Nota. Diagrama de la distribución de las aplicaciones de los servidores de la ESPE, tomado de UTICS, 2021.

Catálogo de Servicio Tecnológicos

Los servicios de Tecnologías de la Información y Comunicación los describimos a continuación:

Tabla 3

Catálogo de Servicios Tecnológicos de la ESPE

Servicios	Accesos
Sistema de Gestión Académica	A través de la web
Servicios Web	A través de la Web
Sistemas de gestión Administrativa	A través de la web
Sistema Banner- Administrativo (RRHH)	At través de la web
Sistema Banner- Digitalización Sistema Banner – Workflow	
Sistema Banner – MiEspe	
Sistema Ex alumnos ALUMNO	
Sistemas de Gestión Administrativa	Dentro de Intranet
Sistema SIFRHE	
Sistemas Olympo (Contabilidad, Facturación, Inventario, Especies, Activos Fijos)	
Repositorios Digitales de archivos	A través de la web
Soporte Técnico Mantenimiento	En la universidad o externa a través del teléfono
Internet/Wifi	Internet Comercial avanzando a través de cableado Wifi requiere de una autenticación
Correo institucional	A través del portal
Telefonía	Por llamada internas y nacionales, se requiere de una clave
Videoconferencias	Las salas de video conferencias virtuales que se crean constantemente
Virtualización de servidores	De acuerdo a los requerimientos
Alojamiento de infraestructura	De acuerdo a los requerimientos

Nota. Servicios tecnológicos de la ESPE, tomado de UTIC ESPE, 2015.

Provisión de servicios

La UTIC para atención a los alumnos cuentas con una mesa de servicios mediante la cual se ejecuta la atención sobre los incidentes del sistema en nivel 0 y 1, también se atiende del hardware hasta el nivel 2.

Plan de Contingencia

Dentro del plan de contingencias se ejecuta diferentes fichas con los procedimientos para incidentes como:

- No tener accesibilidad de los sistemas
- Daño en la red de datos

- Incendio de las instalaciones
- Pandemia mundial
- Daño en componentes físicos
- Desastres naturales: terremotos, sismos
- Suspensión de energía
- Defecto en el motor de base de datos
- Defecto en el sistema operativo
- Ciberataques
- Ataques terroristas
- Daño de la telefonía IP
- Daño de equipos de seguridad perimetral.

Plan estratégico

Introducción

La tecnología cada vez crece a pasos agigantados y en este caso tan especial por la Pandemia que se encuentra atravesando el mundo, la tecnología ha crecido con una rapidez única revolucionado los diferentes aplicativos y programas que usamos todo el tiempo, con varias vulnerabilidades e inseguridades.

Debido a esto muchos procesos se automatizaron permitiendo tener toda la información de manera digital. Siendo así que la información se la almacena de manera lógica en una base de datos y se ocupe software para el manejo de la misma, tomando en consideración la implementación de seguridades informáticas para que la información sea integra y disponible todo el tiempo.

Por este motivo se ha planteado instalar un SOC en la Universidad de las fuerzas Armadas ESPE, donde se manejará la información sensible tanto de alumnos como de profesores y sus notas académicas, se está creando un servicio de monitoreo y mitigación

de los mismos siendo el SOC el centro de protección y respuesta a incidentes sobre toda la información que manera la comunidad ESPE.

Fortalezas

- Disponer de profesionales con conocimientos sobre seguridades informáticas.
- Iniciar un equipamiento idóneo para ofrecer un servicio tecnológico de la mano con la ciberseguridad
- Disponer de la infraestructura física.

Oportunidades

- Iniciar las investigaciones sobre la creación de procesos para aplacar los ataques informáticos.
- Contar con el apoyo de entidades externas para mejorar la ciberseguridad.
- Realizar convenios entre universidades sobre temas relacionados a la ciberseguridad.
- Realizar capacitaciones a todo el personal que trabaja con ciberseguridad.

Debilidades

- Falta de capacitación en ciberseguridad a todo el personal que maneja ciberseguridad por falta de presupuesto por parte del estado por las medidas de austeridad por la Pandemia.
- Poca colaboración de docentes para que colaboren en el proyecto.

Amenazas

- Presupuesto reducido por la pandemia y la crisis mundial.
- Deficiencia en la creación de políticas de ciberseguridad a nivel nacional.

Principios

- Trabajar siempre por ofrecer un servicio de alta calidad basándonos en todos los preceptos de ITIL.

- El crecimiento del SOC en brindar los servicios ira enlazado fuertemente con el continuo crecimiento de la comunidad universitarias y sus necesidades.
- Siempre a la vanguardia del desarrollo tecnológico para poder ofrecer un mejor servicio constantemente.
- Trabajar de manera conjunta con otros sistemas como es el CSIRT para poder resolver de una manera más eficiente los incidentes futuros.

Valores

- **Honestidad** Virtud indispensable del ser humano que es parte del SOC actuando correctamente en todo momento cuando lo vean y cuando no.
- **Tenacidad:** Capacidad que caracterizada a todos los miembros del SOC para siempre cumplir con todos los objetivos.
- **Solidaridad:** Cualidad importante ya que al trabajar en equipo se podrá llegar a soluciones más optimas y rápidas.
- **Disciplina:** Virtud que debe caracterizar a todo el equipo del SOC teniendo buenos hábitos de trabajo y profesionalismo.
- **Lealtad:** Cualidad indispensable para cada miembro del equipo del SOC que nos permitirá confiar en ciegamente en el trabajo de todos.

Misión

Ofrecer el servicio de detección y mitigación temprana de ciberataques a la Universidad de Fuerzas Armadas, coadyuvando en la formación y capacitación de personal especializado en ciber seguridad.

Visión

Ejecutar un monitoreo continuo de todas las áreas informáticas dentro de la Universidad de las Fuerzas Armadas con el fin de mitigar incidentes de seguridad.

Objetivos estratégicos, indicadores y estrategias

Oe1. Innovar y acrecentar el servicio de respuesta ante incidentes sobre la seguridad de la información, para una comunidad universitaria de la ESPE.

Estrategias

- Fomentar procesos nuevos de ciberseguridad para la protección de los sistemas informáticos de la Comunidad Universitaria.
- Buscar nuevos métodos para evitar los ataques informáticos.
- Tener un constante crecimiento en la cobertura de los servicios ofrecidos debido al crecimiento constante de la comunidad.

Oe2. Ofrecer los servicios de respuesta inmediata a los incidentes de ciberseguridad de acuerdo los estándares internacionales.

Estrategias

- Aplicando estándares internacionales para la respuesta oportuna a los incidentes de ciberseguridad.
- Fomentar las relaciones internacionales con otras universidades que tengas formación en ciberseguridad.
- Realizar una valoración de forma constante a los procesos ejecutados y mejorando sobre la marcha.

Oe3. Acrecentar la contribución financiera y humana de la comunidad universitaria para el crecimiento del SOC.

Estrategias

- Cooperar en convocatorias y buscar el apoyo financiero de entidades privadas.
- Buscar el auspicio para publicaciones de artículos científicos que tengan como temas relacionados el SOC.

Análisis y Gestión de la Demanda

Con el avance de la tecnología las instituciones enfrentan cada vez más ataques en el área tecnológica por este motivo la Universidad de las Fuerzas Armadas ESPE ofrece el servicio de monitoreo de su sistema informático para la búsqueda y la mitigación de ciberataques.

Las redes de la organización se mantendrán en continuo monitoreo del SOC, contarán con la seguridad de estar protegidos antes los ciberataques, teniendo protocolos para reaccionar a ataques y frenar los mismos.

Toda la información que ingrese a nuestras bases de datos en cuanto a ataques y procesos de mitigación servirá a la comunidad universitaria como base de información y protección sobre ellos, mejorando la confidencialidad de la información sensible que se maneja dentro de la universidad.

Siempre se brindará un servicio personalizado a cada miembro de la comunidad universitaria.

Portafolio de servicios

Para realizar el portafolio de servicios que brindará el SOC, será necesario realizar una matriz de evaluación sobre las necesidades de la comunidad universitaria en cuanto a la ciberseguridad, dentro de la siguiente matriz se relacionará los funciones que cubren los servicios y el impacto sobre las actividades a desarrollarse:

Tabla 4

Matriz de Impactos de Servicios

Servicios/ Criterios	Sedes	Comunidad Universitaria (Demanda)	Infraestructura tecnología	Servicios Tecnológicos	Riesgos Tecnológicos	Investigación	Formación Profesional
Alertas y advertencias							
Manejo de Incidentes							
Manejo de Vulnerabilidad							
Manejo de problemas							
Anuncios							
Observatorio de Tecnología							
Evaluaciones o Auditorias de la Seguridad.							
Configuración y mantenimiento de las herramientas, aplicaciones, infraestructura y servicios de seguridad.							
Desarrollo de herramientas de seguridad							
Detección de intrusos							
Difusión de información relacionada con la seguridad.							
Análisis de Riesgo							
Planificación de la continuidad del Negocio y recuperación de desastres							
Consultoría de seguridad							
Concientización							
Educación/ Capacitación							
Evaluación o certificación de productos							

Interpretamos dentro de esta tabla de la siguiente manera:

Sedes: Influencia en todas las sedes y extensiones.

Comunidad Universitaria: Conformada por docentes, personal administrativo, estudiantes.

Infraestructura tecnológica: Influencia en la infraestructura física y en el hardware y software que dispone la universidad.

Servicios críticos: Mejoran la disponibilidad de los servicios que ofertados por la UTIC

Riesgos tecnológicos: Mitiga puntos ciegos para fallas principales

Investigación: Contribución al desarrollo de las investigaciones relacionadas a la ciberseguridad dentro de la Universidad.

Formación profesional: Colaboración para el desarrollo y formación de la comunidad universitaria.

En la siguiente tabla se muestra un cálculo mediante una escala de colores priorizando los servicios para el inicio del SOC:

Tabla 5

Ponderación de Impacto y Priorización de Servicios

Servicios/ Criterios	Altos	Medio	Bajo	Valor
Alertas y advertencias	4	2	1	17
Manejo de Incidentes	4	2	1	17
Manejo de Vulnerabilidad	4	2	1	17
Manejo de problemas	2	2	3	13
Anuncios	3	3	1	16
Observatorio de Tecnología	2	3	2	14
Evaluaciones o Auditorias de la Seguridad.	2	2	3	13
Configuración y mantenimiento de las herramientas, aplicaciones, infraestructura y servicios de seguridad.	1	2	4	11
Desarrollo de herramientas de seguridad	2	3	2	14

Servicios/ Criterios	Altos	Medio	Bajo	Valor
Detección de intrusos	3	1	3	14
Difusión de información relacionada con la seguridad.	6	1	0	20
Análisis de Riesgo	1	4	2	13
Planificación de la continuidad del Negocio y recuperación de desastres	2	4	1	15
Consultoría de seguridad	2	3	2	14
Concientización	5	2	0	19
Educación/ Capacitación	3	4	0	17
Evaluación o certificación de productos	1	2	4	11

El presente análisis se realizó tomando como base las necesidades de la Universidad y basado en las guías y normativas para la creación de un SOC propio, logrando los posibles servicios como lo detallamos a continuación:

Tabla 6

Propuesta Inicial de Servicios de SOC-ESPE

Tipo de servicios	Servicio
Servicios Reactivos	Alertas y advertencias Manejo de incidentes Manejo de vulnerabilidades
Servicios Proactivos	Comunicados y alertas Difusión de información relacionada con la seguridad de la información
Servicios de gestión de la Calidad de la Seguridad	Sensibilización Educación y Capacitación

Con el crecimiento del SOC- ESPE en sus etapas de desarrollo su portafolio de servicios ira avanzando, debido a la gran demanda que está en constante crecimiento la comunidad universitaria, como se detalla a continuación:

Tabla 7

Propuesta de servicios para el crecimiento del SOC-ESPE

Tipo de servicios	Servicios
Servicios Reactivos	• Manejo de problemas
Servicios Proactivos	• Observatorio de tecnología • Evaluaciones o auditorias de seguridad • Desarrollo de herramientas de seguridad • Detección de intrusos
Servicios de gestión de la Calidad de la Seguridad	• Análisis de riesgos • Consultoría de seguridad • Continuidad del negocios y recuperación después de un desastre.

Políticas y Procedimientos

Para empezar con la instalación del SOC se han propuesto políticas y procedimientos para la elaboración de instructivos para el inicio del funcionamiento del SOC entre algunas de ellas tenemos: Políticas de divulgación y distribución de información y Procesos para el manejo de incidentes.

Estructura Organizacional

Modelo Organizacional

El modelo organizacional va hacer el interno central, debido a que los servicios de TI que maneja la universidad van desde su matriz en Sangolquí hacia las diferente sedes y extensiones. Entonces el SOC-ESPE se ubicará en un sitio central, recopilando y diseminando toda la información de varias fuentes de entrada y salida de la universidad. Adicional a este trabajo, el SOC mantendrá la responsabilidad de manejar la elaboración de informes y análisis de incidentes se presenten, pudiendo publicar advertencias, procedimientos de mejores prácticas, pasos y recuperación de incidentes que puedan suceder.

El SOC-ESPE centralizado va a trabajar cohesionados con los expertos de la unidad de información de universidad (UTIC), debido a la extensión de la universidad no se podrá ofrecer respuesta a incidentes insitu, pero se lo realizará de manera remota ante cualquier requerimiento.

Organización por procesos

El SOC en cuanto a los proyectos se a organizado en tres procesos importantes que son los que detallo a continuación:

a) **Procesos gobernantes**

Descripción: Coordinación directa y asesoría de procesos estratégicos de la institución con el SOC

Responsable: Analista de seguridad

Descripción: gerencia del laboratorio con la organización y el control de la provisión de servicios.

Responsable: Director SOC

b) **Procesos Generadores de Valor**

Descripción: Preparación, monitoreo y rastreo de incidentes de seguridad que se pueda reflejar como un evento de seguridad informática.

Responsable: Operador -Monitoreo de redes.

Descripción: Manejo, análisis y prevención de incidentes.

Responsable: Analista de Seguridad- operador.

Descripción. Preparación de talleres y elaboración de cursos sobre las actividades a realizarse dentro del SOC.

Responsable: Director

c) **Procesos de apoyo**

Descripción: Organizador y planificador de presupuestos y financiamiento del sector donde se va a ubicar el SOC- ESPE.

Responsable: Director-Operador- analista de finanzas

Jerarquía organizacional

Dentro de la organización, el SOC se encontrara dependiente de la UTIC.

Responsabilidades del SOC

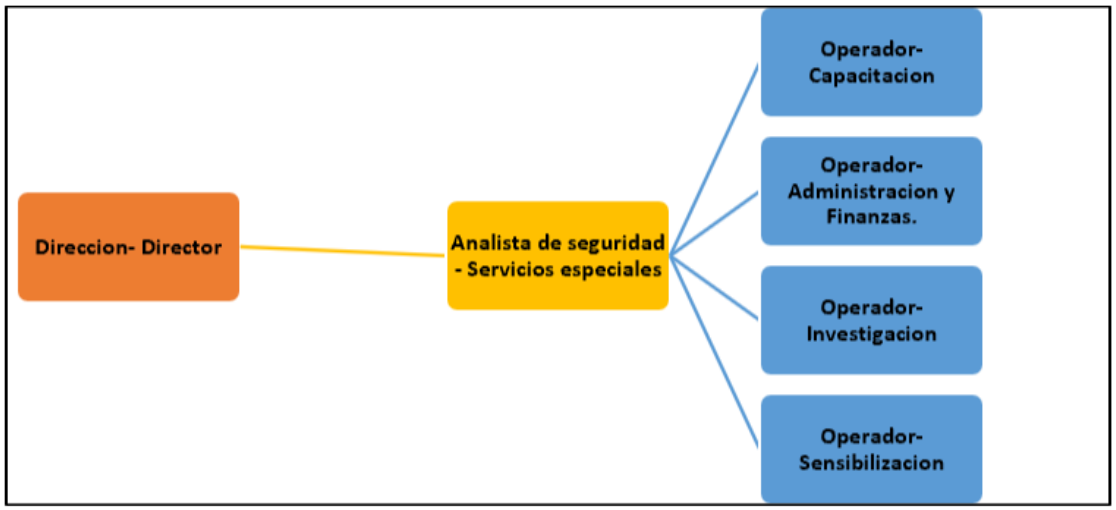
- Difundir información sobre alertas y advertencia a la ciberseguridad.
- Ofrecer consultoría y asesoramiento en temas sobre la ciberseguridad.
- Tener un conocimiento actualizado sobre los procedimientos para una respuesta efectiva y oportuna a los incidentes.
- Tener una buena relación con la comunidad de los diferentes SOC´s Nacionales y extranjeros.
- Monitorizar, analizar y procesar incidentes y vulnerabilidades.

Clasificación de Puestos-Especificaciones de clase

El SOC – ESPE al tener una ubicación central dentro de la universidad se encarga de coordinar las actividades de la institución y tendrá la siguiente clasificación:

Figura 16

Clasificación de puestos SOC



A continuación, detallo los puestos específicos para el SOC:

Tabla 8

Especificaciones Puesto director general

No.	Primer Puesto
Denominación del Puesto	Director General
Objetivos	Organizar y ser parte del control de los procesos del SOC
Responsabilidades	• Capacidad para planificar y organizar al equipo del SOC • Aprobar acciones del SOC basadas en sus experiencia y conocimiento. • Tener un control continuo del avance del SOC. • Controlar el cumplimiento de las actividades Programadas. • Elaborar los informes y reportes periódicos • Aplicar estrategias para la aprobación de los gerentes • Notificar novedades a las unidades subordinadas.
Características del Puesto	Responsable directo de la administración y gestión del SOC.
Competencias Técnicas/Actitudinales	• Grado de Magister en informática o afines. • Capacidad de actuar autónomamente. • Poder aportar soluciones o alternativas novedades. • Capacidades de comunicación. • Aptitud para una relación intrapersonal. • Capacidad de razonamiento y desarrollo de resolución de problemas. • Demostrar conocimiento y comprensión dentro SOC.
Autoridad y accesos	Toda la información del SOC

Tabla 9

Especificaciones del puesto de investigador

No.	**Segundo Puesto**
Denominación del Puesto	Operador- Investigador
Objetivos	Realiza labores de investigación Científica y tecnológica
Responsabilidades	• Diseñar e implementar proyecto de investigación. • Realizar un fortalecimiento de la investigación continuo al SOC. • Realizar investigaciones para la publicación de alertas y advertencias de ciberseguridad. • Reportar avances de todas sus tareas. • Participar en eventos sobre nueva información sobre incidentes y advertencias • Cumplir con todas las actividades programadas. • Elaborar informar y reportes periódicos.
Características del Puesto	Responsable de los proyectos de investigación del SOC-ESPE.
Competencias Técnicas/Actitudinales	• Grado de Magister en informática o afines. • Capacidad de actuar autónomamente. • Poder aportar soluciones o alternativas novedades. • Capacidades de comunicación. • Aptitud para una relación intrapersonal. • Capacidad de razonamiento y desarrollo de resolución de problemas. • Demostrar conocimiento y comprensión dentro SOC.
Autoridad y accesos	A toda la red de información para la mejorar del SOC.

Tabla 10

Especificaciones del puesto de Analista de servicios especiales

No.	**Tercer puesto**
Denominación del Puesto	Analista seguridad- servicios especiales- Monitor de Redes
Objetivos	Análisis de incidentes y vulnerabilidades dentro del SOC-ESPE y Monitorear, detectar los eventos que se puedan convertir en incidentes contra la seguridad informática
Responsabilidades	• Localizar vulnerabilidad y explorar su afectación y solución. • Ejecutar los análisis al hardware y software de forma técnica. • Identificar alcance, extensión de daño, estrategias y soluciones a los posibles incidentes. • Reportar avances de tareas programadas • Elaborar informes y reportes periódicos. • Realizar los procedimientos operativos para garantizar una efectiva monitorización • Coordinar, dirigir planear y evaluación la utilización de herramientas de monitoreo • Administrar la información sensible del monitoreo realizado periódicamente. • Reportar avances y cumplimiento de de todas las actividades programadas.
Características del Puesto	Responsable de realizar los procedimientos de análisis técnicos para los posibles incidentes y vulnerabilidades.
Competencias Técnicas/Actitudinales	• Grado de Magister en informática o afines. • Capacidad de actuar autónomamente. • Tener motivación. • Poder aportar soluciones o alternativas novedades. • Capacidades de comunicación. • Aptitud para una relación intrapersonal. • Capacidad de razonamiento y desarrollo de resolución de problemas. • Demostrar conocimiento y comprensión dentro SOC.
Autoridad y accesos	A todos los incidentes u eventos A todos los sistemas informáticos de la universidad Ambientes de prueba.

Tabla 11

Especificaciones del Puesto de Capacitador

No.	**Cuarto Puesto**
Denominación del Puesto	Operador- Capacitador
Objetivos	Proveer información acerca de las actividades principales realizadas para la seguridad de la información.
Responsabilidades	• Dar capacitaciones sobre seguridad informática, como son talleres, cursos y tutoriales. • Recomendar mejorar continuas en la resolución de incidentes • Recopilar, investigar ya analizar nuevos desarrollos técnicos, actividades de posibles intrusos y las últimas tendencias con el fin de identificar posibles amenazas. • Llevar el control de todas las capacitaciones impartidas • Reportar avances de sus tareas • Cumplir con actividades programadas • Elaborar informes y reportes periódicos
Características del Puesto	Responsable de brindar toda la información y capacitación sobre ciberseguridad.
Competencias Técnicas/Actitudinales	• Grado de Magister en informática o afines. • Capacidad de actuar autónomamente. • Poder aportar soluciones o alternativas novedades. • Capacidades de comunicación. • Aptitud para una relación intrapersonal. • Tener motivación. • Capacidad de razonamiento y desarrollo de resolución de problemas. • Demostrar conocimiento y comprensión dentro SOC.
Autoridad y accesos	Toda la información de seguridad informática, mejores prácticas de seguridad de la información Documentar el desempeño de los pasantes.

Tabla 12

Especificaciones del Puesto de Concientizador

No.	**Quinto Puesto**
Denominación del Puesto	Operador- Concientizador
Objetivos	Dirige el cumplimiento de las buenas prácticas de seguridad informática.
Responsabilidades	• Busca continua para generar conciencia sobre la seguridad informática. • Sensibilizar el cumplimento de prácticas de seguridad. • Sensibilizar la comprensión de cada problema de seguridad que se genera por no cumplir con los estándares implementados dentro de la universidad • Ejecutar reuniones, semanarios, boletines sobre seguridad informática. • Recopilar, investigar y analizar nuevos ataques informáticos en los organismos internaciones. • Reportar avances de sus tareas programadas • Cumplir con actividades programadas • Elaborar informes y reportes periódicos.
Características del Puesto	Responsable de generar conciencia a todos los integrantes de la comunidad universitaria sobre la seguridad informática.
Competencias Técnicas/Actitudinales	• Grado de Magister en informática o afines. • Capacidad de actuar autónomamente. • Poder aportar soluciones o alternativas novedades. • Capacidades de comunicación. • Aptitud para una relación intrapersonal. • Capacidad de razonamiento y desarrollo de resolución de problemas. • Tener motivación. • Demostrar conocimiento y comprensión dentro SOC.
Autoridad y accesos	A toda la información de la seguridad informática, mejores prácticas de seguridad. Documentar el desempeño de los sensibilizados

Tabla 13

Especificaciones del puesto de analista administrativo financiero

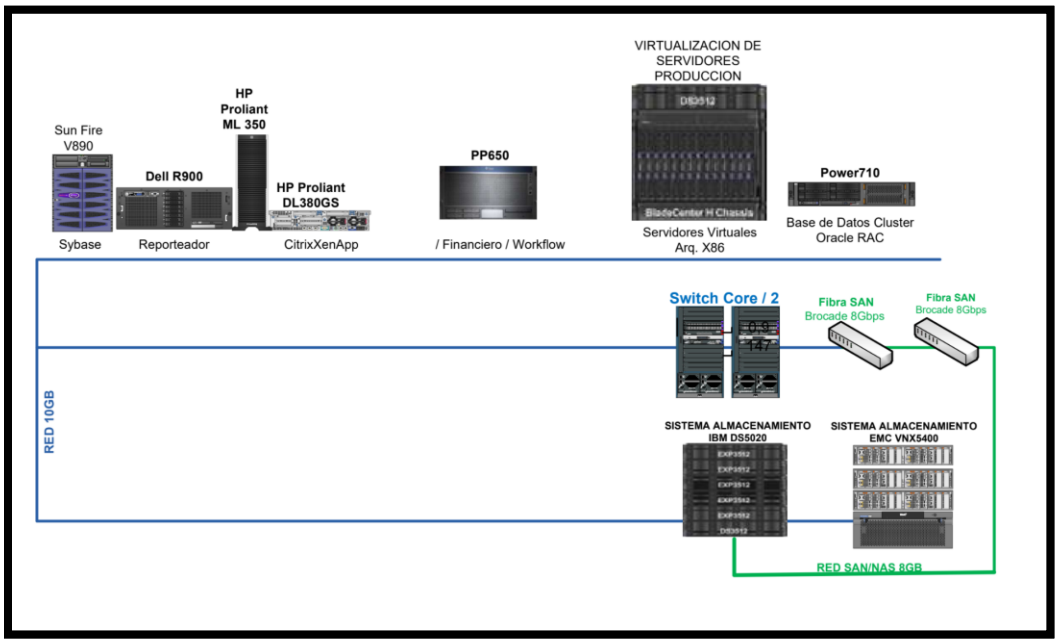
No.	**Sexto Puesto**
Denominación del Puesto	Operador -Administración y finanzas
Objetivos	Coordinar servicios administrativos y apoyo logísticos al SOC.
Responsabilidades	• Registrar plan de comprar de bienes. • Planificar, organizar y controlar presupuestos asignados para el SOC. • Proponer mejorar para optimizar recursos y servicios. • Establecer cronogramas de ejecución. • Reportar el avance de sus tareas • Cumplir con las actividades programas. • Elaborar informes y reportes periódicos.
Características del Puesto	Responsable de apoyar las actividades de manejo de servicio administrativos y de apoyo logístico.
Competencias Técnicas/Actitudinales	• Grado de Magister en informática o afines. • Capacidad de actuar autónomamente. • Poder aportar soluciones o alternativas novedades. • Capacidades de comunicación. • Aptitud para una relación intrapersonal. • Capacidad de razonamiento y desarrollo de resolución de problemas. • Demostrar conocimiento y comprensión dentro SOC.
Autoridad y accesos	A toda la información de infraestructura, equipamiento, presupuesto y financiamiento.

Infraestructura y equipamiento

a. Infraestructura del centro de datos de la UTIC

Figura 17

Infraestructura de las UTICS



Nota. Tomado de la infraestructura de la ESPE

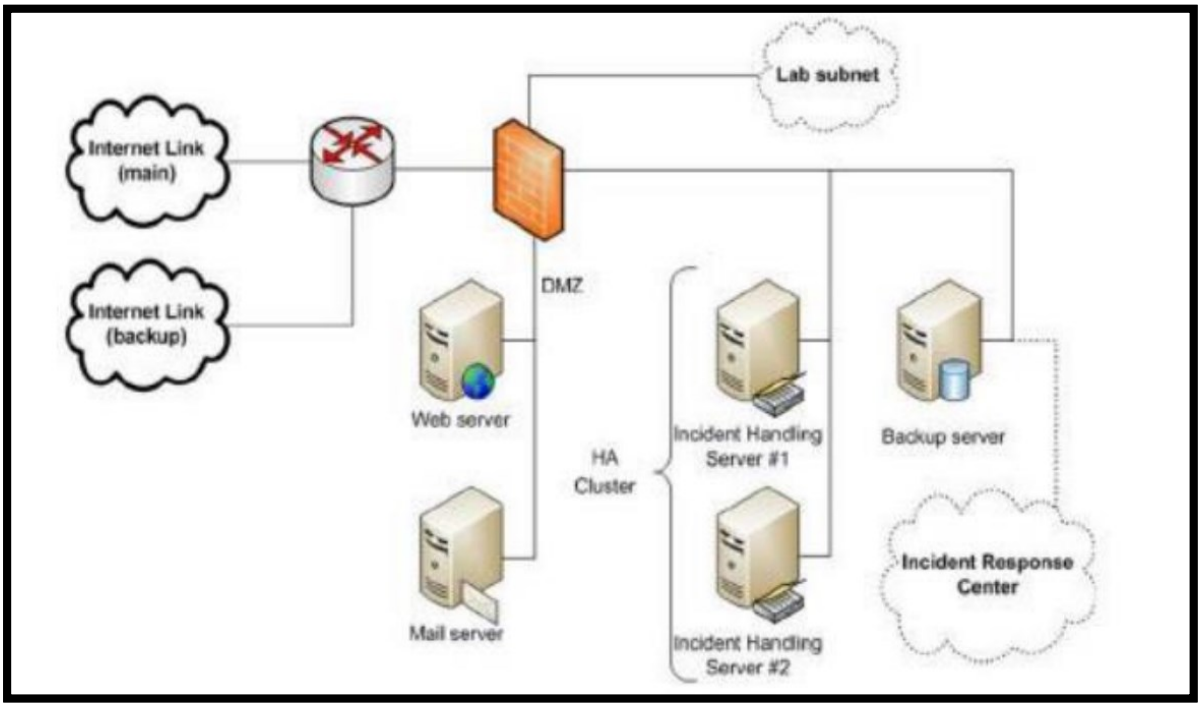
b. Infraestructura del laboratorio SOC-ESPE

Infraestructura Inicial del SOC

Iniciando la primera etapa del SOC con la implementación de los servicios básicos se propone una red simple como mostramos a continuación.

Figura 18

Infraestructura Inicial SOC



Nota. Infraestructura inicial SOC-ESPE, tomado de Enisa, 2016.

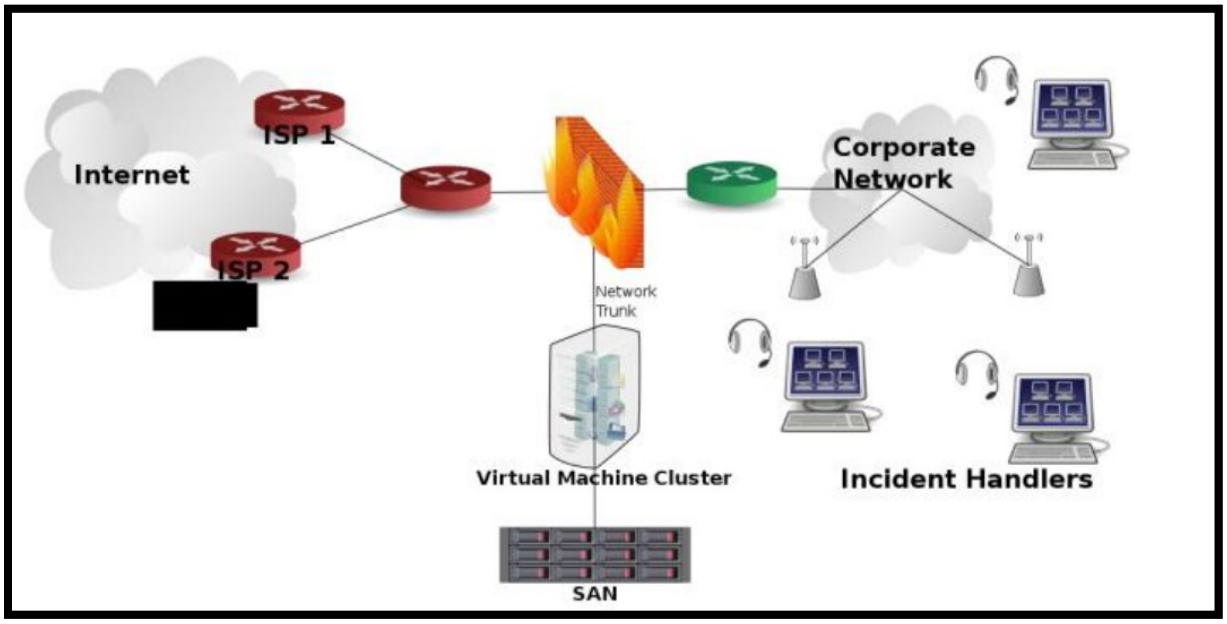
Infraestructura

Etapa de crecimiento y desarrollo

Con el pasar del tiempo las etapas de crecimiento y desarrollo del SOC nos permitirán ir mejorando la infraestructura junto con más tecnologías.

Figura 19

Infraestructura futura



Nota. Infraestructura Futura SOC-ESPE, tomado de Enisa, 2016.

INFRAESTRUCTURA	Software
• **Hardware** • Servidor web • Servidor de correo • Servidor de manejo de incidentes (2) • Servidor de backup. • Computadoras de escritorio. • Notebook. • Impresoras láser Jet.	• Software escaneo de puertos (Nmap). • Software escaneo de redes (nagios). • Software gestión de vulnerabilidades (nessu, metasploit, kali). • Software detección de intrusos (Snort, Tripwire). • Software seguimiento incidentes (Request tracker,). • Software almacenamiento datos (Mysql)

c. Propuesta de ubicación Física

El centro de Operaciones de Seguridad se encontrará dentro de la unidad de UTIC, en el primer piso, en una oficina designada para este servicio a la universidad y se

encontrará adecuado de manera correcta. Se designo este sitio debido a la seguridad que posee, con accesos dependente las UTIC, posee acceso a todos los sistemas y la cercanía a los mismo.

Planes de seguridad, recuperación de desastres y continuidad de servicios

Plan de seguridad

Como hemos venido argumentando a lo largo de todo el presente trabajo existen muchos riesgos en cuanto a la ciberseguridad y para poder mitigar esta amenaza se a elaborado un Plan de Seguridad el mismo que es aplicable en toda la Universidad de las Fuerzas Armadas ESPE. (Plan de seguridad Anexo A.)

Plan de recuperación de desastres

Los desastres naturales cuando ocurren dañan todo tipo de bien material y a los que menos les prestamos atención son los sistemas informáticos los mismos que son más sensibles que otros bienes materiales y si no se elabora un plan de recuperación de la información con antelación se pierde toda la información.

El plan de recuperación de desastres está conformado por 2 partes, la primera se indica como seguirá funcionando la institución mientras se recupera del desastre que en ese momento este sufriendo la institución y la segunda parte como recuperar la información perdida durante el desastre. (Anexo A. Plan de recuperación de desastres.)

Plan de continuidad de servicios

El SOC al brindar el servicio de protección y la mitigación de ciberataques garantizando la disponibilidad de sus servidores, de esta formar se puede cumplir con todos los objetivos planteados por el SOC brindando un servicio de calidad a las organizaciones que disponen de un SOC propio.

Motivo suficiente para que exista el Plan de continuidad de Servicios dentro del cual se exponen varios métodos para solventar las caídas del servicio y poder recuperar

el mismo en el menor tiempo posible, con varios planes de mitigación sobre este tipo de incidentes (Anexo A. Plan de Continuidad de Servicios)

Presupuesto y Financiamiento

Teniendo en cuenta que el SOC se va alojar en las UTICS, en su etapa inicial se instalara en un espacio ya existente, instalándose con el mobiliario existente, adicional dentro de la adquisición de hardware y software se utilizara la infraestructura de networking y almacenamiento de alto rendimiento, también ocuparemos herramientas de código abierto que no tienen costo, tomando en cuenta todo esto se realizó un presupuesto referencia como detallo a continuación:

Tabla 14

Presupuesto referencial de Equipos de oficina

Equipos de Oficina	Cantidad	Precio Uni.	Subtotal
Computadores de escritorio	8	400	3200
Impresora multifuncional	1	500	500
Sillas	8	40	320
Escritorios de trabajo	8	150	1200
Archivadores de pared	4	60	240
Armarios	1	200	200
Suministros de oficina	1	1300	1300
TOTAL			6960

Tabla 15

Presupuesto referencia Hardware

Hardware	Cantidad	Precio Uni.	Subtotal
Servidores Físicos	1	25000	25000
Sistema de almacenamiento Unificado EMC VNX	1	8000	8000
Sistema de respaldo EMC AVAMAR	1	8000	8000
TOTAL			41000

Tabla 16

Presupuesto referencial Software

Software	Cantidad	Precio Uni.	Subtotal
Soporte herramientas de código abierto	12	350	4200
TOTAL			4200

Diseño y cronograma de implantación del proyecto

Tabla 17

Cronograma de implantación del Proyecto

Ord.	Tarea	Ord	Inicia	Termina
1	Presentación y aprobación del Proyecto.	**2**	01/10/2021	15/10/2021
2	Comunicar la visión y plan Operativos del SOC	**1**	15/10/2021	22/10/2021
3	Asignación de recursos	**2**	22/10/2021	08/11/2021
4	Adquisiciones, contrataciones	**3**	08/11/2021	27/11/2021
5	Instalación y configuraciones	**2**	27/11/2021	10/12/2021
6	Capacitación	**2**	10/12/2021	02/01/2022
7	Elaboración de pruebas	**3**	03/01/2022	31/01/2022
8	Establecimiento de acuerdo de niveles de servicio	**2**	01/02/2022	20/02/2022
9	Evaluación y operación	**3**	20/02/2022	26/03/2022

Definición de indicadores de evaluación de la implantación del proyecto

Tabla 18

Indicadores de evaluación de la implantación del proyecto SOC-ESPE

Metas	Resultados	Índices de Medición
Creación formal del equipo SOC-ESPE	Equipos de respuesta conformado y establecido formalmente	Acta de aprobación de proyecto
Comunicar el plan estratégico del SOC	Publicación del Plan estratégicos (Misión, visión, valores, objetivos estratégicos, estrategias) por medio de la comunicación interna de la universidad (Correos, página institucional)	Cantidad de personas informadas del SOC **Indicador** Número de estudiantes, docentes, investigadores y personal administrativo informados frente al número total de estudiantes, docentes investigadores y personal administrativo no informado
Asignación de recursos	Adecuación de las instalaciones y oficinas	Centro SOC Entregado
Adquisiciones, contrataciones	Adquisición de equipos	Cantidad de equipos, material de oficina, hardware, software y otros requerimientos
Instalaciones y configuraciones	Instalación y configuración completadas del software y hardware.	Cantidad de software y hardware instalado frente al software y hardware requerido.
Capacitación	Capacitaciones en los procesos diseñados con el personal asignado.	Actas de capacitación elaboradas
Elaboración de pruebas	Realización de pruebas y validaciones (Satisfactoria, erróneas, corregidas).	Numero de pruebas satisfactorias frente al número de pruebas realizadas.
Establecimiento de acuerdo de niveles de servicio	Conciencia del tipo y calidad de servicios que se brindara por los representantes de la comunidad y proveedores internos, externos.	Cantidad de (SLA, OLA) firmados con los clientes.
Evaluación	Parámetros del diseño establecido evaluado por el personal designado	Informe de procesos.

Capítulo IV

Transición de Servicios basado en ITIL

Plan de transición

INFORMACION GENERAL

1. **Nombre del proyecto:**

Creación de un Centro de Seguridad SOC-ESPE en las UTICS de la ESPE

2. **Fecha:** Febrero del 2022
3. **Área de gestión Estratégica:** Seguridad Informática.
4. **Objetivo Estratégico:**

Incrementar la producción científica, académica y tecnológica de calidad, con énfasis en el ámbito de la seguridad y la defensa.

5. **Estrategia:**

Fortalece los centros de investigación tecnológica aplicada a la industria e la defensa.

6. **Unidades Responsables:**

Departamento de Ciencias de la Computación (DECC) y Unidad de Tecnologías de la Información (UTICS).

7. **Responsable del proyecto:**

Ing. Mario B. Ron Egas – Docente Tiempo completo DECC

Capt. Maria J. Angos Cosios – Alumna de la Carrera de Ing. en sistemas.

8. **Tiempo de ejecución**

Aproximadamente 6 meses de implementación

Antecedentes:

Con el avance de los servicios digitales alrededor del mundo , todo el tiempo son más las organizaciones que requieren un acceso constante, permanente y que su infraestructura dependa básicamente de la posibilidad que tienen todos sus clientes del ingreso al internet es así que por la situación mundial todos los servicios se han vuelto digitales convirtiéndolos en dependientes de una conectividad permanente y la interrupción de esta pudiera provocar grandes pérdidas económicas a nivel mundial regional y local.

Motivo por el cual la actividad maliciosa digital se ha incrementado a pasos agigantados y ahora se ha convertido en una prioridad la inversión ya no el gasto en: contención, resolución y daños potenciales la protección contra estos ataques, la respuesta clave a estos incidentes es el actuar de forma rápida y eficaz.

Tomando en cuenta lo expresado anteriormente entra en contexto el SOC, con un equipo de técnicos-expertos en seguridad de la información de TI que dan una respuesta a oportuna ha incidentes y amenazas de ciberseguridad, los mismo que poseen la formación académica y la experticia para poder detectar y manejar dichos incidentes, donde se mitigara las vulnerabilidades y los riesgos que se pueden presentar.

Cuando suceden los ataques se debe responder oportunamente para poder contener el daño actual y mitigar daños futuros y colaterales.

De acuerdo con (Ron Egas Mario, 2017) en algunos países de Sudamérica se han implementado los SOC Nacionales para brindar apoyo a las necesidades de seguridad en entidades del estado. A pesar de ello, no proporcionaron la ayuda esperada, en la mayoría de los casos por falta de formación y expertiz, y la solución de las universidades

es simplemente prescindir de la creación de un SOC. En la región latinoamericana son pocas son las universidades que han creado sus SOC académicos de una forma eficiente y oportuna, promoviendo el uso de las buenas prácticas de seguridad y la formación adecuada de su personal.

JUSTIFICACION E IMPORTANCIA

Por los momentos que atravesamos actualmente se realiza la prestación de servicios de forma telemática para la mayoría de procesos, que permiten el funcionamiento adecuado de la universidad.

El crecimiento agigantado del internet y sus servicios han generado que la ESPE tenga un nivel de riesgo medio ante muchos incidentes informáticos debido a un mal manejo de varios recursos o por ataques externos.

De acuerdo a los procesos de la ESPE no existe un Centro Propio que emita las alertas de los incidentes de la seguridad de la información es decir no se tiene un área formalmente instalada para realizar este procedimiento

Resulta primordial la creación de un Centro de Operaciones de Seguridad SOC como respuesta a que se cumplan actividades de proactividad y reactivas que permitan estar preparados para evitar los posibles daños por incidentes informáticos que se puedan ocasionar y así poder contribuir a una mejora continua de la ciberseguridad de los sistemas de información de la ESPE.

DISEÑO ORGANIZACIONAL DEL CENTRO

A. Direccionamiento estratégico

Visión

Ofrecer los servicios de identificación y mitigación de ciberataques a la Universidad de las Fuerzas Armadas ESPE, colaborar en la formación del personal.

Misión

Instaurar al SOC-ESPE con el equipo de respuesta oportuna a los incidentes y vulnerabilidades informáticas en la Universidad de las Fuerzas Armadas ESPE

Objetivos

1. Ofrecer los servicios de respuesta oportuna a los incidentes informáticos mediante procesos certificados internacionalmente.
2. Acrecentar los recursos disponibles tanto materiales como humanos para brindar un servicio integro de calidad.
3. Acrecentar e innovar los servicios de respuesta informática de acuerdo al crecimiento de la comunidad universitaria.

Estructura organizacional

Responsabilidades generales del Centro.

Se establecen las siguientes responsabilidades generales:

- Supervisar, examinar y dar tratamiento a incidentes y vulnerabilidades.

- Emitir información, alertas y advertencias sobre la ciberseguridad.
- Ofrecer consultoría y asesoramiento en temas referidos a la ciberseguridad
- Encontrarse en constantes actualizaciones sobre nuevos procedimientos para dar respuestas oportunas y rápidas a los incidentes.
- Mantener el sigilo sobre los incidentes de ciberseguridad.

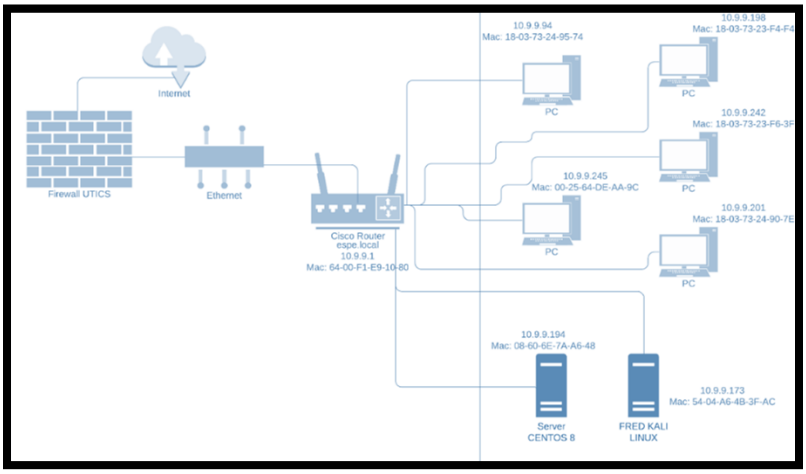
Configuración de activos de servicio

Se procederá a describir la información de la infraestructura TI que se va a necesitar para poner en marcha el SOC, donde se usó una CMDB para guardar la información de la configuración realizada en cada activo.

Para poder implementar y configurar los activos se realizó una revisión de la infraestructura que se requiere y que posee en UTICS, de las cuales se va proceder a utilizar cinco computadores y 2 servidores como podemos ver en la siguiente Figura.

Figura 20

Infraestructura SOC-ESPE



Para la implementación del SOC, se realizó una selección del hardware y software que sean óptimos para las necesidades iniciales del SOC. Dentro de la siguiente tabla se

va a exponer varios de los criterios que se utilizó para escoger las herramientas mas optimas que puedan brindar servicios con más aplicaciones.

Tabla 19

Selección del Software para implementación del SOC

Herramienta	Portabilidad	Documentación	Fiabilidad	Precio	Observaciones
Nessus	✓	✓	✓	$4190	Al ser la ESPE socios de CEDIA, el licenciamiento es gratuito.
Cisco Stealthwatch	✓	✓	✓	$13995	Falta de recursos y socios que provean el servicio
Alienvault (AT&T Cybersecurity)	✓	✓	✓	$8000	Provee la empresa privada con altos costos
Análisis de puertos Nmap	✓	✓	✓	Gratuito	
Snort 3.0		✓	✓	Gratuito	Falta de soporte en varios sistemas operativos como Kali Linux 2020
Fortinet		✓	✓	-	Se cuenta con equipos firewall e IDS propios de la Universidad.
Shodan	✓	✓	✓	$900	Servicio Web de monitoreo y búsqueda de vulnerabilidades en todo el mundo.
FreshDesk	✓	✓	✓	Gratuito	Software de Gestión de Tickets para ordenar pedidos y soluciones.
GLPI	✓	✓	✓	Gratuito	Software de acceso remoto, Y gestionado de tickets.

Nota. Herramientas para la implementación del SOC, con costos, tomado de la Tesis de Jonathan Benavides, 2020

Por todas sus características específicas y generales se ha decidido escoger el software para la puesta en marcha del SOC fue Nessus, FortiAnalyzer (FortiGate), FreshDesk, Shodan, GLPI.

Tabla 20

Software seleccionado para el SOC de la ESPE

Herramienta	Descripción	Versión	Observaciones
Nessus	Es el escáner de vulnerabilidades más utilizado en el mundo. Esta herramienta de alto nivel detecta amenazas en tiempo real y gracias a su precisión evita la ocurrencia de falsos positivos. Previene de manera eficiente los ataques a la red al identificar debilidades y errores de configuración que pueden usarse para permitir que las amenazas ingresen al sistema.	8.10.1	El software se encuentra trabajando en perfectas condiciones con la IP local 10.9.9.194

FortiAnalyzer	FortiAnalyzer ayuda a realizar una gestión centralizada de los registros de todos los productos de Fortinet. Tiene como objetivo interconectar diferentes tipos de soluciones, para tener una visión completa de la red y así automatizar la respuesta a incidentes. Se realiza una auditoría de seguridad continua de la red, donde se destacan las brechas en las áreas de seguridad y sus problemas típicos: • Identificar los dispositivos que necesitan ser parcheados. • Calcular un valor en función de las mejores prácticas, ayudando a los administradores de red a medir la postura de seguridad de su red.	-	Se escogió el FortiAnalyzer de Fortinet ya que la universidad cuenta con esos equipos.
Shodan	Se lo conoce como el motor de búsqueda de los hackers, con el objetivo de realizar tareas de investigación de nuevas vulnerabilidades. No obstante, esta herramienta puede usarse con fines maliciosos a razón de la cantidad de	-	Servicio web para monitoreo en tiempo real de amenazas https://www.shodan.io/

	información detallada que se proporciona con cada búsqueda realizada. Auditores, investigadores y toda persona que necesite información		
Freshdesk	Servicio de gestión de tickets, ya que administra los procesos críticos con simplicidad, precisión y rapidez.	**-**	Para la correcta gestión de incidentes es importante implementar una aplicación de gestión de tickets para tramitar cada incidente ordenadamente.
GLPI	Es una solución libre de gestión de servicios de tecnología de la información (ITSM), un sistema de seguimiento de incidencias y de solución service desk. Este software de código abierto está editado en PHP y distribuido bajo una licencia GPL.2 Como cualquier tecnología de código abierto, se puede ejecutar, modificar o desarrollar el código que es libre. GLPI es una aplicación web que ayuda las empresas con la gestión de su sistema de información. Entre sus características, esta solución es capaz de construir un inventario de todos los recursos de la organización y de gestionar tareas administrativas y financieras. Las	**9.3.3**	Servicio web para monitoreo en tiempo real de incidentes y seguimiento de los mismos. http://gestionenlinea.espe.edu.ec/

	funcionalidades de este software ayudan a los administradores IT a crear una de base de datos de activos técnicos, así como a gestionarla y proporciona un historial de las intervenciones de mantenimiento. La funcionalidad de asistencia (ticket) ofrece a los usuarios un servicio de declaración de incidencias o de solicitudes basadas en activos técnicos o no

Configuración de Nessus

Dentro de los requerimientos mínimos para su instalación son las siguientes:

- CPU: 4 2GHz cores.
- Memoria: 4 GB RAM (8 GB RAM recomendado).
- Espacio de Disco: 30 GB.

La configuración del Nessus se realizó en el servidor 10.9.9.194 ya que cuenta con las características suficientes para operar sin fallos. A continuación, se lista las características del equipo:

- DELL INTEL X89
- 12 GB RAM
- 1TB HDD
- Intel® Core™ i7-3930K CPU @ 3.20GHz × 12 cores

Para la realización de la configuración y operación del Nessus al proveedor (CEDIA) se realizó los siguientes pedidos para el licenciamiento:

- Solicitan una IP pública que permita el acceso desde la IP: 190.15.141.77 por el puerto 8834
- Abrir ICMP en el puerto 8834 y 8835 en tcp.

Las UTIC respondió el pedido realizando el NAT de la IP pública a la IP local 10.9.9.194 juntamente con los permisos a los puertos 8834 y 8835.

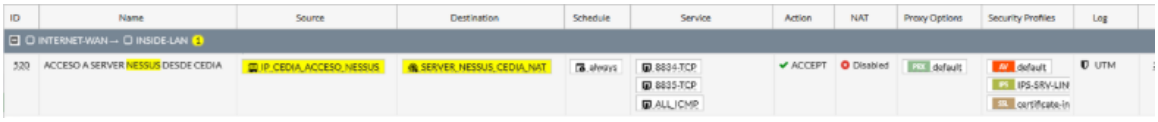
Figura 21

NAT de IP pública a IP local

Nota. En la Figura se observa la configuración de las UTICs para el servidor Nessus.

Figura 22.

Permisos de puertos a IP local



Nota. En la Figura se observa Configuración de las UTIC para el servidor Nessus.

Por los requerimientos resueltos por las UTICS se procedió al licenciamiento respectivo de la herramienta Nessus.

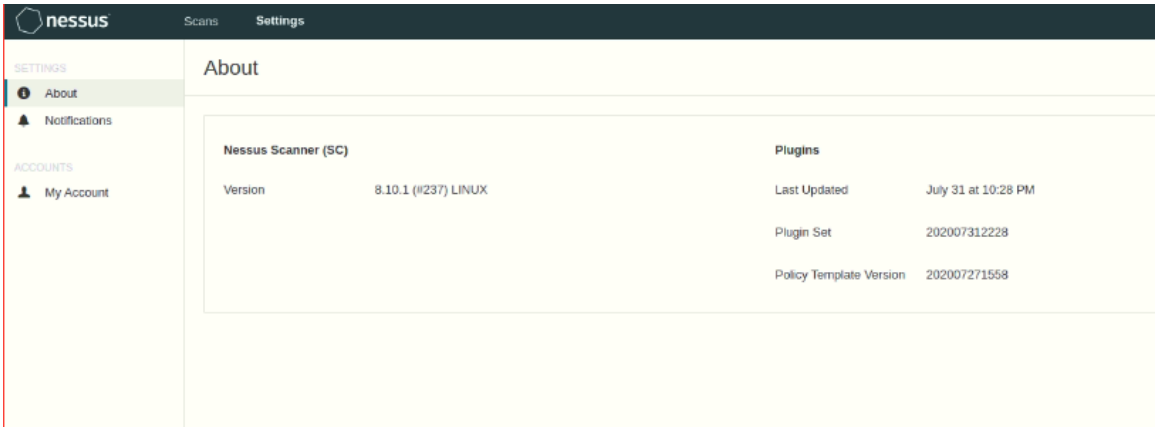
Figura 23

Dashboard de CEDIA (Licenciamiento de Nessus)

Nota. En la Figura se observa el dashboard de CEDIA indicando que el licenciamiento es un éxito.

Figura 24

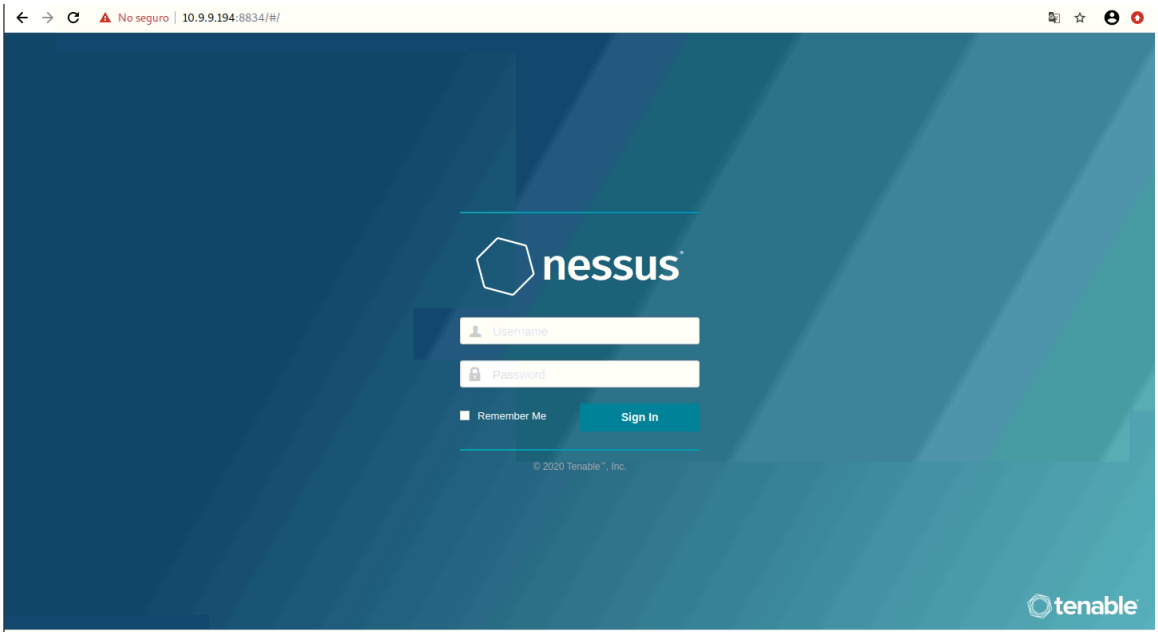
Licenciamiento de Nessus versión 8.10.1 SOC-ESPE



Nota. En la Figura se observa cómo indica que el licenciamiento de la herramienta fue un éxito.

Figura 25

Operación de Nessus versión 8.10.1



Nota. En la Figura se observa el funcionamiento de Nessus en el servidor 10.9.9.194.

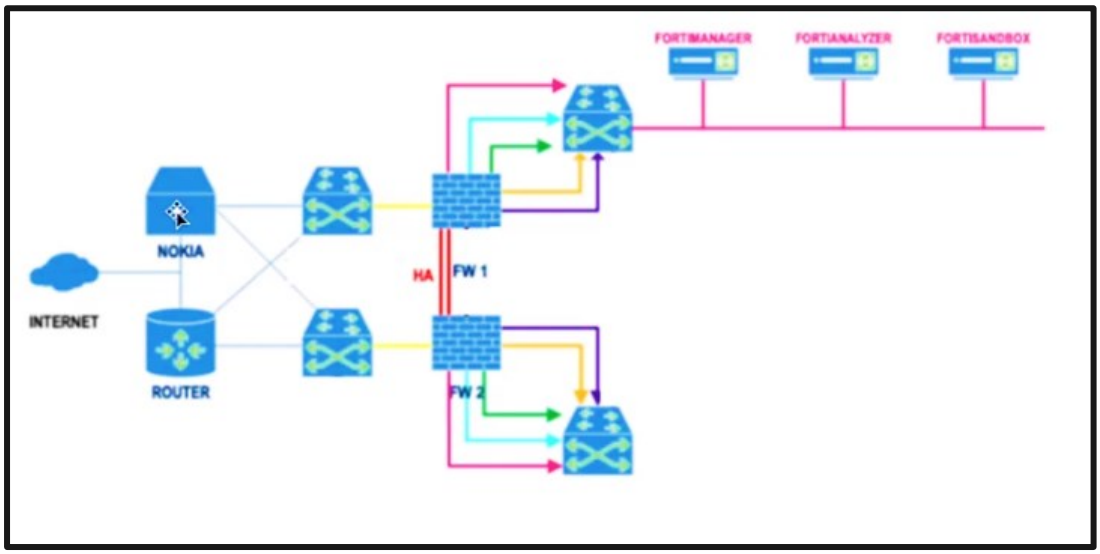
Configuración FortiAnalyzer

FortiAnalyzer es el producto de Fortinet el mismo que nos permite monitorear el tráfico de red de una institución en este caso la universidad mediante la unión de componentes como un firewall. FortiAnalyzer le permite al usuario poder llevar un control de tráfico, aplicaciones usadas, hosts comprometidos, análisis de eventos, IPS, análisis de amenazas y búsqueda de vulnerabilidades.

La Universidad de las Fuerzas Armadas ESPE cuenta con todos los equipos como observamos a continuación:

Figura 26

Diagrama de red y configuración de FortiAnalyzer

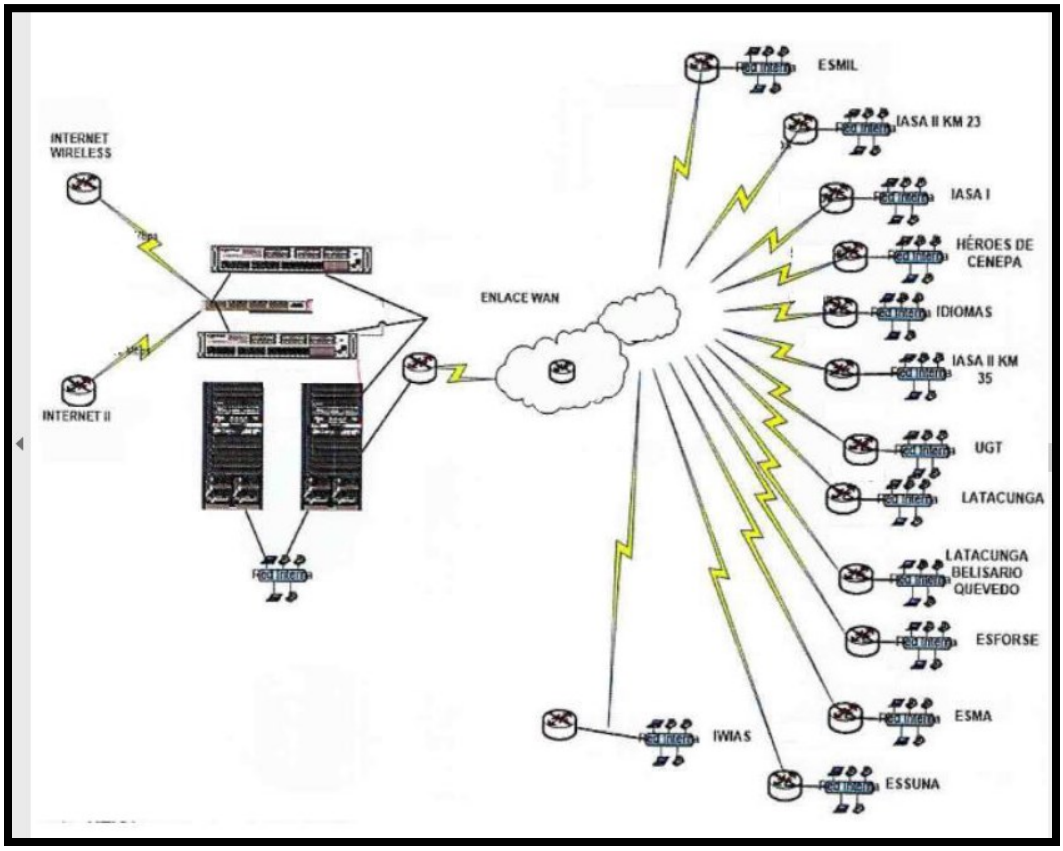


Nota. En la Figura se observa el lugar dentro de la infraestructura de red de la instalación del FortiAnalyzer.

En donde el proveedor es CEDIA con 1.8 GB de Internet y cuentan con dos ruteadores uno principal Nokia y otro de backup CISCO, estos ruteadores ingresan a dos switches de distribución y después al firewall FortiGate-3200D para proveer internet a todas las sedes de la institución.

Figura 27

Diagrama de red de la Universidad de las Fuerzas Armadas ESPE

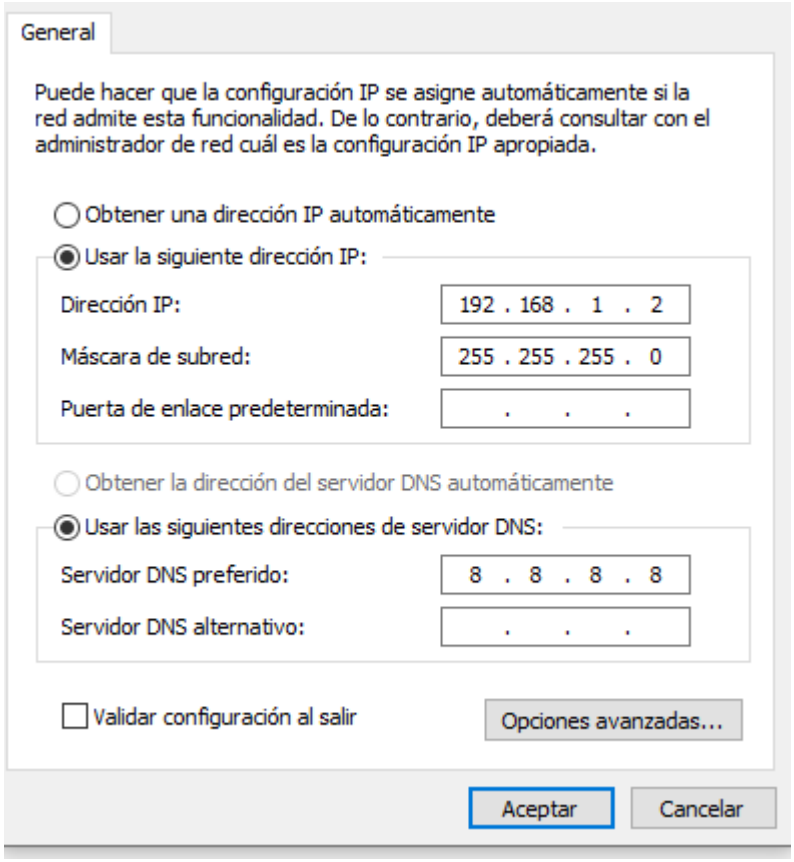


Nota. Tomado del *Plan Estratégico de Tecnologías de la Información y Comunicaciones* por UTIC ESPE, 2015.

Para la configuración manual se debe ingresar mediante el cable de comunicaciones al puerto 1 del dispositivo con los siguientes cambios en la red interna.

Figura 28.

Configuración manual FortiAnalyzer

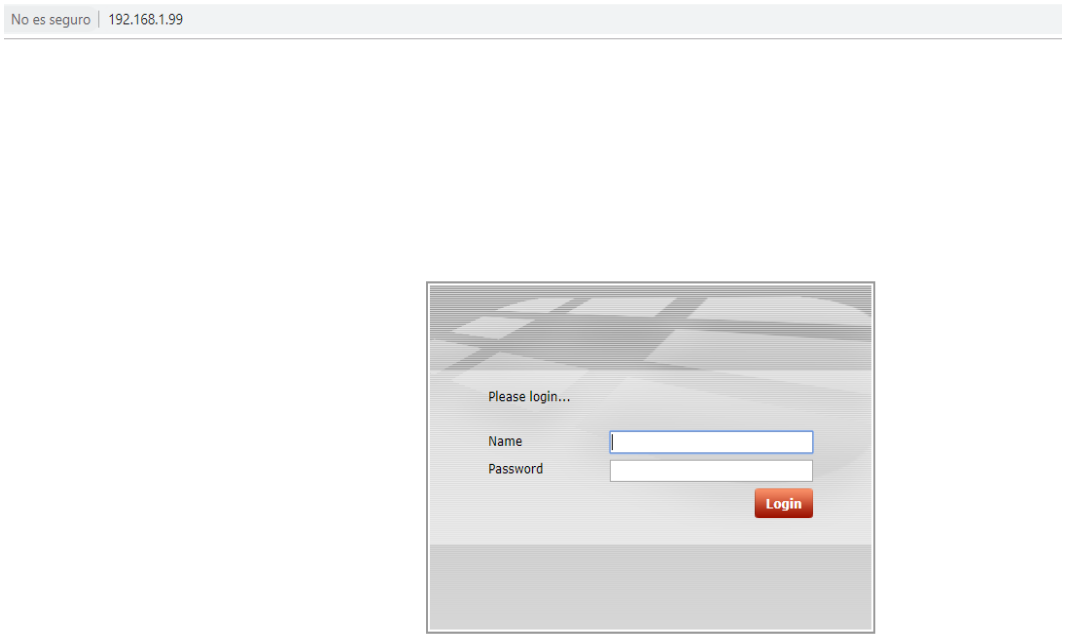


Nota. En la Figura se observa la configuración manual de FortiAnalyzer.

Luego se ingresa el usuario y contraseña mediante el navegador web con la dirección https//192.168.1.99

Figura 29.

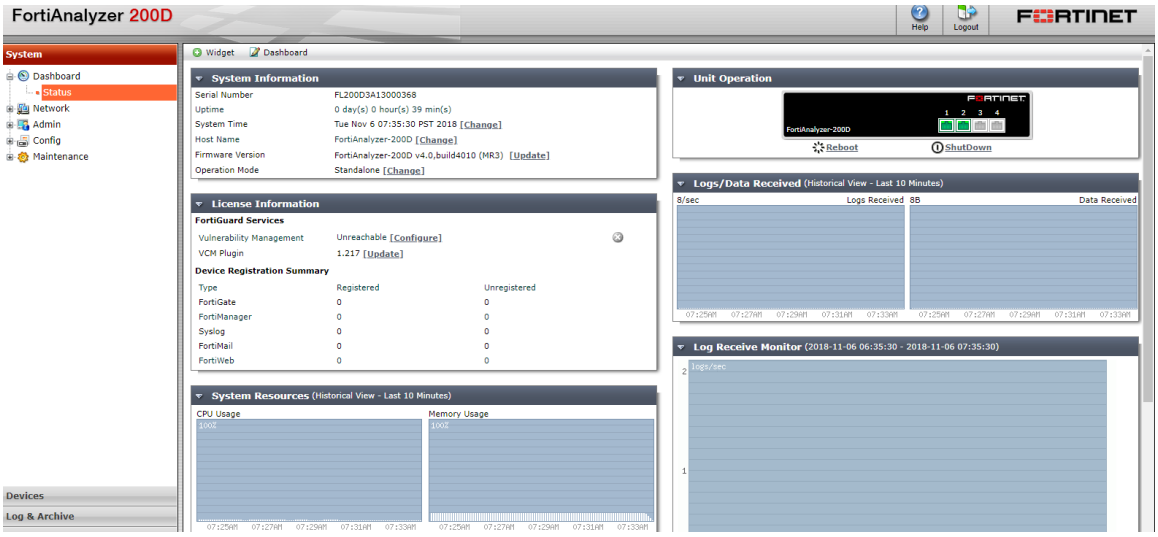
Ingreso a FortiAnalyzer de forma manual.



Nota. En la Figura se observa el ingreso a FortiAnalyzer de manera virtual.

Figura 30.

Dashboard de configuración de FortiAnalyzer

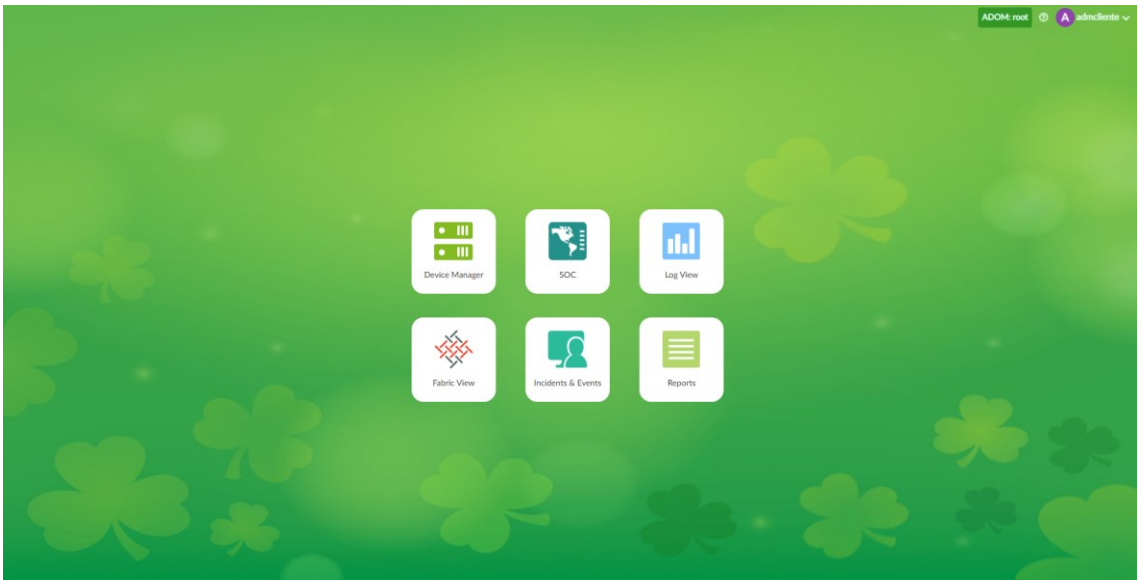


Nota. En la Figura se observa el *Dashboard de configuración de FortiAnalyzer.*

En el caso particular de la Universidad de las Fuerzas Armadas, el servicio de Fortinet es tercerizado, por lo cual se realizó la gestión para que el administrador permita el ingreso a la visualización del dispositivo y monitorear posibles eventos.

Figura 31.

FortiAnalyzer centralizado ESPE

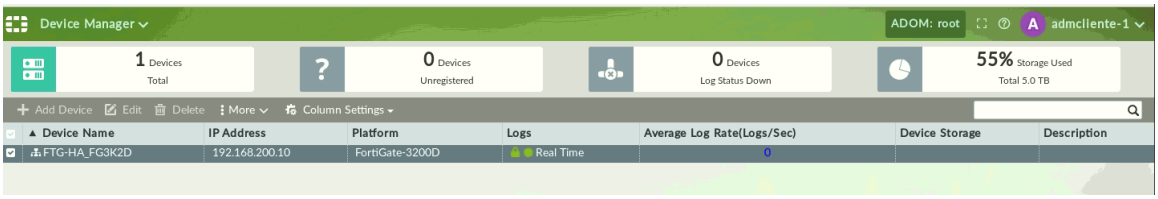


Nota. En la Figura se observa el *FortiAnalyzer centralizado ESPE.*

Los dispositivos fueron configurados para que el tráfico de red del Firewall Fortigate-3200D sea analizado por el dispositivo FortiAnalyzer 2000E.

Figura 32

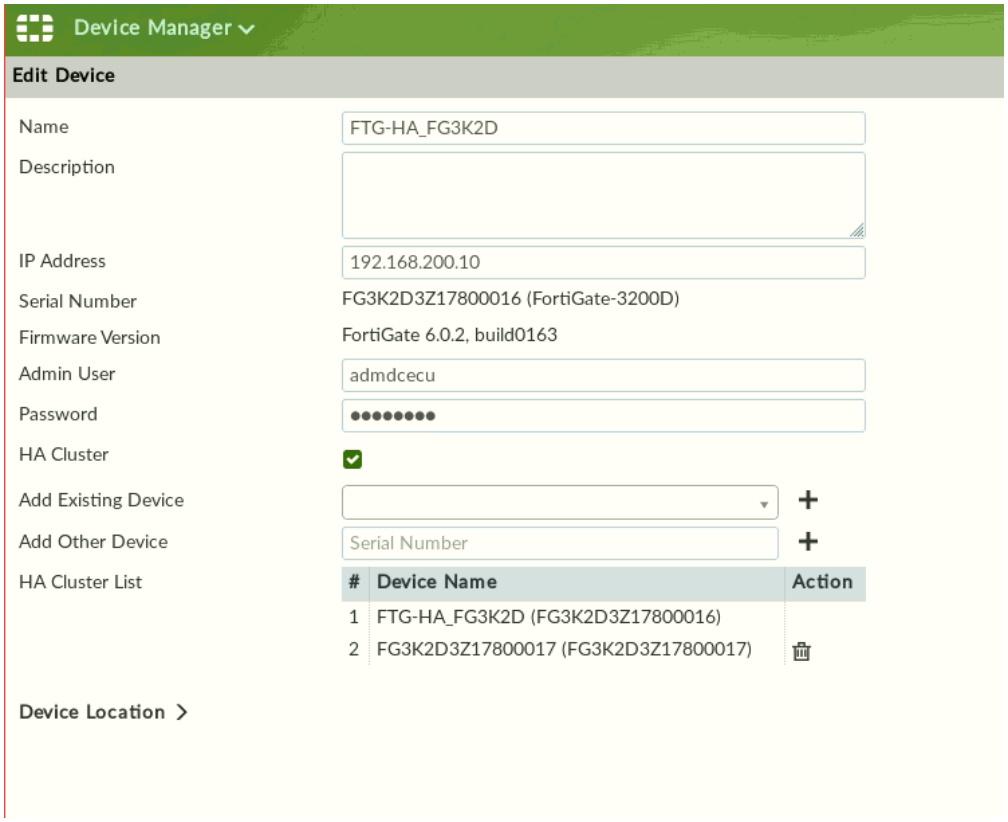
Configuración de dispositivos en FortiAnalyzer



Nota. En la Figura se observa los dispositivos agregados para analizar tráfico por el FortiAnalyzer.

Figura 33

Ingreso de firewall a FortiAnalyzer



Nota. En la Figura se observa los datos del dispositivo agregado para que el FortiAnalyzer analice el tráfico.

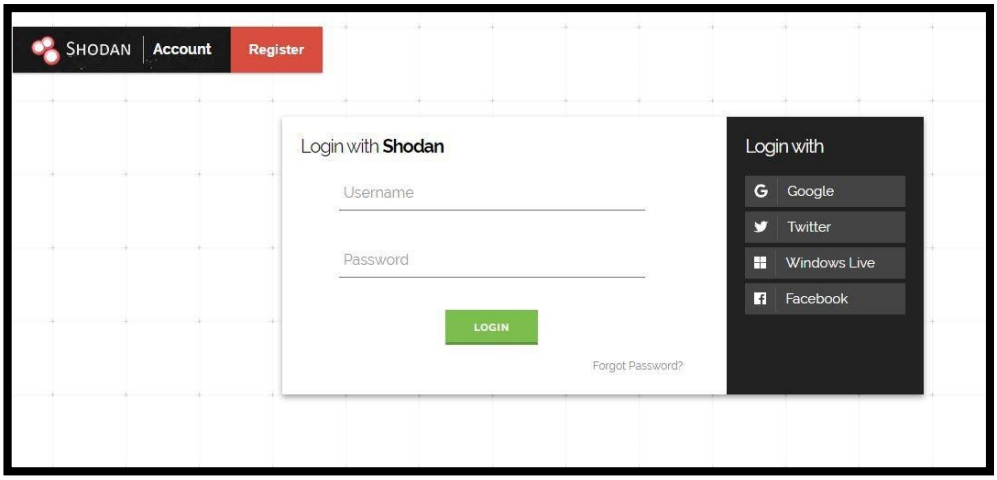
Configuración Shodan

Shodan es un motor de búsqueda de dispositivos (Shodan, 2020) que se encuentran conectados a internet y también sirve para recabar toda la información de: servicios, puertos, vulnerabilidades y amenazas de los dispositivos conectados alrededor del mundo. El acceso se hace mediante su página web shodan.io, no es necesario descargarse y dispone de varios servicios como lo son: motor de búsqueda, monitoreo en tiempo real, APIs para servicios, reportes, búsqueda de exploits y mapas.

Uno de los servicios a entregar para el SOC es el de alertas de incidentes, lo cual se necesitó los servicios de Shodan Monitor. La configuración se realizó de la siguiente manera.

Figura 34

Registro Shodan.

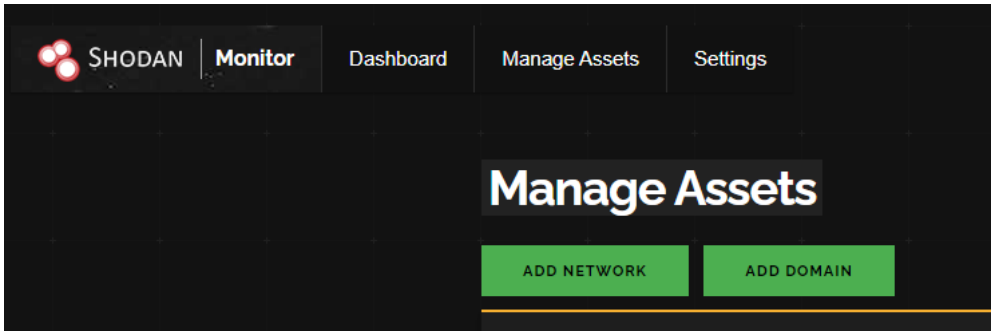


Nota. *Tomado de la web* Shodan.io *por Shodan, 2021.*

Para realizar el monitoreo en tiempo real Shodan cuenta con dos formas de ingreso, una es colocar el rango de red que queremos monitorear, en el caso de la ESPE las IP públicas son 192.188.58.0/24 y la otra es por el dominio, en este caso sería “espe.edu.ec”.

Figura 35

Formas de registro de IP para monitoreo

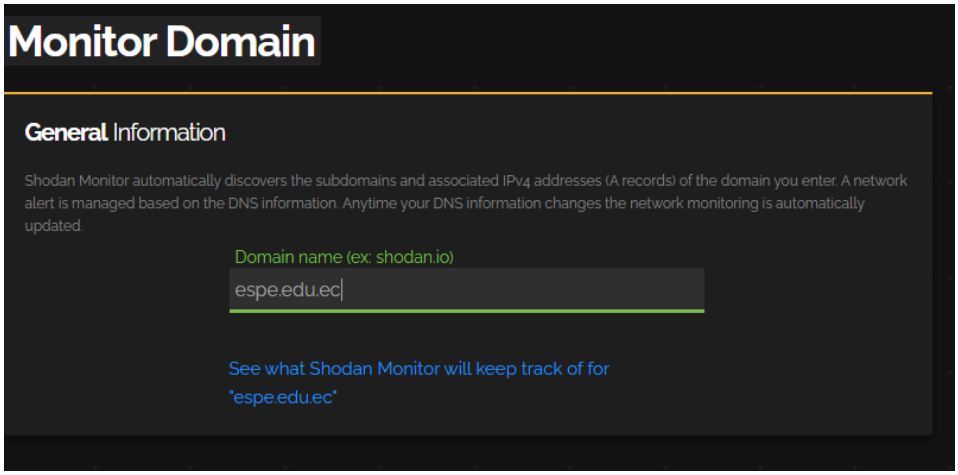


Nota. Tomado de la web *Shodan.io* por Shodan, 2021.

Para el caso de la ESPE escogimos el monitoreo según el dominio, y la configuración queda de la siguiente manera:

Figura 36.

Registro del dominio ESPE en Shodan Monitor

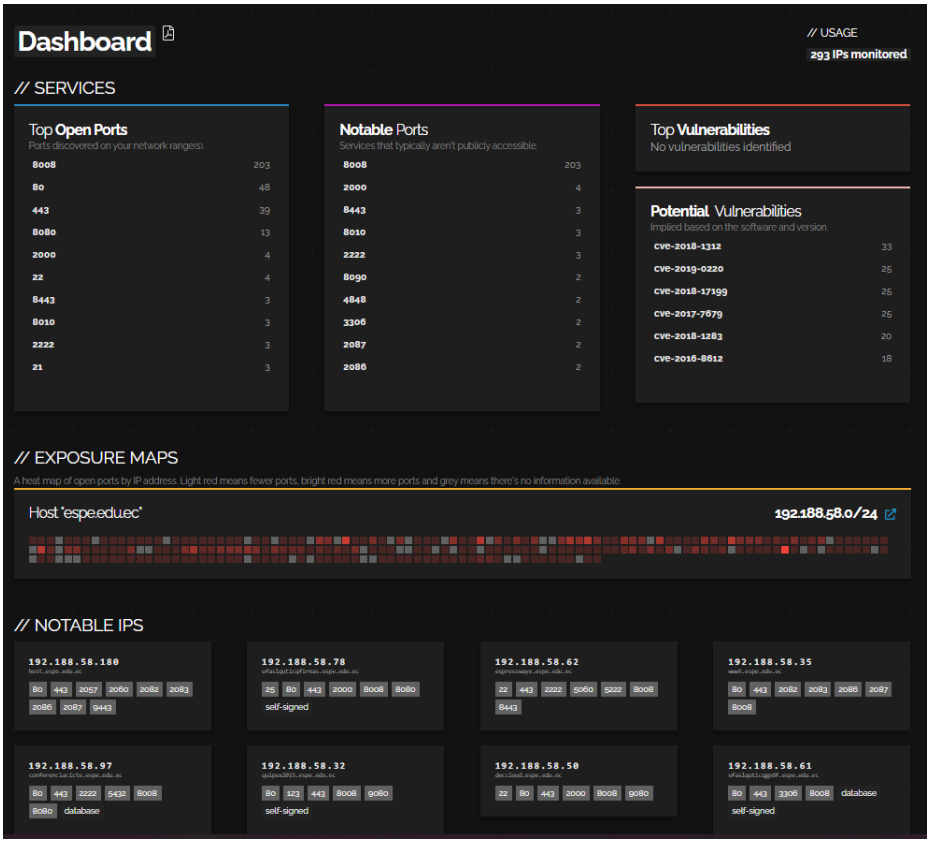


Nota. Tomado de la web *Shodan.io* por Shodan, 2021.

Dentro del el Dashboard de monitoreo se resalta las IP más importantes, los puertos abiertos más comunes, y la mayoría de las vulnerabilidades de estos dispositivos.

Figura 37

Dashboard de monitoreo Shodan

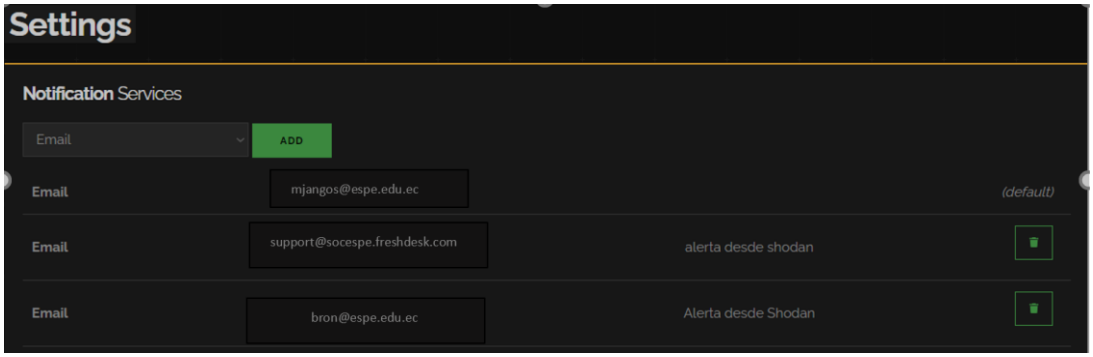


Nota. Tomado de la web *Shodan.io* por Shodan, 2021.

Para el manejo de incidentes y alertas se enlazó el Shodan con el correo de soporte del SOC para gestionar de mejor manera centralizada y ordenada los incidentes.

Figura 38

Configuración al correo electrónico.



Nota. Tomado de la web *Shodan.io* por Shodan, 2021.

Configuración Freshdesk

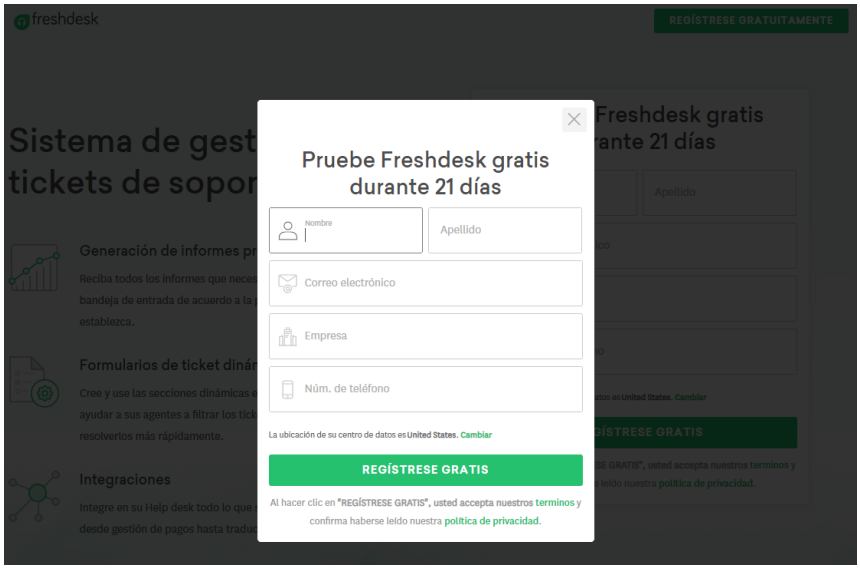
Este es un servicio web donde se gestionan tickets, el mismo sirve para la generación tickets o turnos dinámicos que van a ayuda al equipo de trabajo designado a solucionar los problemas de los clientes de una mejor forma siendo más óptimos y ordenados. Los turnos o tickets que se van a entregan se van a categorizar de acuerdo a su importancia con el personal a cargo y finalmente se generarán reportes que servirán de documentación para analizar la operación de servicio y un crecimiento futuro.

Este servicio de tickets o turnos va a ayudar al SOC en la gestión de incidentes ya que le permite asignar al personal a cargo del desarrollo de dichos incidentes y priorizar los eventos. Cada incidente es tratado desde que inicia hasta que se soluciona o se queda pendiente por diferentes motivos y finalmente es registrado en el dashboard permitiendo hacer un seguimiento en el caso de requerir informes sobre algún evento.

A continuación, se describe la configuración de Freskdesk adaptado a las necesidades requeridas por el SOC.

Figura 39

Registro Freshdesk

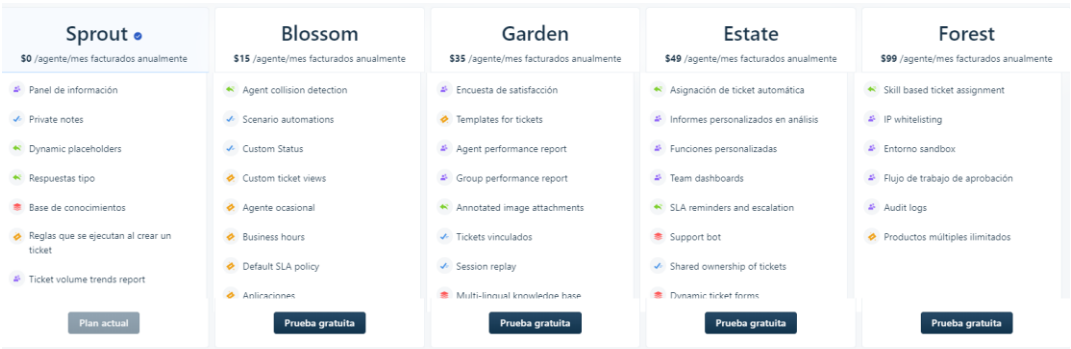


Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2021

Freshdesk dispone de varios planes según la necesidad de forma personal o empresarial; para este proyecto y la puesta en marcha inicial del SOC bastó con el plan gratuito, ya que ofrece la gestión de tickets de forma dinámica junto con alertas a los correos para una mejor gestión.

Figura 40

Planes del servicio Freshdesk

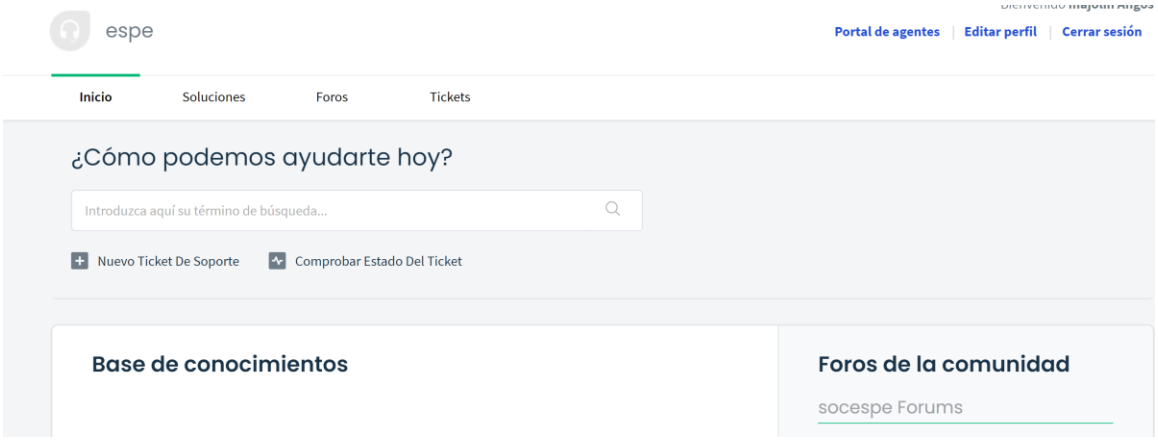


Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2021

Para el control de incidentes y servicio al cliente, Freshdesk entrega a los usuarios la posibilidad de configurar un sitio oficial de soporte, correo electrónico de soporte y nombre de la compañía. Para el caso del SOC se configuro el correo support@socespe.freshdesk.com con el nombre de SOC y página de soporte https://socespe.freshdesk.com/support/home que servirán para la gestión de incidentes.

Figura 41

Portal servicio al cliente SOC



Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2021

Figura 42

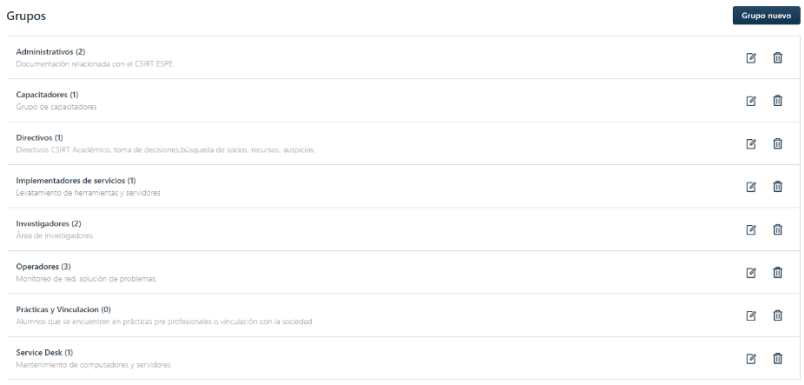
Configuración del correo de soporte SOC

Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2021

Se cuenta con una configuración de grupos de trabajo que sirve para categorizar a cada persona según las funciones que cumple cada uno de ellos, esto sirve para gestionar de mejor manera los eventos de a cuerdos a los roles designados.

Figura 43

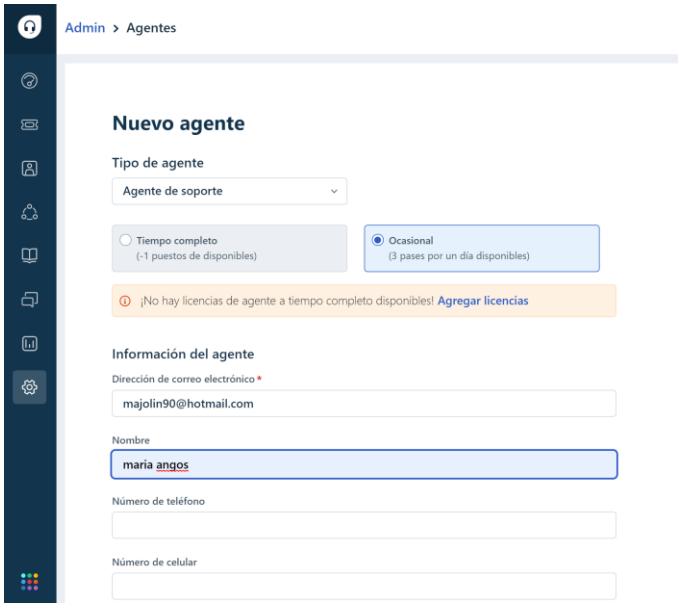
Grupos de trabajo SOC



Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2021

Figura 44

Registro de agentes SOC

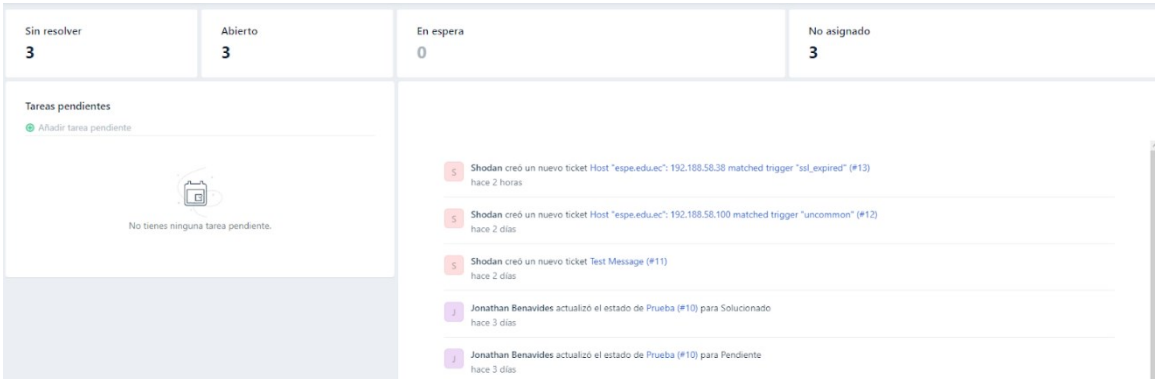


Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2021

Ya configurado el Freshdesk, el dashboard de soporte indica los eventos sin resolver, los abiertos, en espera y no asignados, permitiendo hacer un seguimiento a cada incidente y poder atender todos los requerimientos del cliente.

Figura 45

Dashboard principal de la gestión de tickets



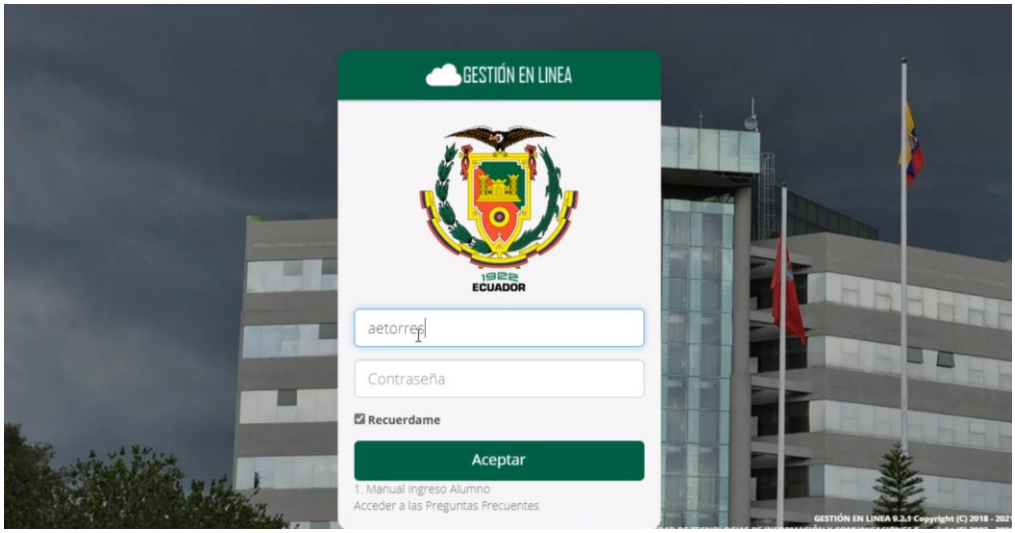
Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2021

GLPI

Es un software libre que está adaptado para utilizarse en la universidad y por el cual se tramita los tickets.

Figura 46

Ingreso a la plataforma

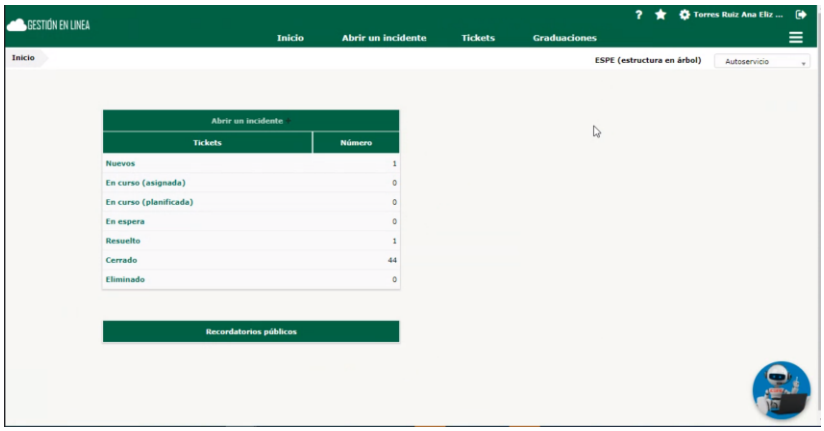


Nota. Tomado de *la web gestionenlinea* por ESPE, 2021

Podemos observar los diferentes incidentes que ocurren dentro de la plataforma.

Figura 47

Incidentes

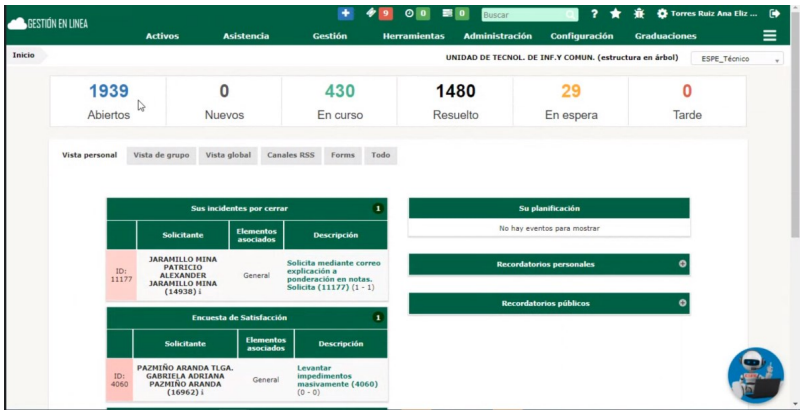


Nota. Tomado de *la web gestionenlinea* por ESPE, 2021

Plataforma donde podemos observar los estados de todos los tickets generados, podemos ver los abiertos, que son los que han ingresado recién, los que se encuentran en curso son los que se están solucionando, los resulto son los que ya terminaron con una solución y los de espera son los que se escalan a un nivel 2 o 3 dependiendo del incidente.

Figura 48

Estados de los tickets

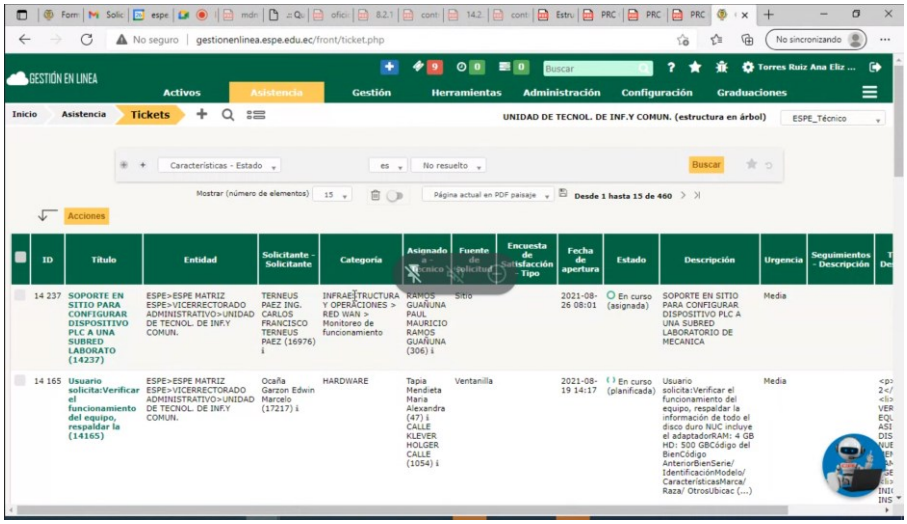


Nota. Tomado de *la web gestionenlinea* por ESPE, 2021.

A continuación, ingresamos a todos los tickets que tenemos en la bandeja de cada agente que se encargar de la solución de los mismos

Figura 49.

Bandeja de entrada de cada agente



Nota. Tomado de *la web gestionenlinea* por ESPE, 2021.

Validación y pruebas del servicio

Se puede asegurar que la configuración de esta infraestructura de TI cumpla con los requisitos y servicios ofrecidos en el Diseño del Servicio, intentando validar a cada activo para cumpla su función y logre satisfacer las metas y objetivos planteados por el equipo de SOC.

Para continuar con la validación y pruebas es importante comprender que los servicios iniciales que prestará el SOC- ESPE los cuales se representan en la siguiente tabla:

Tabla 21

Servicios iniciales SOC-ESPE

Servicio	Funciones
Alertas y advertencias	Se reportará todo incidente, vulnerabilidad, malware o intrusión informática, permitiendo que el administrador pueda conocer todos los detalles de cada incidente
Tratamiento de incidentes	Se recomendará al administrar buscar soluciones ante problemas que han escalado a un ente superior por la complejidad de los mismos.
	No cerrar un caso y su seguimiento hasta que se encuentre resuelto.
Análisis de incidentes	Realizar un correcto análisis del incidente de acuerdo al tiempo de solución del mismo, entregando un informe con posibles soluciones.
Apoyo en la respuesta de incidentes	Siempre se debe seguir el procedimiento adecuado para solventar el incidente con la infraestructura adecuada.
Coordinación de la respuesta a incidentes	Une esfuerzos para dar respuesta a un incidente, en el caso de no encontrar solución se puede consultar a otros SOC para pedir soporte.

En la tabla que tenemos a continuación se puede observar la validación de los activos según los servicios del SOC; de la forma que para cada servicio se valida con la herramienta que se va a utilizar comprobando que sus componentes sirvan para dar solución al proceso.

Tabla 22

Validación de herramientas

Servicio	Herramientas						Funciones de las herramientas
	Nessus	Nmap	FortiAnalizer	Shodan	GLPI	Freshdesk	
Alertas y advertencias	✓	✓	✓	✓	✓		Monitorear incidentes de seguridad
Tratamiento de incidentes					✓	✓	Gracias a software de tickets se puede gestionar el incidente hasta se resuelto
Análisis de incidentes	✓			✓			Dichos softwares entregan un análisis automático del incidente
Apoyo en la respuesta de incidentes	✓			✓	✓	✓	Monitoreo Análisis Ayuda remota
Coordinación de la respuesta a incidentes					✓	✓	Seguimiento del incidente Ayuda remota exterior.

En conclusión, las herramientas cumplen en dar solución al ciclo de vida del servicio entregando funcionalidades que sirvan para cumplir los objetivos de cada uno de ellos ya que son herramientas completas y su uso es intuitivo, y sobre todo, pueden ser usadas remotamente tomando en cuenta la pandemia actual del Covid-19 aun la universidad continua trabajando semi presencialmente. También se evaluó el lugar físico para que este en óptimas condiciones para la siguiente fase de operación del servicio.

Gestión de conocimiento

Dentro de la gestión del conocimiento se describe la información del personal juntamente con los equipos designados y contacto con proveedores guardados en una

SKMS (Sistema de Gestión del Conocimiento del Servicio) que servirán para compartir la información con otras áreas y facilitar el proceso de toma de decisiones. Hay que tomar en cuenta que las computadoras designadas al equipo de trabajo están configuradas para aceptar sesiones remotas, ya que en el presente la Universidad se encuentra en trabajando con teletrabajo entonces van solo 2 días a la semana.

Implementación del servicio

Metodología de implementación

La metodología de implementación para el presente proyecto de titulación se da con la ayuda del marco referencial de ITIL 4, descrita en capítulos anteriores, tiene una estructura lógica que nos permite levantar procesos y servicios de manera ordenada y optima la misma que tiene las siguientes características:

- Flexibilidad
- Información
- Niveles de servicio
- Adaptabilidad
- Manejo correcto de Incidentes.

Gestión de eventos

Para poder definir un evento dentro de la seguridad informática es cualquier hecho u ocurrencia relacionada con algún dispositivo que puede o no comprometer sus niveles de riesgo de la institución. Para el SOC, los eventos deben ser categorizados según su importancia ya que no todos los eventos se pueden poner dentro de los formularios porque existen muchos eventos que producen los incidentes y en este caso solo se toma los incidentes que más se repiten en la Universidad. Para gestionar un evento del SOC

se ha optado por herramientas que entregan dichas ocurrencias los cuales deben ser analizados por el personal y determinar qué proceso se llevara a cabo según su importancia.

Eventos de Nessus

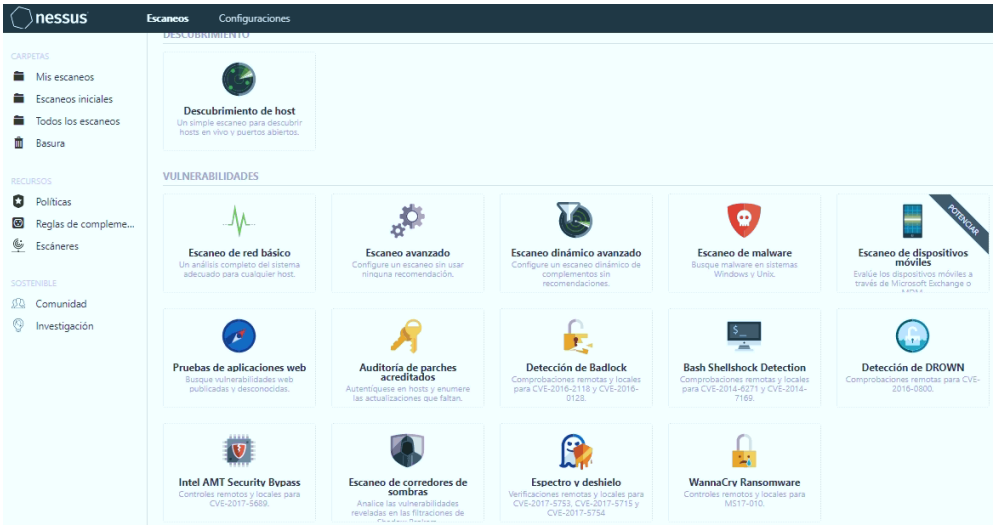
Esta herramienta nos entrega información al momento de realizar un escaneo a la red, no lo hace automáticamente y el usuario debe escoger que tipo de escaneo se realiza como los siguientes:

- Descubrimiento de host: Se realiza escaneo simple de todo el sistema para descubrir hosts en vivo y puertos abiertos.
- Escaneo de red básico: Se realiza un análisis completo de todo el sistema con cualquier host.
- Escaneo avanzado: Se realiza una configuración avanzada de escaneo sin recomendaciones ni guías.
- Escaneo dinámico avanzado: Se realiza un escaneo dinámico de todos los complementos.
- Escaneo de malware: Realiza la búsqueda de los malware en sistemas operativos Windows y Unix.
- Escaneo de dispositivos móviles: Se realiza una evaluación a través de Microsoft Exchange o MDM.
- Pruebas de aplicaciones web: Se encarga de buscar la mayoría de vulnerabilidades web publicadas y desconocidas.
- Auditoría de parches acreditados: Realiza la búsqueda de todas las actualizaciones de los sistemas que se utilizan.
- Bash Shellshock Detection: Se realizan todas las comprobaciones remotas y locales para los siguientes equipos CVE-2014-6271 y CVE-2014-7169.

- Detección de DROWN: Se realizan las comprobaciones remotas para CVE-2016-0800.
- Intel AMT Security Bypass Controles remotos y locales para CVE-2017-5689.
- Escaneo de corredores de sombras: Analice las vulnerabilidades reveladas en las filtraciones de Shadow Brokers.
- WannaCry Ransomware: Se realizan los controles remotos y locales para MS17-010.
- Auditoría de la infraestructura de la nube: Se puede auditar la configuración de servicios en la nube para terceros.
- Escaneo interno de red PCI: Se realiza un análisis de las vulnerabilidades internas del PCI DSS (11.2.1).
- Auditoría de configuración de MDM: Se realiza la auditoria de la configuración de los administradores para los dispositivos móviles.
- Auditoría de configuración sin conexión: Se realiza la auditoria de la configuración de dispositivos de red.

Figura 50

Tipos de escaneo en Nessus

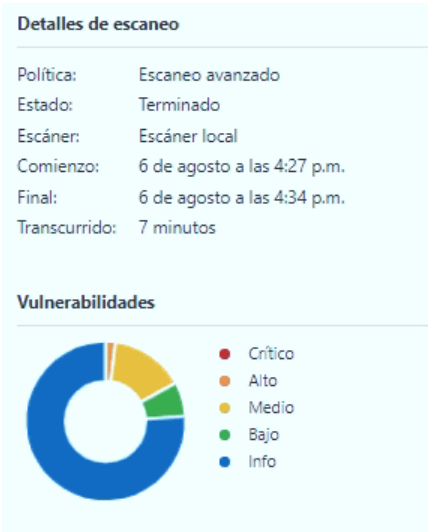


Nota. Dashboard para un escaneo en Nessus.

Cuando se realizan cualquier tipo de escaneo, Nessus presenta los eventos divididos en crítico, alto, medio, bajo e informativo juntamente con los detalles del escaneo:

Figura 51

Resultados de escaneo Nessus

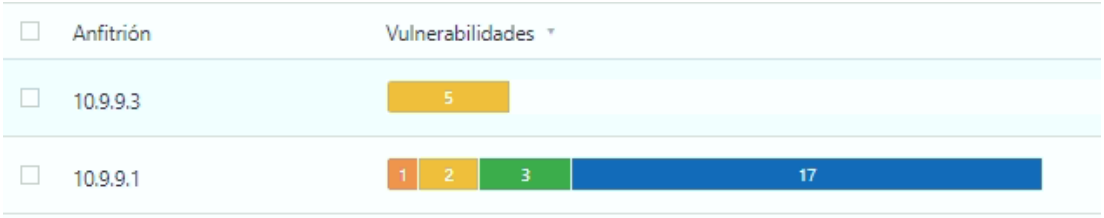


Nota. *Detalles de escaneo en Nessus.*

Esta herramienta divide los escaneos según los hosts encontrados, categorizando los resultados en crítico, alto, medio, bajo e informativo, una vez analizado indica información detallada para que el agente u operador pueda proceder a analizar y determinar si se trata de un incidente o un evento sin riesgo para la institución.

Figura 52

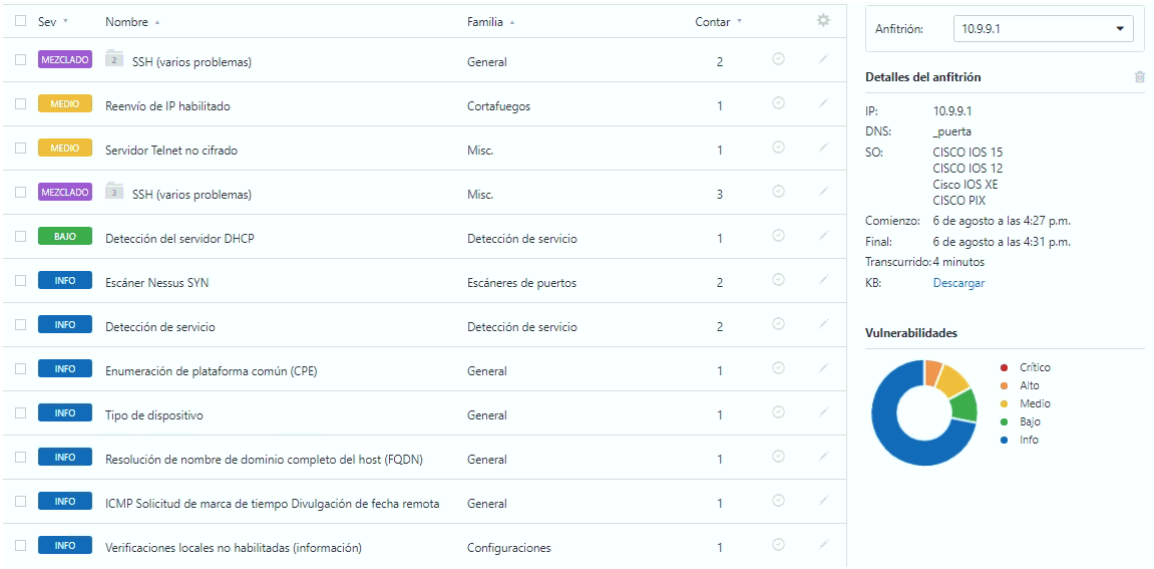
Resultados de escaneo según el host



Nota. Resultados del escaneo divido por host encontrados.

Figura 53

Detalles del escaneo por host



Nota. Detalles de vulnerabilidades encontradas en un host.

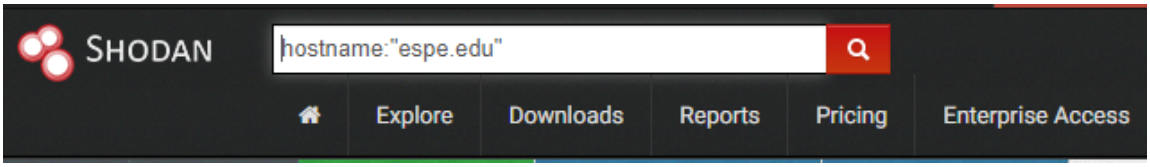
Eventos de Shodan

Como se mencionó anteriormente es un buscador de dispositivos que se encuentra con conexiones a internet en todo el mundo, se pueden encontrar varios equipos como: servidores, cámaras, computadoras, dispositivos médicos, IoT, y en conclusión todo aparato que pueda conectarse al internet. Los diferentes tipos de eventos que se manejan en esta herramienta son pasivos y activos; pasivos son los que le permiten al buscador revisar los servicios y vulnerabilidades de los varios dispositivos, y activos son los que le permiten monitorear en tiempo real todas las vulnerabilidades conocidas y desconocidas de los equipos que el usuario se encuentre ocupando.

Para el SOC se utilizan estos eventos donde se busca determinar la mayoría de riesgos para la Universidad y así poder ofrecer una solución oportuna ante algún fallo de seguridad. Para tales casos se realizan la búsqueda con filtros y cadenas de caracteres para encontrar los objetos:

Figura 54

Ejemplo de búsqueda en Shodan

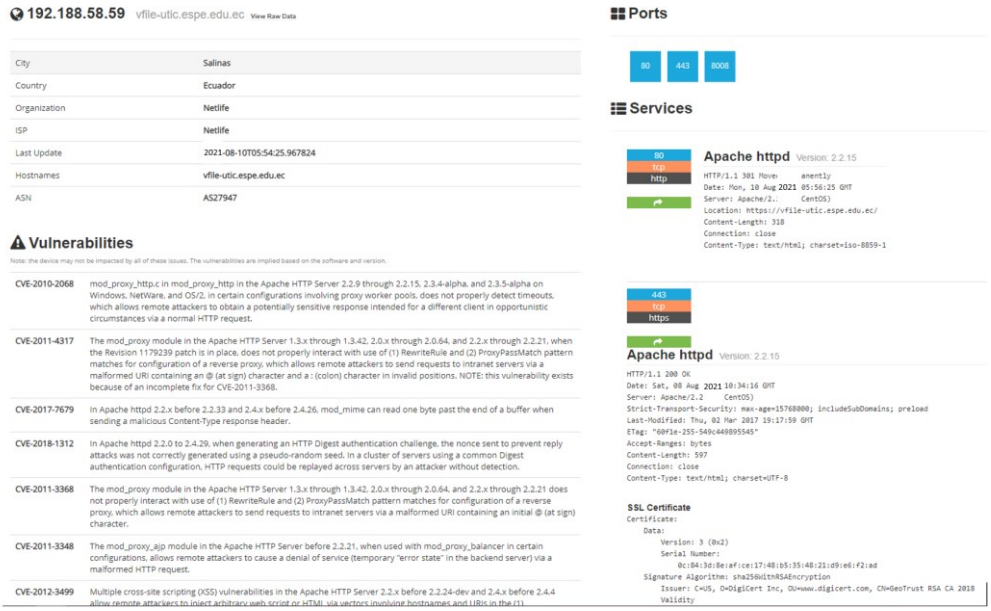


Nota. Tomado de *shodan.io* por Shodan, 2021.

El personal del SOC realiza todas las búsquedas en base a lo requerido y esta herramienta presenta la siguiente información como: el nombre de dominio, ubicación, puertos usados, servicios y vulnerabilidades que sirven para el uso del personal y determinar si se trata de algún incidente de seguridad.

Figura 55

Detalle de búsqueda en Shodan

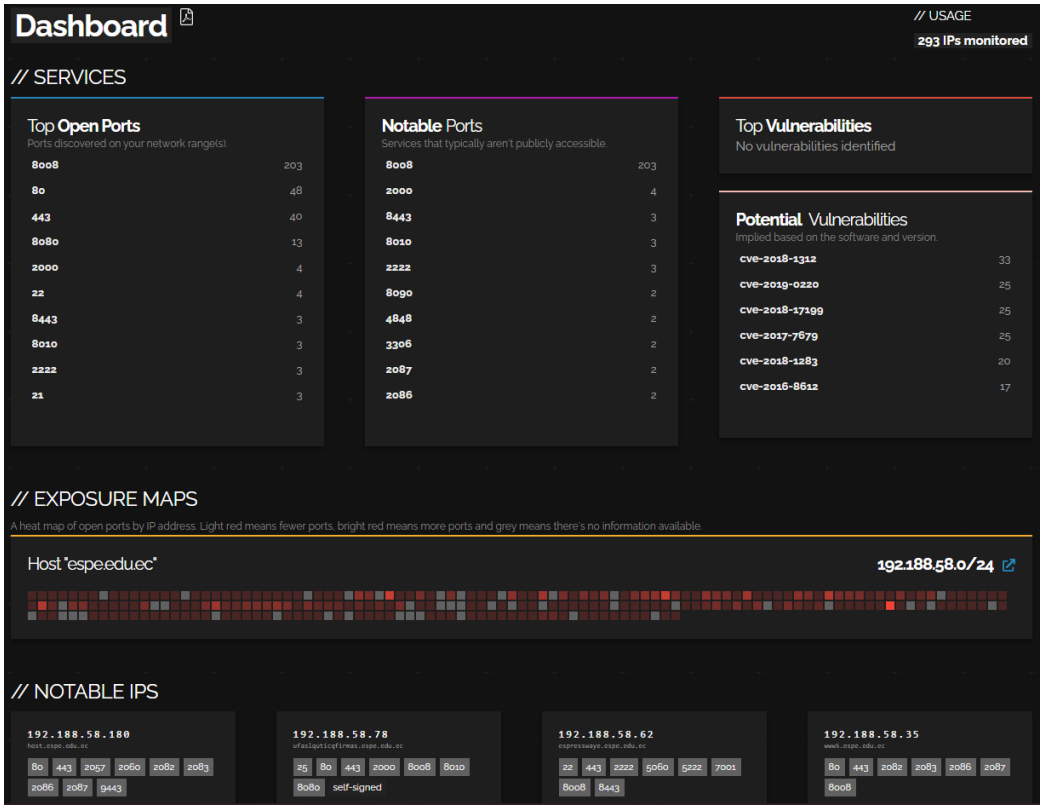


Nota. Tomado de *shodan.io* por Shodan, 2021.

Dentro de herramienta también nos permite realizar el monitoreo de las amenazas de seguridad en tiempo real, en donde la información que presenta Shodan es determinada por el número de IPs que determine el usuario en la configuración, con el hostname “espe.edu.ec”.

Figura 56

Dashboard de monitoreo en tiempo real del host “espe.edu.ec”

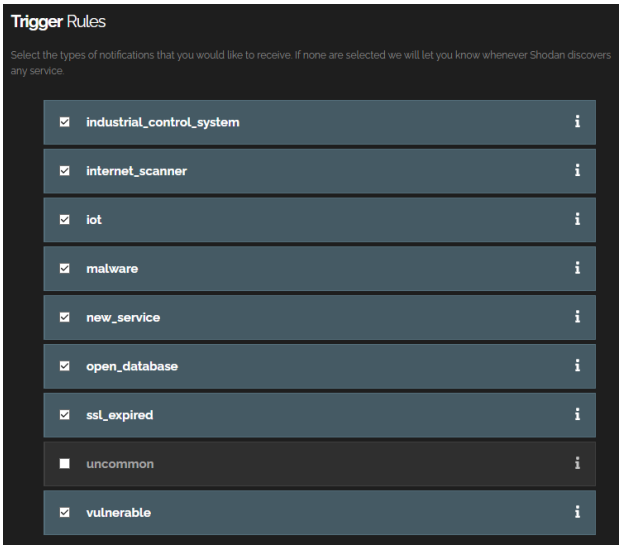


Nota. Dashboard de monitoreo en tiempo real del hostname “espe.edu.ec”. Tomado de shodan.io por Shodan, 2021.

En esta herramienta posee varios tipos de eventos de los cuales están configurados en las reglas de activación que sirven como filtros para verificar que alertas se van a usar.

Figura 57

Reglas de activación de alertas Shodan

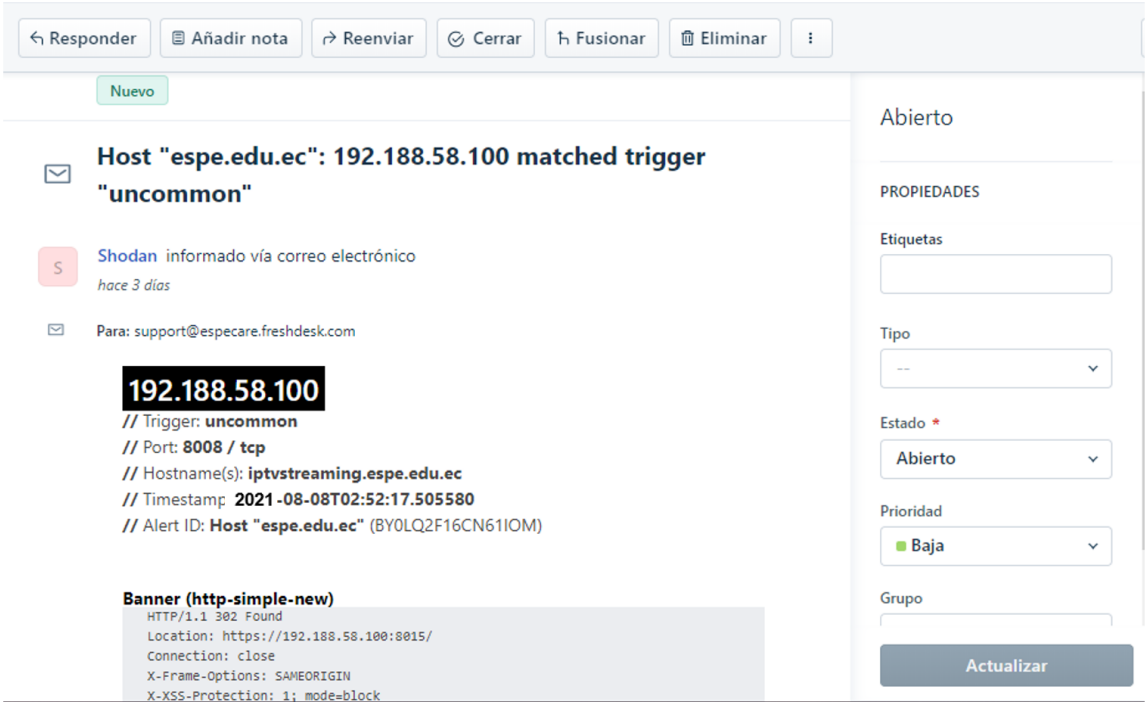


Nota. La figura representa los tipos de eventos seleccionado para dar alertas. Tomado de shodan.io por Shodan, 2021.

Estas alertas son enviadas por correo electrónico para que el operador o agente pueda realizar un análisis y así determinar si se trata de un incidente o no. La alerta está configurada para que llegue al correo electrónico de soporte y se genere un ticket automáticamente.

Figura 58

Recepción de alertas Shodan en el correo electrónico



Nota. La figura representa la recepción de la alerta en el portal de tickets del SOC-ESPE.

Eventos FortiAnalyzer

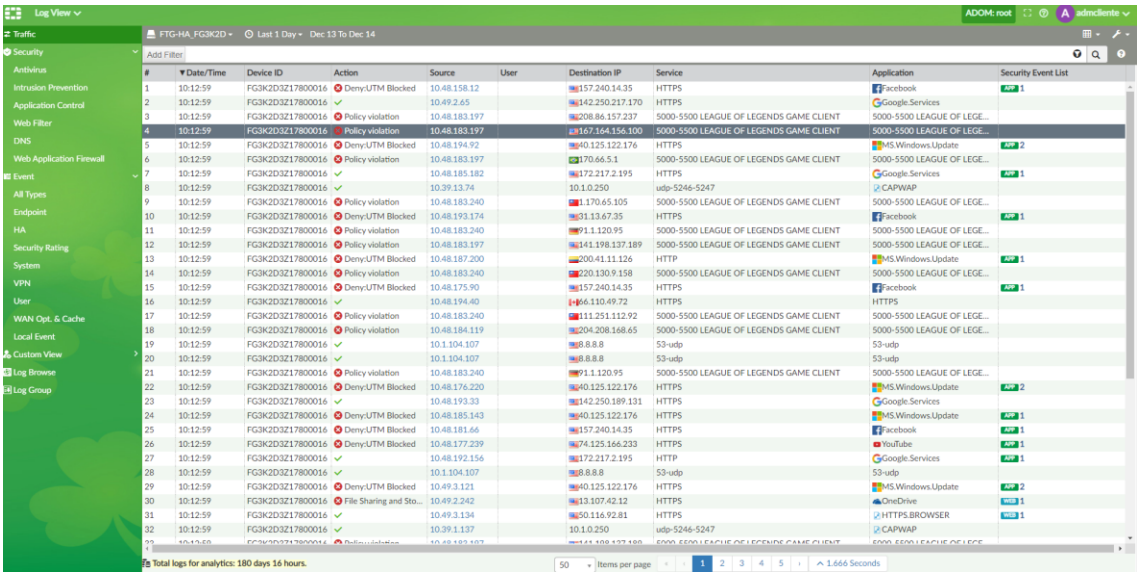
Dentro de esta herramienta podemos realizar la visualización de eventos en tiempo real que provee el FortiAnalyzer con el que trabaja la ESPE es completo ya que divide el tráfico de la red: en amenazas, destino, origen, países, vulnerabilidades, hosts comprometidos, eventos, aplicaciones y reglas aplicadas por el firewall.

Debemos tomar en cuenta que este servicio es ofrecido por Telconet Cedía los mismos que tienen un control compartido con las UTICS para poder solventar acontecimientos que se deben solucionar en el mismo momento.

La forma de ver los eventos en el FortiAnalyzer son las siguientes:

Figura 59

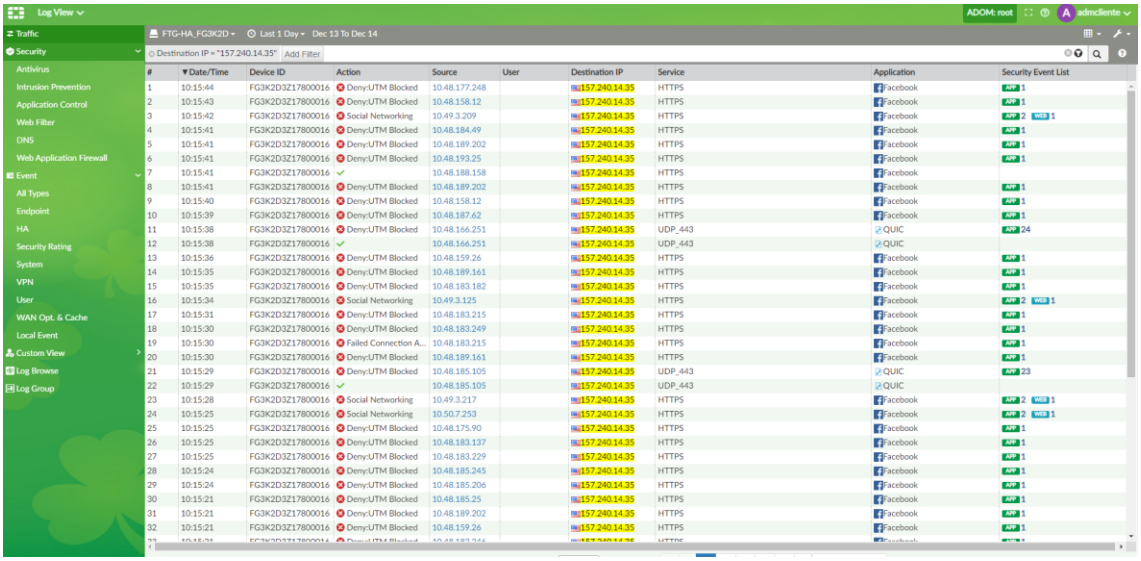
Amenazas bloqueadas en tiempo real



Nota. Amenazas tiempo real tomado de FortiAnalyzer.

Figura 60

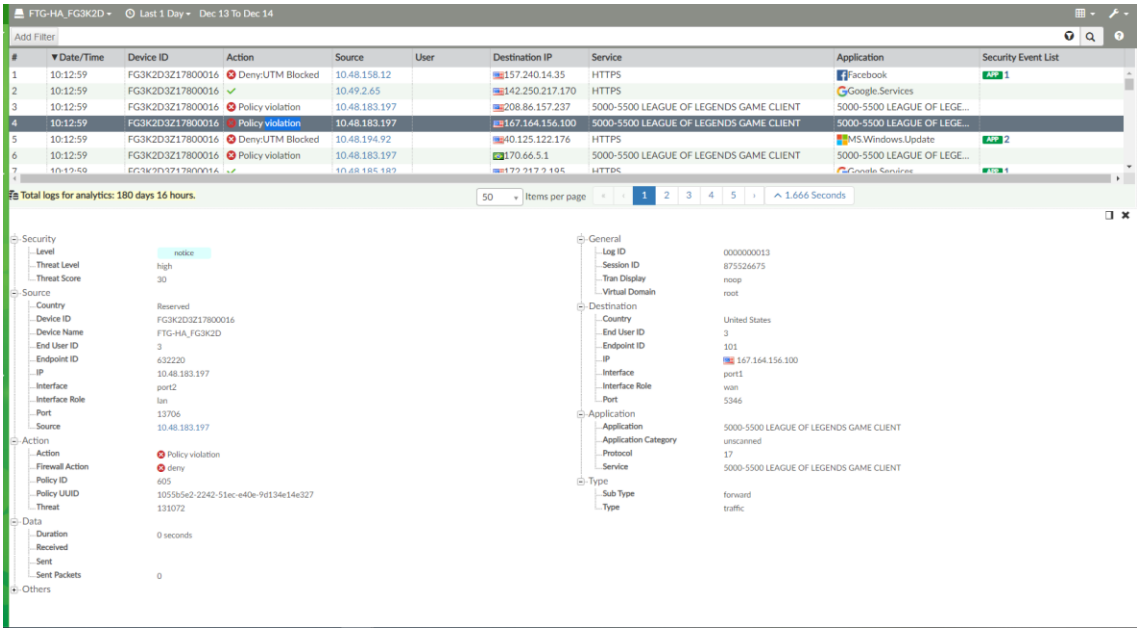
División de tráfico por países



Nota. División del tráfico por países tomado de FortiAnalyzer

Figura 61

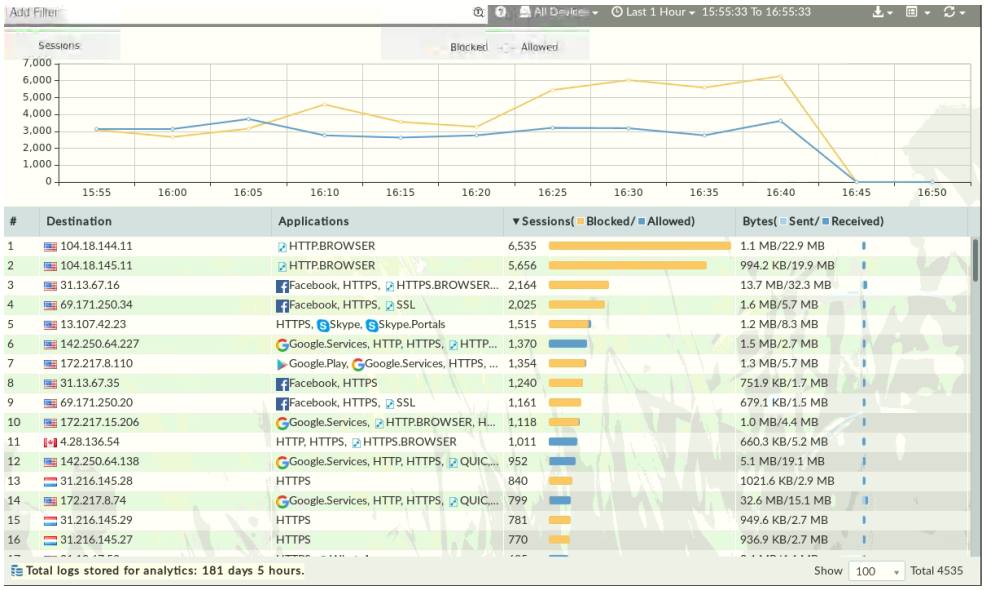
Violación de Políticas de Seguridad



Nota. La figura representa cuando se viola una de las políticas de seguridad impuestas por la autoridad, y podemos qué tipo de política se ha violado y cuál es la IP que ha incurrido en este incidente.

Figura 62

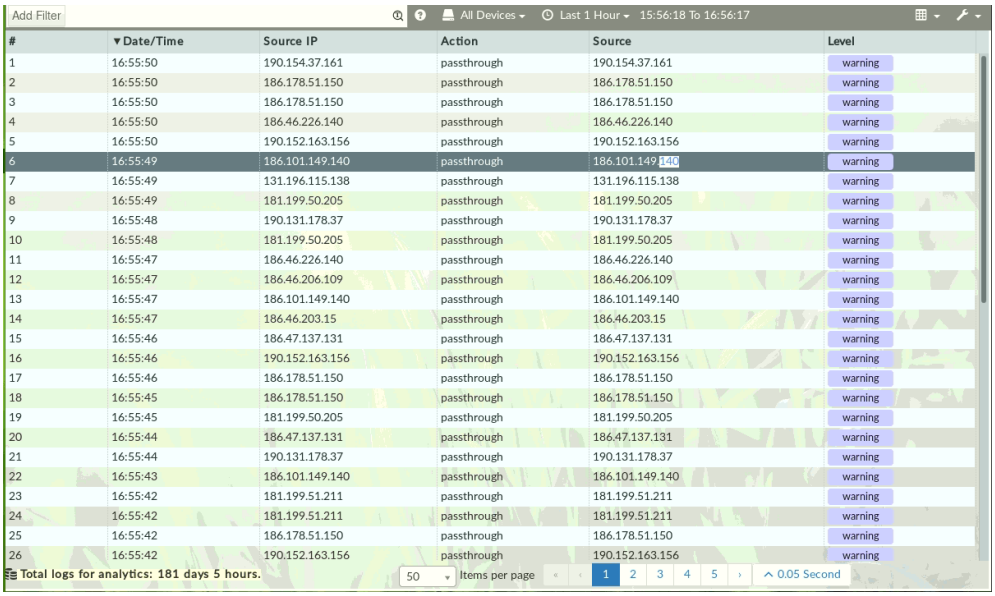
Destinos comunes



Nota. Los destinos comunes tomado de FortiAnalyzer.

Figura 63.

Conexiones aceptadas por el firewall

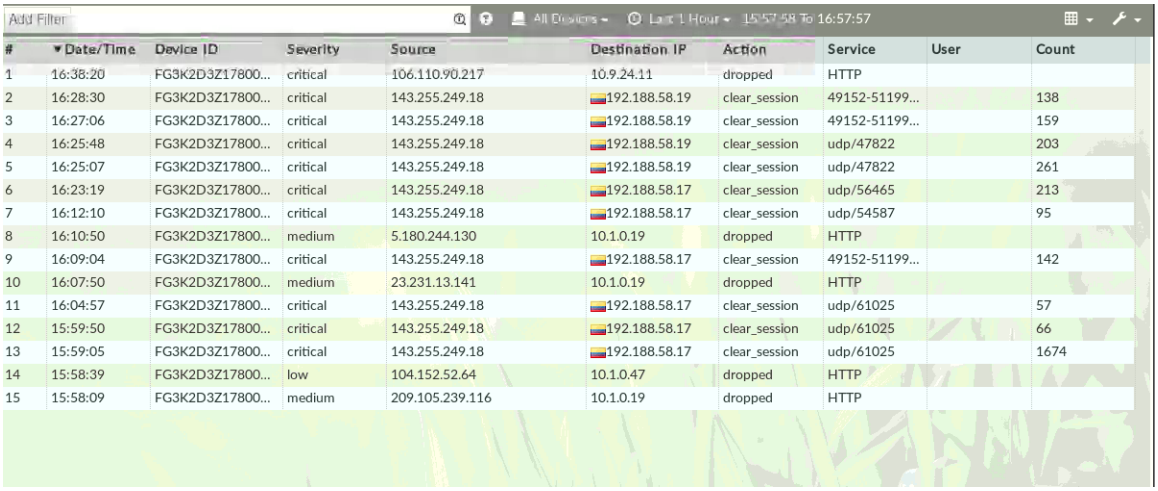


#	Date/Time	Source IP	Action	Source	Level
1	16:55:50	190.154.37.161	passthrough	190.154.37.161	warning
2	16:55:50	186.178.51.150	passthrough	186.178.51.150	warning
3	16:55:50	186.178.51.150	passthrough	186.178.51.150	warning
4	16:55:50	186.46.226.140	passthrough	186.46.226.140	warning
5	16:55:50	190.152.163.156	passthrough	190.152.163.156	warning
6	16:55:49	186.101.149.140	passthrough	186.101.149.140	warning
7	16:55:49	131.196.115.138	passthrough	131.196.115.138	warning
8	16:55:49	181.199.50.205	passthrough	181.199.50.205	warning
9	16:55:48	190.131.178.37	passthrough	190.131.178.37	warning
10	16:55:48	181.199.50.205	passthrough	181.199.50.205	warning
11	16:55:47	186.46.226.140	passthrough	186.46.226.140	warning
12	16:55:47	186.46.206.109	passthrough	186.46.206.109	warning
13	16:55:47	186.101.149.140	passthrough	186.101.149.140	warning
14	16:55:47	186.46.203.15	passthrough	186.46.203.15	warning
15	16:55:46	186.47.137.131	passthrough	186.47.137.131	warning
16	16:55:46	190.152.163.156	passthrough	190.152.163.156	warning
17	16:55:46	186.178.51.150	passthrough	186.178.51.150	warning
18	16:55:45	186.178.51.150	passthrough	186.178.51.150	warning
19	16:55:45	181.199.50.205	passthrough	181.199.50.205	warning
20	16:55:44	186.47.137.131	passthrough	186.47.137.131	warning
21	16:55:44	190.131.178.37	passthrough	190.131.178.37	warning
22	16:55:43	186.101.149.140	passthrough	186.101.149.140	warning
23	16:55:42	181.199.51.211	passthrough	181.199.51.211	warning
24	16:55:42	181.199.51.211	passthrough	181.199.51.211	warning
25	16:55:42	186.178.51.150	passthrough	186.178.51.150	warning
26	16:55:42	190.152.163.156	passthrough	190.152.163.156	warning

Nota. Conexiones aceptadas por el firewall, tomado de FortiAnalyzer.

Figura 64

Trafico bloqueado por el IPS incluido en los equipos Fortinet



#	Date/Time	Device ID	Severity	Source	Destination IP	Action	Service	User	Count
1	16:38:20	FG3K2D3Z17800...	critical	106.110.90.217	10.9.24.11	dropped	HTTP		
2	16:28:30	FG3K2D3Z17800...	critical	143.255.249.18	192.188.58.19	clear_session	49152-51199...		138
3	16:27:06	FG3K2D3Z17800...	critical	143.255.249.18	192.188.58.19	clear_session	49152-51199...		159
4	16:25:48	FG3K2D3Z17800...	critical	143.255.249.18	192.188.58.19	clear_session	udp/47822		203
5	16:25:07	FG3K2D3Z17800...	critical	143.255.249.18	192.188.58.19	clear_session	udp/47822		261
6	16:23:19	FG3K2D3Z17800...	critical	143.255.249.18	192.188.58.17	clear_session	udp/56465		213
7	16:12:10	FG3K2D3Z17800...	critical	143.255.249.18	192.188.58.17	clear_session	udp/54587		95
8	16:10:50	FG3K2D3Z17800...	medium	5.180.244.130	10.1.0.19	dropped	HTTP		
9	16:09:04	FG3K2D3Z17800...	critical	143.255.249.18	192.188.58.17	clear_session	49152-51199...		142
10	16:07:50	FG3K2D3Z17800...	medium	23.231.13.141	10.1.0.19	dropped	HTTP		
11	16:04:57	FG3K2D3Z17800...	critical	143.255.249.18	192.188.58.17	clear_session	udp/61025		57
12	15:59:50	FG3K2D3Z17800...	critical	143.255.249.18	192.188.58.17	clear_session	udp/61025		66
13	15:59:05	FG3K2D3Z17800...	critical	143.255.249.18	192.188.58.17	clear_session	udp/61025		1674
14	15:58:39	FG3K2D3Z17800...	low	104.152.52.64	10.1.0.47	dropped	HTTP		
15	15:58:09	FG3K2D3Z17800...	medium	209.105.239.116	10.1.0.19	dropped	HTTP		

Nota. Conexiones aceptadas por el firewall, tomado de FortiAnalyzer.

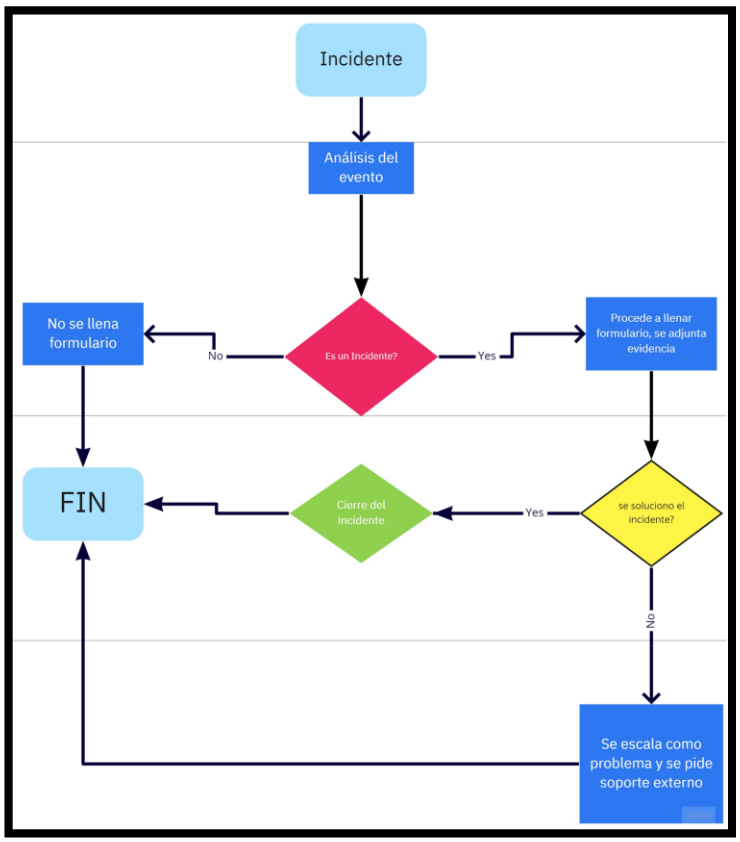
Gestión de Incidencias

La gestión de incidencias se basa en los análisis previos a cada a evento a suscitarse, y se consideran un incidente cuando perjudican y/o comprometen la seguridad de la información de la institución.

Al momento de Gestionar un Incidente el personal del SOC va a necesitar hacer un análisis previo de los eventos que las herramientas de seguridad informática proveen como son los PRTG que son las alertas enviadas por el servidor cuando pasa algún incidente al personal encargado de esta actividad. La siguiente figura es un diagrama de procesos que describe los pasos que ejecuta el personal del SOC para la Gestión de una Incidencia.

Figura 65

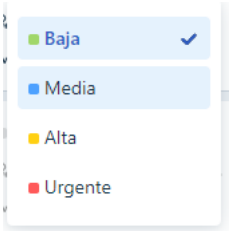
Diagrama de procesos para gestionar un incidente



Se va a llevar a cabo la gestión de un incidente cuando en este caso se realice una solicitud en el portal https://socespe.freshdesk.com/support/home o cuando el operador encuentre algún incidente dentro de las herramientas Shodan, Nessus, FortiAnalyzer, GLPI. El personal designado a tratar el incidente debe categorizarlo en el software de gestión de tickets y proceder a la revisión y análisis del mismo

Figura 66

Categorización de un incidente

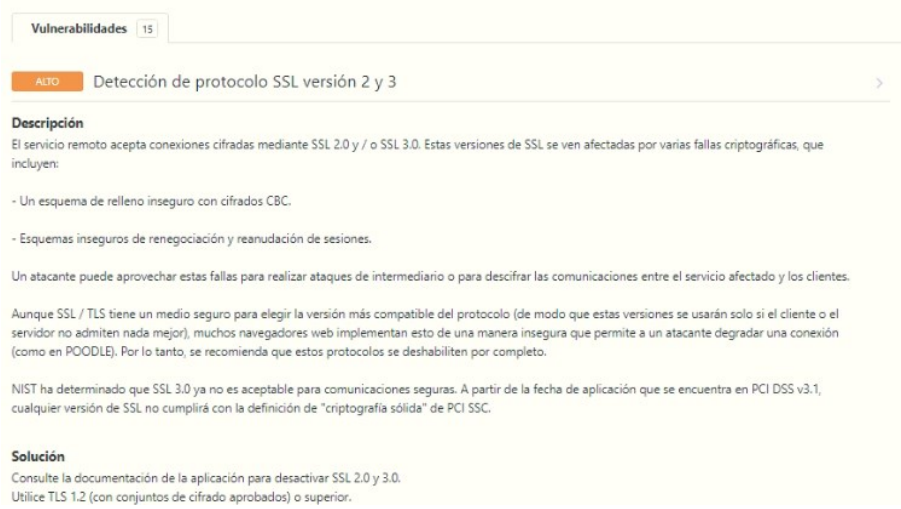


Nota. La figura indica la categorización del incidente en la página que genera los tickets seleccionando las opciones baja, media, alta y urgente

En el caso de realizar un escaneo de vulnerabilidades en Nessus, este categoriza automáticamente la información para dar facilidades al operador entregando los tipos de vulnerabilidades divididos por su importancia; cada análisis de vulnerabilidad viene acompañado de su descripción y una recomendación que facilita al personal a solucionar problemas.

Figura 67.

Ejemplo de entrega de información de Nessus

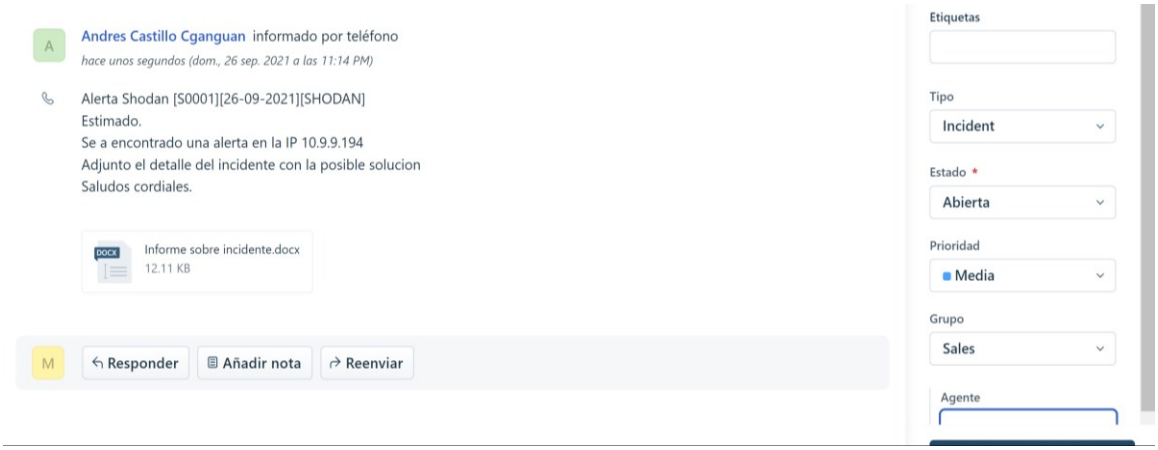


Nota. La figura representa un ejemplo del resultado que arroja la herramienta Nessus sobre una vulnerabilidad encontrada.

Después del análisis del incidente encontrado en las herramientas Shodan, Nessus o FortiAnalyzer el operador realiza un informe indicando los detalles del incidente: IPs involucradas, nombres de usuarios o host, tipos de servicios, puertos vulnerados y recomendaciones para su solución y si se solucionó o no sino se escala al siguiente nivel. El informe es enviado vía correo electrónico al administrador de la infraestructura TI de la institución para dar cierre al incidente sino para seguir escalando para su resolución. Este informe también sirve para ser documentado dentro de las bases de datos para tener respaldo ante cualquier necesidad o novedad a fututo.

Figura 68

Ejemplo de correo electrónico para alertas de un incidente

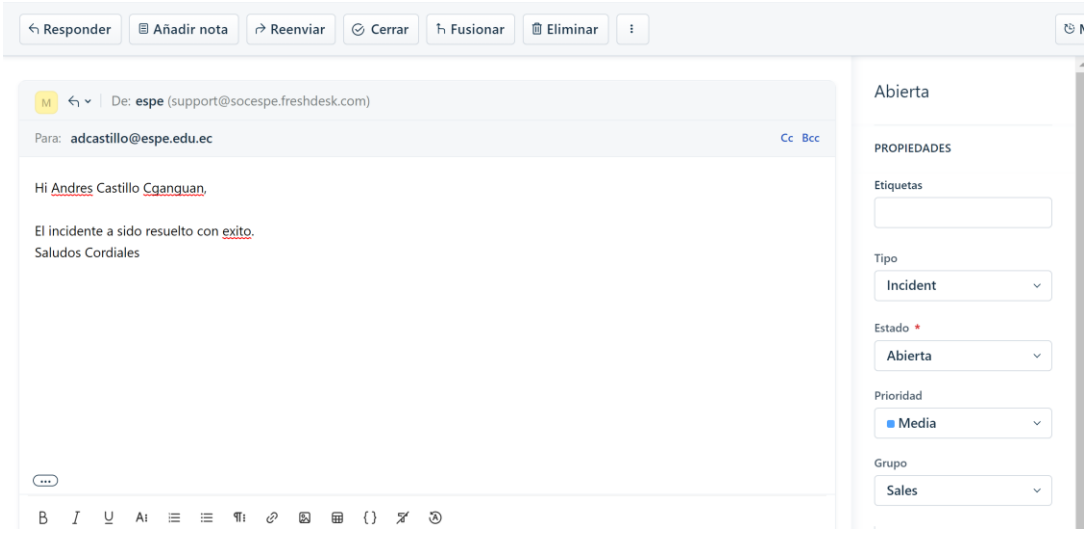


Nota. La figura es un ejemplo de correo electrónico enviado al administrador de la infraestructura TI para alertar un incidente.

Para cerrar el incidente es necesario que el administrador de la infraestructura TI responda indicando que se solucionó el problema; si el administrador no responde, el incidente quedará abierto en el sistema de tickets, esto permite hacer un seguimiento a cada caso.

Figura 69

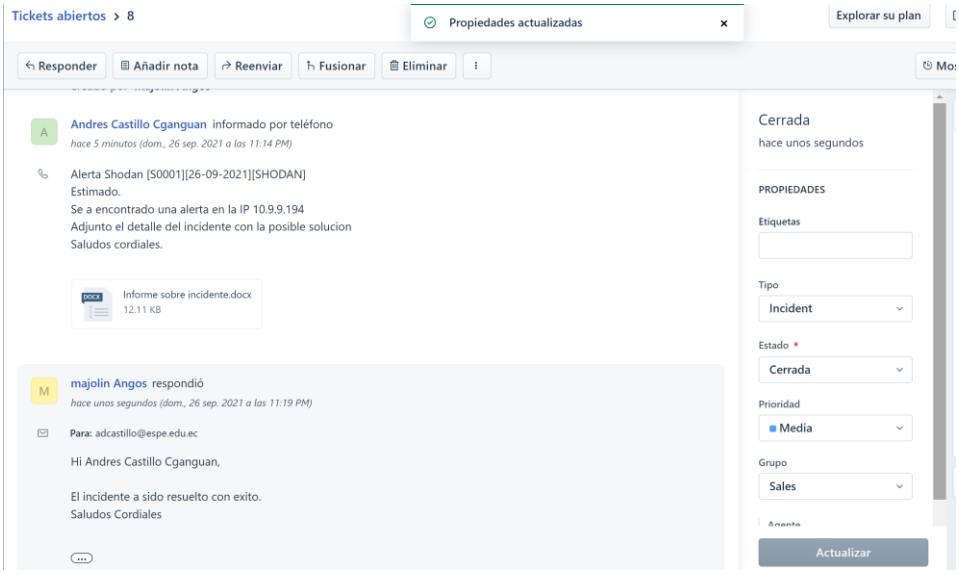
Ejemplo de la respuesta ante un incidente



Nota. La figura es un ejemplo de correo electrónico recibido por parte del administrador de la infraestructura TI indicando que fue solucionada el incidente alertado al SOC y su resolución.

Figura 70

Resolución y cierre de un incidente



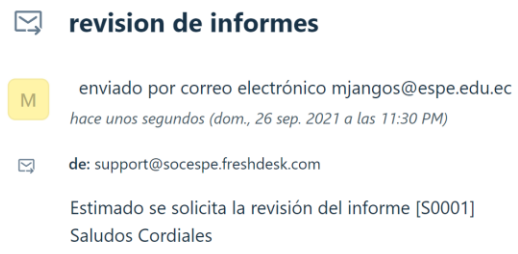
Nota. La figura representa el cierre del incidente después que el administrador de la infraestructura TI haya indicado que fue resuelto.

Gestión de peticiones

Para la gestionar las peticiones de una forma ordenada se configuró un sistema de gestión de tickets, el cual permite al usuario realizar peticiones mediante el correo support@socespe.freshdesk.com con el nombre de SOC y página de soporte https://socespe.freshdesk.com/support/home.

Figura 71

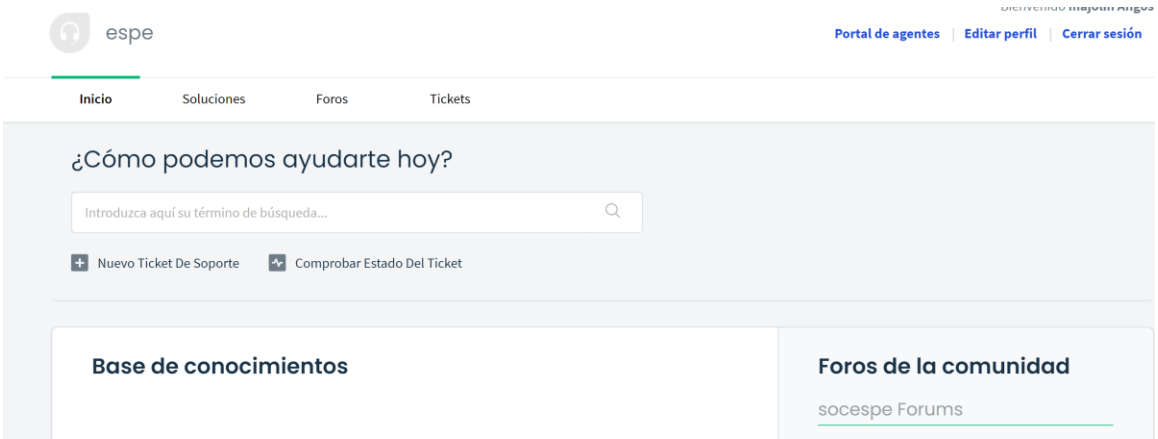
Ejemplo de petición al correo electrónico SOC



Nota. La figura indica un ejemplo de petición de un cliente al SOC.

Figura 72

Ejemplo de petición al portal SOC

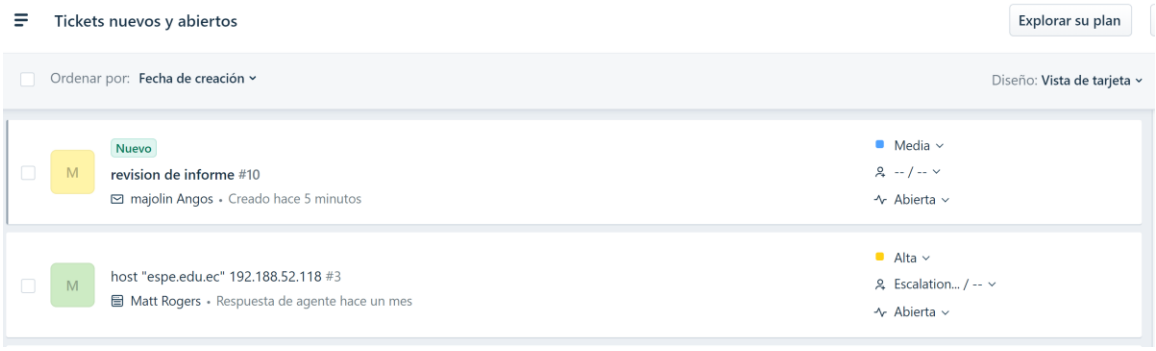


Nota. La figura indica que el portal del SOC cuenta con un botón para generar un ticket o una petición.

Como podemos observar en las anteriores figuras, el cliente puede generar una petición desde correo o desde el portal del SOC, esta petición llegará al dashboard y se transformará en un ticket para que el personal pueda solucionarlo:

Figura 73

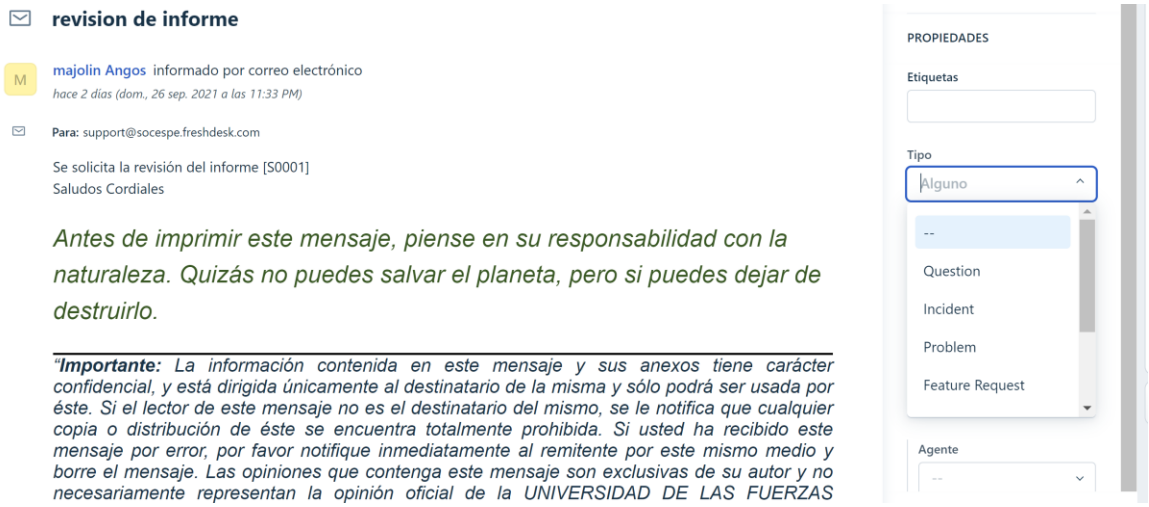
Recepción de petición del cliente



El equipo de trabajo seleccionará al personal encargado de dicha petición y asignará una categorización, dependiendo el tipo de solicitud.

Figura 74

Selección del tipo de solicitud.



Nota. La figura indica la selección que realiza el personal según el tipo de solicitud recibida.

Gestión de Problemas

Un problema es determinado si un incidente es repetitivo y no tiene solución después de seguir los diferentes niveles que se establecen, en este caso del SOC optará por buscar información y soporte con SOC similares dentro de nuestro país, tomando en cuenta que para este caso es importante no enviar información crítica de la universidad ya que sería una violación a nuestra ciberseguridad.

Si el problema sigue sin solucionarse, se solicitará soporte a las marcas de los equipos instalados en la infraestructura vulnerada, si el problema persiste se optará por el cambio de los equipos comprometidos.

Gestión de Accesos

La Gestión de Accesos son los permisos que se da al personal para manejar la infraestructura TI configurada para operar el servicio; esta se realizó según el rol del personal dentro del SOC, intentando proteger los sistemas implementados dando autorización para el mantenimiento y administración solo al personal de directivos e implementadores.

En este sentido se formo el SOC con personal fuera de las UTICS debido a que el SOC va encaminado a controlar que se apliquen correctamente todas las políticas y procedimientos dentro de las UTICS en la seguridad.

Tabla 23

Gestión de Accesos al personal SOC

Personal	Herramienta	Acceso
Walter Marcelo Fuertes Díaz	GLPI	Administrador
	FortiAnalyzer	Visualización
	Nessus	Administrador del sistema
	Freshdesk	Agente
Freddy Mauricio Tapia León	GLPI	Visualización
	FortiAnalyzer	Visualización
	Nessus	Standard
	Freshdesk	Agente
Mario Bernabé Ron Egas,	GLPI	Administrador
	FortiAnalyzer	Visualización
	Nessus	Administrador del sistema
	Freshdesk	Agente
Maria Jose Angos Cosios	GLPI	Administrador
	FortiAnalyzer	Visualización
	Nessus	Administrador del sistema
	Freshdesk	Administrador del Portal

Nota. La tabla representa el control de acceso del personal a las diferentes herramientas implementadas. Si ingresa personal nuevo el implementador y administrador entregará los usuarios y claves de acceso.

Service Desk

El soporte y mantenimiento designado para la infraestructura del SOC viene dado por un service desk virtual, esto significa que se dará soporte de forma remota y personal. Este tipo de Service Desk fue seleccionado por la situación actual de la ESPE ya que por

el momento el país por el virus del Covid-19 y la universidad se encuentra trabajando con los alumnos y docentes de formar virtual y el personal administrativo de forma presencial.

Gestión de Operaciones TI

En el presente literal se describe las actividades del personal dentro del ciclo de vida normal del servicio, garantizando que la operación del servicio sea continua y que la infraestructura TI sea aprovechada de mejor manera. La siguiente tabla lista al personal a cargo de las diferentes actividades que realiza el SOC.

Tabla 24.

Gestión de operaciones TI

Nombre	Rol	Funciones
Walter Marcelo Fuertes Díaz	Director General	- Organizar roles. - Aprobar actividades del SOC - Control de avance del equipo. - Estrategia de crecimiento y creación de nuevos servicios. - Notificación de servicios a las demás unidades de la institución. - Gestión para la contratación de personal. - Procesos administrativos.
Mario Bernabé Ron Egas	Analista de servicios especiales	- Localizar vulnerabilidades. - Análisis técnico de software y hardware para el SOC - Elaborar estrategias y soluciones para un incidente.
	Capacitador	- Dar capacitaciones al personal sobre temas de seguridad de la información. - Encontrar socios o convenios para la capacitación del personal. - Recomendar mejoras de procesos. - Estar al día con temas relacionados al análisis de vulnerabilidades y amenazas de la seguridad de la información.
Maria Jose Angos Cosios	Monitor de redes	- Detección de posibles alertas de seguridad. - Manejo de herramientas de seguridad de la información. - Cuidar la información privada del monitoreo. - Manejo de incidentes. - Informe de incidentes.
	Implementador	- Creación de nuevos usuarios y contraseñas. - Mantenimiento a servicios. - Instalación de actualizaciones. - Implementar infraestructura para nuevos servicios.
Freddy Mauricio Tapia León	Miembro del Comité de Tecnología	- Asesorar cambios en el SOC - Recomendar actividades. - Asesorar en políticas del SOC - Asistencia a la dirección. - Trámites administrativos.
	Investigador	- Planificar y diseñar proyectos de investigación. - Publicar investigaciones sobre el SOC. - Elaboración de artículos científicos.

Nota. Esta tabla muestra las responsabilidades del personal en la operación del servicio.

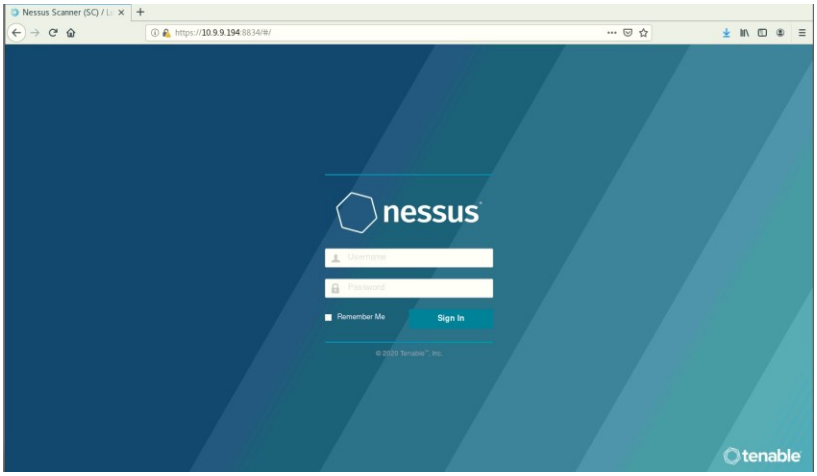
Evaluación de la operación de servicio

Evaluación de Nessus

Para búsqueda de vulnerabilidades dentro de la red de la ESPE se configuró un servidor con Centos 8 para la instalación de Nessus, intentando detectar amenazas, debilidades, errores de configuración y vulnerabilidades los dispositivos conectados dentro de la infraestructura de red de la ESPE.

Figura 75

Panel de control de Nessus



Nota. La figura indica el funcionamiento de Nessus dentro del servidor.

Tabla 25

Evaluación de operación de la herramienta Nessus

Herramienta	Funciones	Cumplimiento	Observaciones
Nessus	Descubre vulnerabilidades	Si	Nessus cuenta con escaneo de vulnerabilidades, detalles de riesgo y los niveles críticos.
	Informes y alertas	Si	Permite generar informes de escaneos hechos por el personal de manera gráfica y ordenada
	Manejo de incidentes	No	No permite el manejo de tickets por host escaneado.

Control de accesos	Si	Utiliza 2 tipos de usuarios: administrador y standard.
Alerta de malware.	Si	Realiza escaneos propios para detectar malware
Información sobre soluciones de problemas.	Si	Siempre da recomendaciones para la solución de varias fallas de seguridad que se suscitan dentro del sistema.
Feeds	Si	Siempre provee información sobre nuevas amenazas encontradas junto con tendencias de ciberseguridad y soluciones a casos detectados.
Monitoreo de eventos en tiempo real	No	No dispone de visualización en tiempo real.

Nota. La tabla representa la evaluación de la herramienta Nessus para cumplir las funciones que requiere un operador del SOC.

$$x=1-\text{Número de funciones faltantes Número de funciones requeridas}\times 10$$

$$x=1-28\times 10=7,5$$

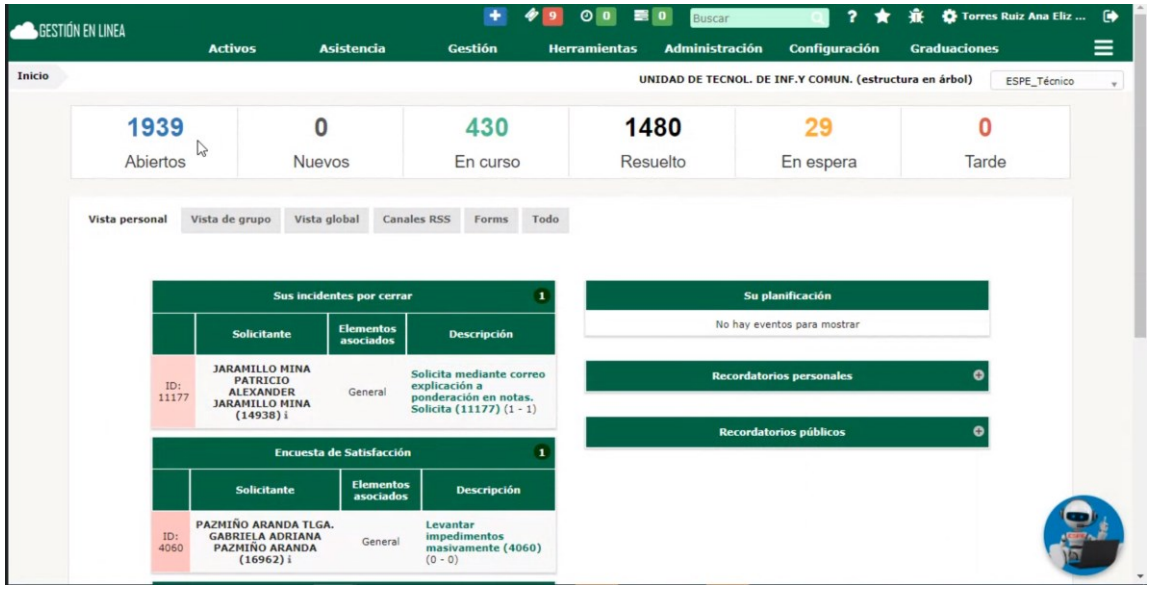
Evaluación de GLPI

El SOC ha optado por utilizar el GLPI, lo cual para el presente proyecto se configuró para recibir alertas en tiempo real sobre los servicios puestos en línea, y los tipos de procedimientos que se deben realizar

Resultado:

Figura 76

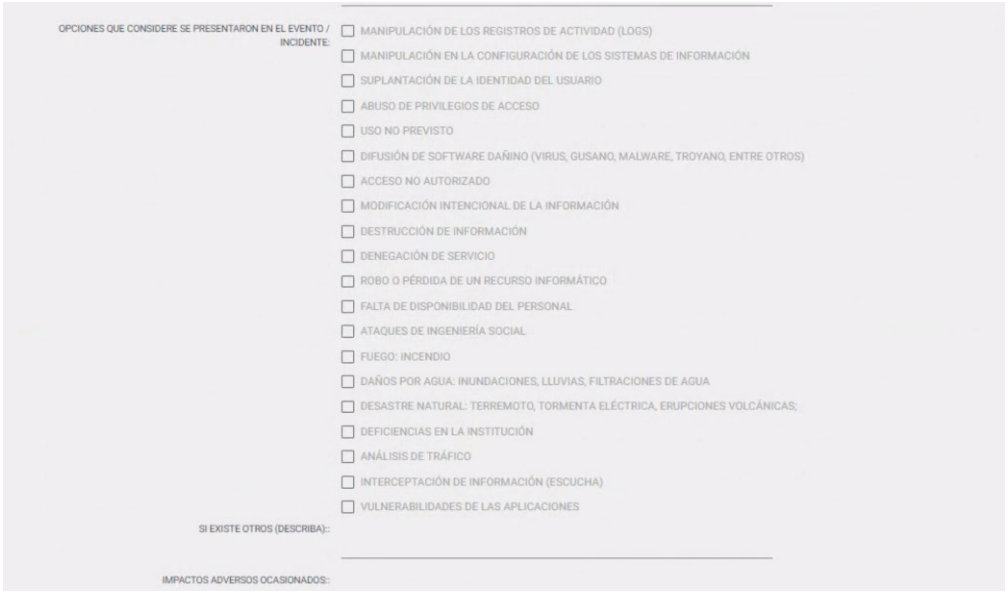
Operación sobre las alertas que envía



Nota. La figura indica el uso de las alertas enviadas

Figura 77

Tipo de incidentes configuradas para el SOC predeterminadas



Nota. La figura indica los tipos de Incidentes que se encuentran predeterminados pero también tiene la opción de escribir una que no haya sucedido.

Tabla 26

Evaluación de operación de GLPI.

Herramienta	Funciones	Cumplimiento	Observaciones
GLPI	Descubre vulnerabilidades	Si	Indica ciertas vulnerabilidades como: puertos abiertos, servicios, etc.
	Informes y alertas	Si	Tiene la posibilidad de generar informes de búsquedas y vulnerabilidades
	Manejo de incidentes	SI	SI maneja los incidentes hasta un segundo escalón.
	Control de accesos	Si	Solo personal autorizado puede ingresar a esta pagina para responder a los incidentes suscitados o subir al escalón superior para que los resuelvan
	Alerta de malware.	Si	Existe escaneos propios para detectar malware.
	Feeds	No	No posee esta cualidad debido a que netamente verifica incidentes.
	Monitoreo de eventos en tiempo real	Si	Permite el monitoreo en tiempo real, mediante alertas enviadas por correo electrónico.
	Uso externo mediate APIs	Si	Usa las llaves de acceso.

Nota. La tabla representa la evaluación de la herramienta GLPI para cumplir las funciones que requiere un operador del SOC.

$$x=1\text{-Número de funciones faltantes Número de funciones requeridas}\times 10$$

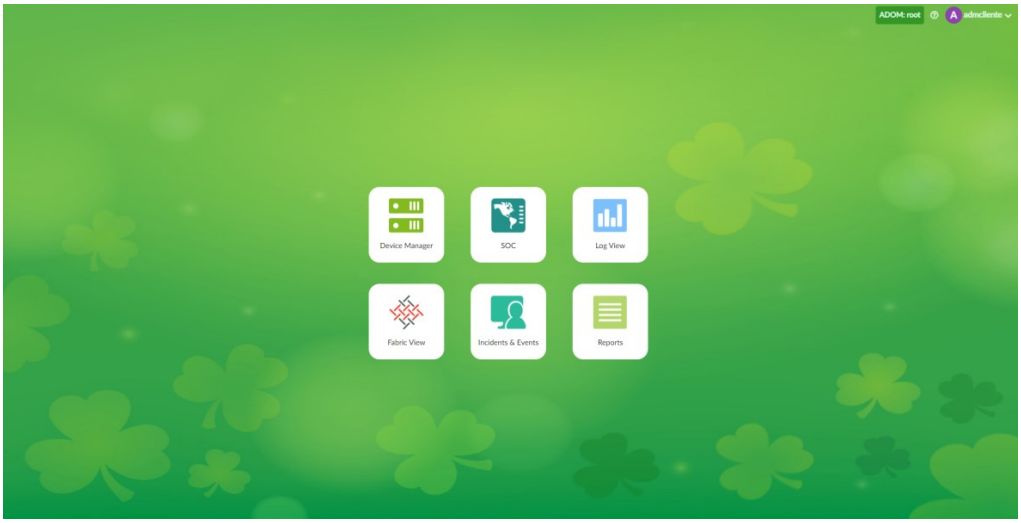
$$x=1\text{-}23\times 10=9{,}0$$

Evaluación de FortiAnalyzer

El FortiAnalyzer es usado por el SOC para generar las políticas del tráfico de todas las extensiones que pertenecen a la ESPE (ESMIL, ESSUNA, IDIOMAS, ESPE SANTO DOMINGO, ETC.), también se puede monitorear en tiempo real las amenazas y los hosts comprometidos dentro de la red local de la universidad ya que analiza todo lo q sale de red interna.

Figura 78.

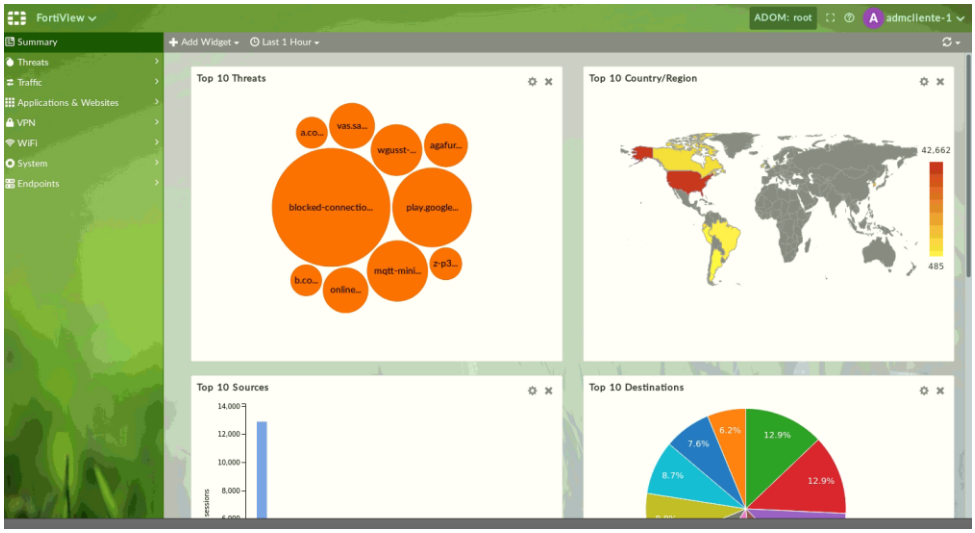
Escritorio de FortiAnalyzer.



Nota. La figura indica el menú principal del dispositivo FortiAnalyzer

Figura 79

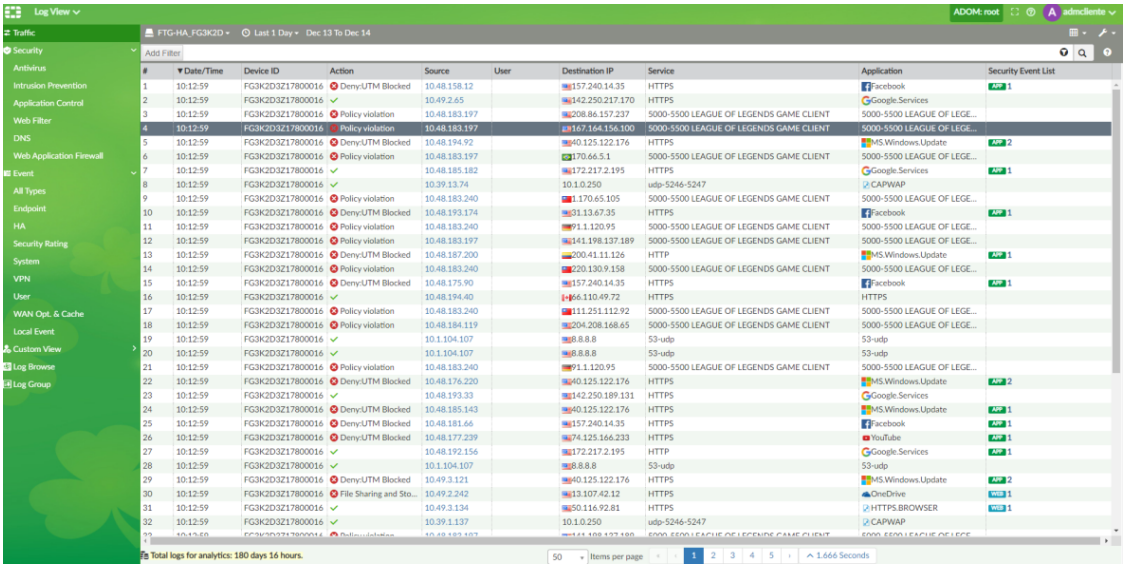
Resumen de amenazas y conexiones maliciosas.



Nota. La figura indica el resumen de amenazas y conexiones maliciosas dentro de la red de la ESPE

Figura 80

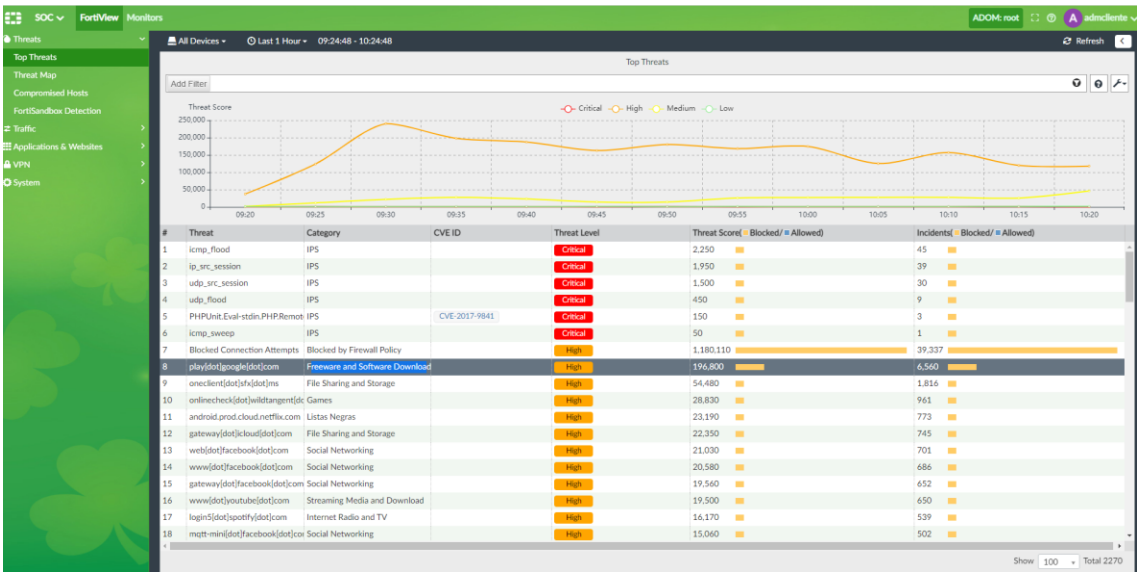
Listado de host comprometidos



Nota. La figura describe los hosts que incumplen las políticas impuestas.

Figura 81

Listado de IPs que incumples con las políticas vistas desde el SOC propio de FortiAnalyzer



Nota. La figura indica el listado de IPs que no cumplen con las políticas.

Tabla 27

Evaluación de operación de FortiAnalyzer

Herramienta	Funciones	Cumplimiento	Observaciones
FortiAnalyzer	Descubre vulnerabilidades	Si	Nos permite verificar las siguientes vulnerabilidades, puertos abiertos, servicios, etc., de la red de la Universidad.
	Informes y alertas	No	No tiene la opción de generar informes
	Manejo de incidentes	No	No permite el manejo de tickets.
	Control de accesos	Si	Se puede manejar la creación de usuarios y contraseñas
	Alerta de malware.	Si	Existe escaneos propios para detectar malware.
	Presenta datos mundiales de amenazas	Si	A través de NOC-SOC del FortiAnalyzer se puede ver las tendencias a ataques mundiales.
	Monitoreo de eventos en tiempo real	Si	Monitorea eventos en tiempo real
	Toma acciones en tiempo real	Si	Tiene un sistema de bloque automático basado en las políticas establecidas por las autoridades.

Nota. La tabla representa la evaluación de la herramienta FortyAnalyzer para cumplir las funciones que requiere un operador del SOC.

$$x=1-\text{Número de funciones faltantes Número de funciones requeridas}\times 10$$

$$x=1-22\times 10=8,25$$

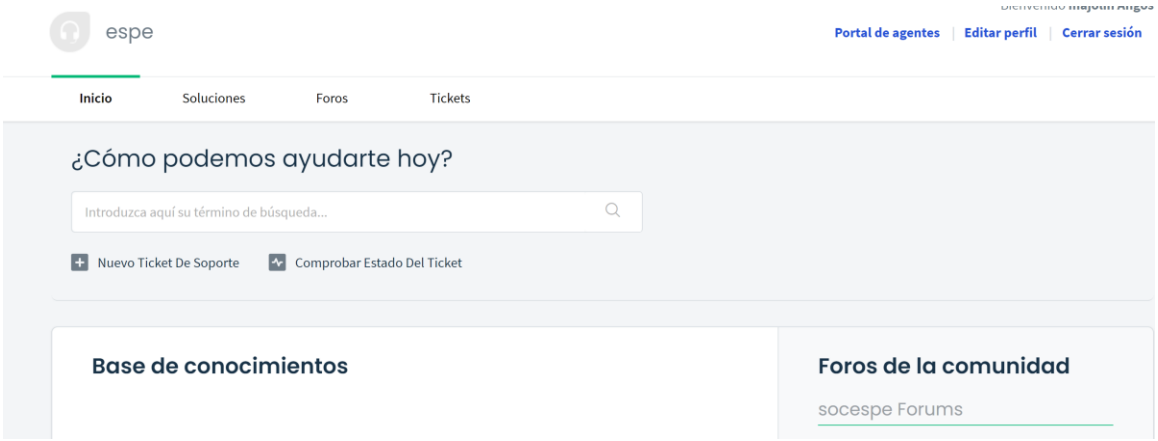
Evaluación de Freshdesk

El servicio web de Freshdesk fue instalado para la gestión de incidentes, herpes, soporte y peticiones de los clientes hacia el SOC. Se levantó un portal de atención al

cliente y un dashboard para gestionar tickets y poder gestionar cada petición de forma ordenada con todo el equipo de trabajo.

Figura 82

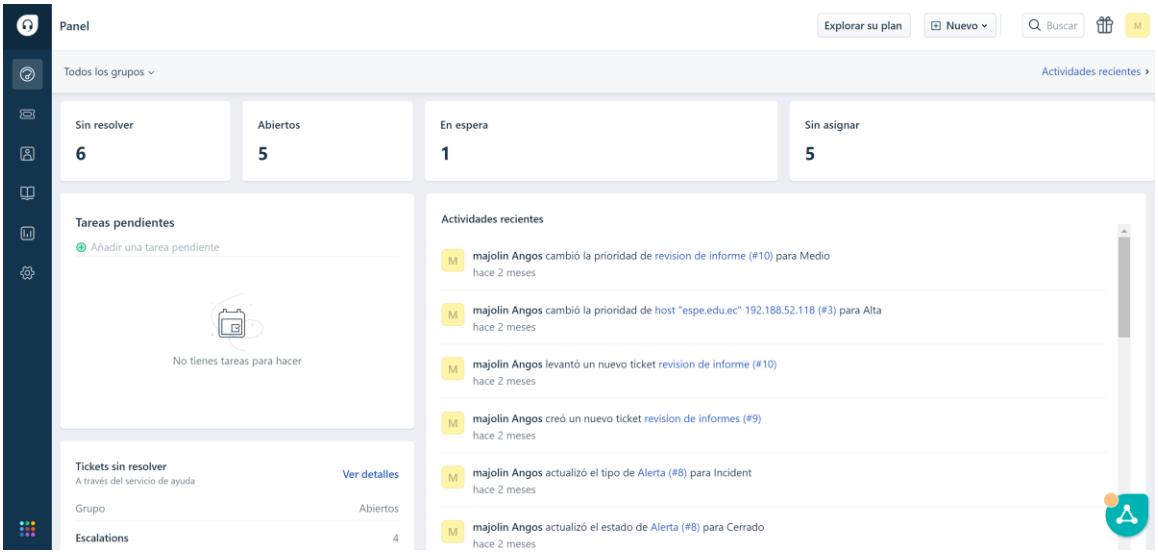
Operación del Portal SOC de servicio al cliente



Nota. La figura indica el portal SOC para servicio al cliente o recepción de solicitudes.

Figura 83

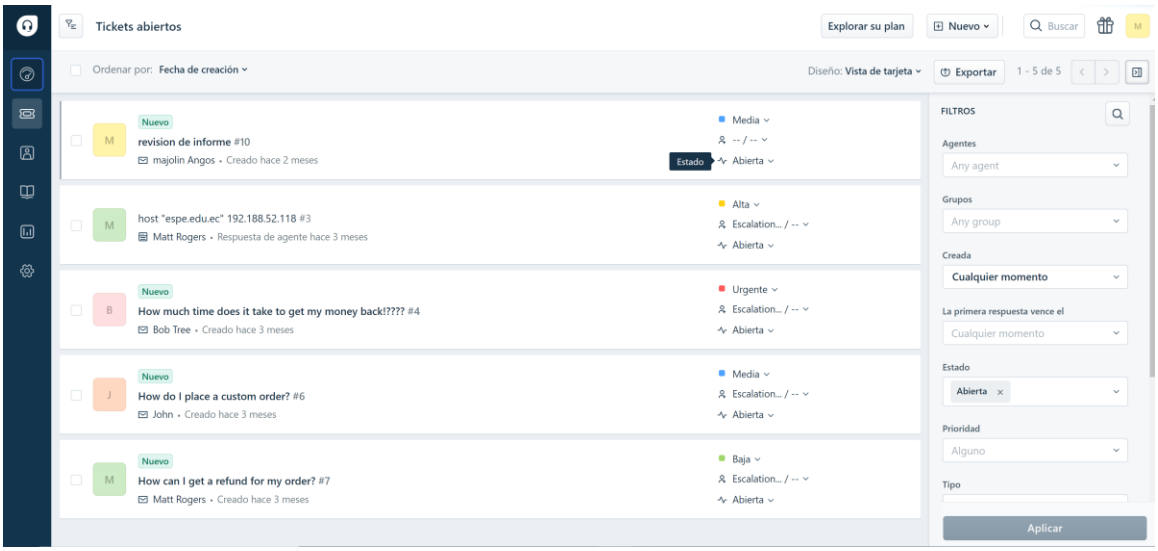
Dashboard de gestión de peticiones e incidentes.



Nota. La figura indica el dashboard principal para el agente de servicios.

Figura 84

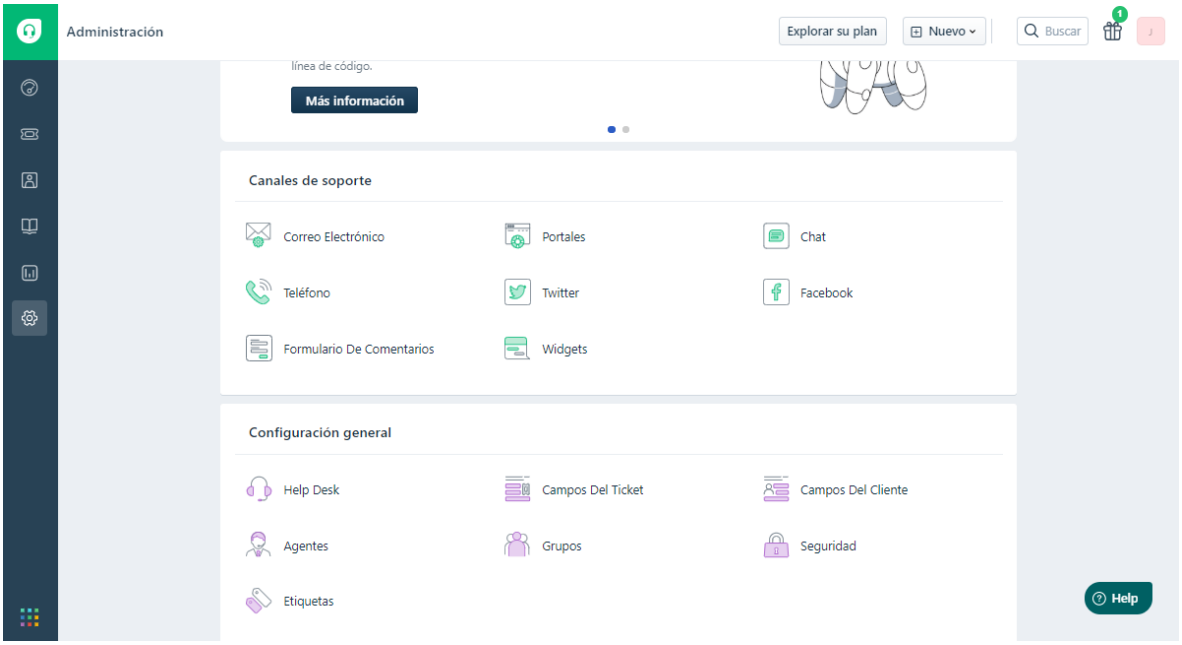
Listado de tickets o solicitudes



Nota. La figura describe el listado de peticiones hechas por los clientes o por los servicios enlazados.

Figura 85

Administración de Freshdesk



Nota. La figura describe el panel de administración del portal SOC

Tabla 28

Evaluación de operación de Freshdesk

Herramienta	Funciones	Cumplimiento	Observaciones
Freshdesk	Manejo de incidentes	Si	Permite gestionar varios tipos de solicitudes
	Manejo de peticiones	Si	Permite gestionar varios tipos de solicitudes
	Comunicación por correo	Si	Cuenta con un correo propio de servicio al cliente.
	Control de accesos	Si	Permite creación de agentes y contraseñas
	Categorización de peticiones	Si	Permite categorizar las peticiones por tipo e importancia.
	Configuración del sitio de acuerdo a las necesidades de la empresa	Si	Fácil administración.
	Seguimiento de ticket	Si	Indica al agente si un ticket no está resuelto.
	Informes	Si	Realiza informes didácticos por semana, mes, año para control de calidad.

Nota. La tabla representa la evaluación de la herramienta Freshdesk para cumplir las funciones que requiere un operador del SOC.

$$x=1-\text{Número de funciones faltantes Número de funciones requeridas}\times 10$$

$$x=1-010\times 10=10$$

Evaluación General de la operación del servicio.

La evaluación general de las herramientas y sus funciones vienen descritos en la siguiente tabla, siendo clasificados los valores de la siguiente manera:

- No cumple: 0-4
- Insuficiente: 4-6
- Aceptable: 6-8
- Satisfactorio: 8-10

Tabla 29

Evaluación general de herramientas del SOC

Herramienta	Estado actual	Métrica		Valor	Puntuación
Nessus	En operación	Cumplimiento funciones	de	7,5	Aceptable
GLPI	En operación	Cumplimiento funciones	de	9,0	Satisfactorio
FortiAnalyzer	En operación	Cumplimiento funciones	de	8,25	Satisfactorio
Freshdesk	En operación	Cumplimiento funciones	de	10	Satisfactorio

Cabe recalcar que las herramientas fueron escogidas para cumplir los servicios iniciales del SOC y estas se complementan entre sí, por ejemplo, si alguna herramienta no cuenta con alguna funcionalidad se implementó otra que cumpla si cumpla y así cubrir todos los requisitos de los servicios básicos del SOC.

Para la evaluación de la puesta en marcha inicial del SOC vamos a tomar en cuenta los servicios implementados juntamente con sus funciones, los cuales comprenden de:

Tabla 30

Funciones de los servicios básicos de un SOC

Servicio	Funciones
Alertas y advertencias	- Descubrir ataque - Descubrir vulnerabilidad - Alerta de malware. - Aviso del problema surgido
Tratamiento de incidentes	- Recepción de peticiones - Respuesta de peticiones - Aportar soluciones a partir de una alerta o vulnerabilidad. - Categorizar peticiones - Actuar para proteger sistemas y redes con vulnerabilidad.
Análisis de incidentes	- Análisis de la información obtenida - Análisis de eventos. - Análisis de alcance de un incidente. - Análisis de soluciones.
Apoyo en la respuesta de incidentes	- Ayuda por teléfono. - Ayuda por correo electrónico. - Ayuda por informes.
Coordinación de la respuesta a incidentes.	- Estrategias de mitigación. - Ayuda en la recuperación. - Análisis de posibles ataques - Colaboración con otras áreas de la institución. - Coordinar con el personal los diferentes casos.

La evaluación general de la operación viene dada por las funciones de cada uno de los servicios básicos de un SOC, contrarrestando con las herramientas implementadas para verificar su cumplimiento.

Tabla 31

Evaluación general del servicio y herramientas

Servicio	Función	Herramienta que sustenta	Cumplimiento de función%
Alertas y advertencias	Descubrir ataque	FortiAnalyzer, GLPI	100
	Descubrir vulnerabilidad	Nessus, FortiAnalyzer, GLPI	100
	Alerta de malware.	Nessus, FortiAnalyzer, GLPI	100
	Aviso del problema surgido	Nessus, FortiAnalyzer, GLPI	100
Tratamiento de incidentes	Recepción de peticiones	Freshdesk, GLPI	100
	Respuesta de peticiones	Freshdesk, GLPI	100
	Aportar soluciones a partir de una alerta o vulnerabilidad.	Nessus, FortiAnalyzer, GLPI	80
	Categorizar peticiones	Freshdesk, Nessus, FortiAnalyzer, GLPI	100
	Actuar para proteger sistemas y redes con vulnerabilidad.	Freshdesk, Nessus, FortiAnalyzer, GLPI,	90

Análisis de incidentes	- Análisis de la información obtenida	Nessus, GLPI, Freshdesk.	90
	- Análisis de eventos.	FortiAnalyzer, Nessus, GLPI.	80
	- Análisis de alcance de un incidente.	Usuario, FortiAnalyzer, GLPI.	80
	- Análisis de soluciones.	Nessus, GLPI	70
Apoyo en la respuesta de incidentes	- Ayuda por correo electrónico.	Freshdesk	100
	- Ayuda por informes.	Freshdesk, Nessus, FortiAnalyzer, GLPI.	100
	- Estrategias de mitigación.	SOC más el personal de las UTICs	80
Coordinación de la respuesta a incidentes.	- Ayuda en la recuperación.	GLPI, Usuario.	70
	- Análisis de posibles ataques	FortiAnalyzer GLPI Nessus	100
	- Colaboración con otras áreas de la institución.	Freshdesk, SOC	100
	- Coordinar con el personal los diferentes casos.	Freshdesk.	100
		PROMEDIO TOTAL	88.7%

En conclusión, la operación del servicio es satisfactoria y cumple con el 88.7% las funciones básicas de un SOC.

Capitulo V

Conclusiones y Recomendaciones

Conclusiones

- La instalación de un SOC requiere un gran aporte para la adquisición de software y hardware para brindar un servicio independiente de las UTIC, ya que no pueden ubicarse dentro de la misma ni con el mismo personal porque el SOC controla que se cumplan todas las políticas de seguridad impuestas por el SOC. En el presente proyecto se logró realizar el Diseño y la transición inicial al SOC tomando en cuenta los servicios básicos que un SOC debe ofrecer.

- La revisión sistemática de la literatura de la documentación existente y proyectos para la implementación de un SOC, permite la aplicación de buenas prácticas que colaboran para ofrecer un servicio de excelente calidad de forma oportuna y eficiente.

- La mayoría de las herramientas que seleccionamos para este proyecto son gratuitas y las mismas fueron tomadas en cuenta en base a la utilidad y la disponibilidad de recursos que nos permitieron lograr el diseño y la transición inicial del proyecto.

- La visión desde otras entidades como Forty Analizer nos permitió tener un enfoque mucho más amplio sobre las verdaderas funciones que cumple un SOC a nivel Mundial.

Recomendaciones

- Insistir en la formación del personal de la comunidad universitaria en temas de ciberseguridad creando campañas de concientización en pregrado y postgrado

- Buscar la inversión privada para la adquisición del software y hardware para la continuidad del SOC, teniendo presente que la iniciación del proyecto se lo realizo con herramientas gratuitas.

- Ejecutar el trámite y la gestión para que la universidad destine parte del presupuesto anual para la creación del SOC, en cuanto a hardware, software y personal especializado, teniendo en consideración que el presente proyecto se realizó con herramientas gratuitas.

- Aplicar todos los conocimientos adquiridos en las Fuerzas Armadas debido a que la información que se maneja es muy sensible y no existen organismos específicos para la protección de esta área en la institución.

Bibliografía

27002, A. A. (2005.). Tecnología de la información – Técnicas de seguridad – Código de práctica para la gestión de la seguridad de la información. Río de Janeiro: ABNT.

Academy, C. N. (21 de 01 de 2020). Introducción a la Ciberseguridad. Cisco.

Andrade, R. F. (2013). Diseño y dimensionamiento de un equipo de . Sangolqui, Pichincha: ESPE.

Aung, W. p., Lwin, H. H., & Lin, K. k. (2020). Developing and Analysis of Cyber Security Models for Security Operation Center in Myanmar.

Avila, F. (24 de Enero de 2020). *Análisis de malware automatizado.* Obtenido de http://www.disoftin.com/2020/01/analisis-de-malware-automatizado.html

AXELOS. (2019). *ITIL 4 FUNDATION .* Axelos Global best Practice.

Beal, V. (2016). *Snort.* Obtenido de https://www.webopedia.com/TERM/S/Snort.html

Brighttalk. (2018). *McAfee ePolicy Orchestrator (ePO).* Obtenido de https://blog.infranetworking.com/servidor-web/#Que_es_un_servidor_web

Ciberseguridad, I. N. (11 de Octubre de 2019). ¿Conoces la nueva norma para la gestión de la privacidad?

Cisco. (2019). *CCNA Cybersecurity Operations.* Obtenido de https://static-courseassets.s3.amazonaws.com/CyberOps11/es/index.html#0.0.1.1

De la Torre Moscoso H.M. & Parra Rosero, M. (2018). Estrategia y Diseño de un equipo de respuesta ante incidentes de seguridad informatica CSIRT academico para la Univrsidad de las Fuerzas Armadas ESPE. Sangolqui, Ecuador.

Delgado, D. O. (21 de Marzo de 2017). *Qué es Snort: Primeros pasos.* Obtenido de https://openwebinars.net/blog/que-es-snort/

Dimitrov, W., & Syarova, S. (2019). Analysis of the Functionalities of a Shared ICS Security Operations Center. *Big Data, Knowledge and Control Systems Engineering (BdKCSE)*, (pág. 6).

Docs, N. (2018). *www.netgate.com/.* Obtenido de https://cdn2.hubspot.net/hubfs/1826203/why-to-series/pfsense-why-64-bit.pdf

ESPE. (2015). Reglamento Organico del Gestion Organizacional por procesos de la ESPE. Sangolqui, Pichincha, Ecuador: ESPE.

ESPE. (2018). Plan Estrategio de Desarrollo Institucional . Sangolqui, Pichincha, Ecuador: ESPE.

García-Peñalvo, F. J. (15 de mayo de 2020). La evaluación online en la educación superior en tiempos de la COVID-19. *Online Assessment in Higher Education in the Time of COVID-19*. salamanca, España.

HelpSystems. (2020 de Mayo de 2020). *¿Qué es un SIEM?* Obtenido de https://www.helpsystems.com/es/blog/que-es-un-siem

Innovablack. (2019). *FIREWALL PFSENSE.* Obtenido de https://www.innovablack.com/firewall/

ISO/ICE. (2005). 17719 Tecnologias de la Informacion- Tecnicas de Seguridad- Codigo para la Practica de la gestion de la seguridad de la informacion.

Kear, S. (16 de enero de 2018). *¿Qué es pfSense?* Obtenido de https://turbofuture.com/computers/Introduction-to-pfSense-An-Open-Source-Firewall-and-Router-Platform

Kemp, S. (s.f.). *we are social*. Obtenido de https://wearesocial.com/

Lubis, M., Wardana, C., & Widjajarto, A. (2020). The Development of Information System Security Operation Centre (SOC): Case Study of Auto Repair Company. *Advances in Intelligent Systems and Computing*, 19.

McAfee. (2019). *McAfee ePolicy Orchestrator.* Obtenido de https://www.mcafee.com/enterprise/enus/products/epolicy-orchestrator.html

Mendoza, M. Á. (18 de Mayo de 2015). *Welivesecurity.com*. Obtenido de https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

Merino, J. C. (2016). Implementación de un modelo de la seguridad de la información basados en ITIL v3 para una Pyme de TI. *Implementación de un modelo de la seguridad de la información basados en ITIL v3 para una Pyme de TI*. Peru.

Minchev, I. G. (2018). Virtual enterprise data protection. *BISEC 2018At:* , (pág. 6). Belgrade, Serbia.

Moloch. (2019). *Moloch - Full Packet Capture*. Obtenido de https://molo.ch/.

Normalización, O. I. (6 de agosto de 2019). ISO/IEC 27701:2019.

OSI. (11 de Octubre de 2016). *Malware. Cuál es su objetivo y cómo nos infecta.* Obtenido de https://www.osi.es/es/actualidad/blog/2016/10/11/malware-cual-es-su-objetivo-y-como-nos-infecta

Perera, V. H., Senarathne, A. N., & Rupasinghe, L. (2019). Intelligent SOC Chatbot for Security Operation Center. *2019 International Conference on Advancements in Computing (ICAC).*

Petersen, F. M. (2018). Grupos de Control.

Pratt, M. (28 de noviembre de 2017). Obtenido de What is SIEM software? How it works and how to choose the: https://www.csoonline.com/article/2124604/what-is-siem-softwarehow-it-works-and-how-to-choose-the-right-tool.html

Rios, S. (2017). *Manual itil V4 integro.*

Ron Egas Mario, V. C. (2017).

Security, S. (2018). *Sandbox Security Defined.* Obtenido de https://www.forcepoint.com/cyber-edu/sandbox-security

Shodan. (25 de julio de 2020). *Shodan.* Obtenido de https://sodan.io

Simon, K. (2021). *We are social* . Obtenido de https://wearesocial.com/

stats, I. w. (2018). *Internet World Stats*. Obtenido de https://www. internetwordstats.com

Techterms. (8 de Julio de 2016). *Sandboxing Definition.* Obtenido de https://techterms.com/definition/sandboxing

Velasco, R. (8 de Noviembre de 2014). *Analiza el tráfico de una red desde la web con Moloch.* Obtenido de //www.redeszone.net/2014/11/08/analiza-el-trafico-de-una-red-desdela-web-con-moloch/

Vieites, A. (2014). Enciclopedia de Seguridad Informatica. Madrid, España: RA-MA, S.A.

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Manfred Vielberth; Fabian Böhm; Ines Fichtinger; Günther Pernul. *Cybersecurity Incident Response*.

Anexo A