Implementación y puesta en marcha de un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT académico) en el Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE basados en ITIL

Benavides Cabascango, Jonathan Francisco

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Sistemas e Informática

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

Ing. Ron Egas, Mario Bernabé Ms.C

17 de agosto 2020

URKUND

Document Information

Analyzed document	Tesis CERT ESPE Jonathan Benavides.docx (D77823983)
Submitted	8/16/2020 6:03:00 PM
Submitted by	RON EGAS MARIO BERNABE
Submitter email	mbron@espe.edu.ec
Similarity	3%
Analysis address	mbron.espe@analysis.urkund.com

MARIO BERNABE RON EGAS
Firmado digitalmente por MARIO BERNABE RON EGAS
Fecha: 2020.08.16 13:16:42 -05'00'

Revisado Ing. Mario B. Ron Egas MSc
16/28/2020

Sources included in the report

SA	**Universidad de las Fuerzas Armadas ESPE / Tesis Creación CSIRT_ESPE -Parra-De la Torre.docx** Document Tesis Creación CSIRT_ESPE -Parra-De la Torre.docx (D40778738) Submitted by: mbron@espe.edu.ec Receiver: mbron.espe@analysis.urkund.com	13
W	URL: https://docplayer.es/1122086-Universidad-nacional-autonoma-de-mexico.html Fetched: 10/22/2019 4:52:03 PM	5
W	URL: https://upcommons.upc.edu/bitstream/handle/2099.1/20065/Adaptacion_de_la_metodolog ... Fetched: 10/9/2019 11:01:04 PM	2
SA	**PLAN DE INVESTIGACIÓN 1.docx** Document PLAN DE INVESTIGACIÓN 1.docx (D61985591)	8
SA	**Informe Final de Tesis - 2019.pdf** Document Informe Final de Tesis - 2019.pdf (D59937174)	4
W	URL: https://docplayer.es/41151389-Universidad-peruana-union.html Fetched: 11/25/2019 9:58:50 PM	1
SA	**Universidad de las Fuerzas Armadas ESPE / Trabajo Integrador Final_Mario Ron_Especialización en Criptografía y Seguridad Tel ...** Document Trabajo Integrador Final_Mario Ron_Especialización en Criptografía y Seguridad Tel ... (D27888826) Submitted by: mbron@espe.edu.ec Receiver: mbron.espe@analysis.urkund.com	1

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Implementación y puesta en marcha de un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT académico) en el Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE basados en ITIL**" fue realizado por el señor **Benavides Cabascango, Jonathan Francisco** 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, 14 de agosto del 2020

Firma:

.....

Ron Egas, Mario Bernabé Ms.C

C. C 1704229747

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

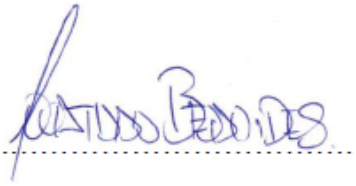
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

RESPONSABILIDAD DE AUTORÍA

Yo, **Benavides Cabascango, Jonathan Francisco**, con cédula de ciudadanía n° 1722736590, declaro que el contenido, ideas y criterios del trabajo de titulación: **Implementación y puesta en marcha de un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT académico) en el Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE basados 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, 14 de agosto del 2020

Firma



Benavides Cabascango, Jonathan Francisco

C.C.: 1722736590

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

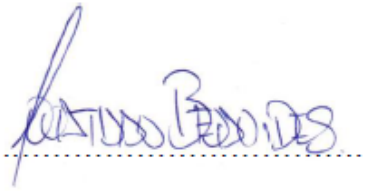
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

AUTORIZACIÓN DE PUBLICACIÓN

Yo **Benavides Cabascango, Jonathan Francisco,** con cédula de ciudadanía n° 1722736590, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Título: Implementación y puesta en marcha de un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT académico) en el Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE basados en ITIL** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 14 de agosto del 2020

Firma



Benavides Cabascango, Jonathan Francisco

C.C.: 1722736590

Dedicatoria

El presente trabajo lo dedico principalmente a Dios,

Y a mis padres que han sido mi motivación y fuerza para seguir adelante,

y cumplir mis metas como profesional.

Agradecimiento

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 padres y familiares que han sido mi apoyo y guía en todo este proceso.

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

A mi pareja que ha me ha apoyado en las buenas y malas, y ha servido de motivación para alcanzar mis metas.

A mis compañeros cercanos que han sido motivación y amigos 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

Las amenazas informáticas han ido incrementando a los largos de los años, en donde Ecuador es el tercer país más atacado de América del sur y el cuarenta y cinco de todo el mundo. Estas amenazas son una parte fundamental que se debe considerar para el levantamiento de nuevos servicios tecnológicos ya que implican un riesgo para cualquier organización. El presente trabajo de titulación tiene como objetivo poner en marcha inicial a un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT Académico) dentro de la Universidad de las Fuerzas Armadas ESPE mediante un análisis previo de la situación actual de la universidad y seleccionando herramientas de seguridad de la información que sean óptimas para levantar un nuevo servicio que tenga como objetivo detectar amenazas y mitigar riesgos para garantizar al personal de la ESPE seguridad en sus conexiones y dispositivos. La Espe pretende extender su desarrollo cognitivo sobre seguridad de la información dando continuidad al proyecto implementando más servicios en el futuro que servirán para la investigación continua y generar nuevas formas de protección de red en la universidad.

PALABRAS CLAVES

- **CSIRT**
- **CERT**
- **ITIL V3**
- **CIBERSEGURIDAD**

Abstract

Computer threats have been increasing over the years, where Ecuador is the third most attacked country in South America and the 45th in the world. These threats are a fundamental part that must be considered for the creation of new technological services since they imply a risk for any organization. The objective of the present degree work is to start up a Computer Security Incident Response Team (Academic CSIRT) within the Universidad de las Fuerzas Armadas ESPE by means of a previous analysis of the current situation of the university and selecting tools of Information security that are optimal for setting up a new service that aims to detect threats and mitigate risks to guarantee ESPE personnel security in their connections and devices. The Espe intends to extend its cognitive development on information security giving continuity to the project, implementing more services in the future that will serve for continuous research and generate new forms of network protection at the university.

KEYWORDS

- **CSIRT**
- **CERT**
- **ITIL V3**
- **CYBERSECURITY**

Capítulo I

Introducción

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 juntamente con sus objetivos. Este capítulo nos sirve como premisa para el inicio del proyecto para tener la claridad de la problemática y hacia dónde queremos llegar con dicho proyecto de titulación. En el capítulo veremos también, la importancia de implementar un CSIRT académico en la ESPE, 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 ha convertido en los últimos años en una parte fundamental del diario vivir de las personas. Actualmente, gracias a una sociedad globalizada por medio del Internet, todo tipo de compañía 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, siendo este un activo importante para cualquier institución, la cual se debe cuidar para evitar poner en riesgo a la organización (Dentzel, 2013).

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 (Cisco Networking Academy, 2020). Una de las practicas que tratan de mitigar y proteger a la información es la consolidación de un CSIRT (Computer

Security Incident Response Team, Equipo de Respuesta ante Incidentes de Seguridad de la Información) que realizan un monitoreo constante de la red y de la infraestructura de TI de la organización, con el objetivo de detectar, informar, mitigar y documentar los riesgos y amenazas tecnológicas encontradas para evitar hechos críticos en base a la seguridad de la Información.

Para el presente proyecto de titulación se ha tomado en cuenta la tesis titulada "Estrategia de diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la universidad de las fuerzas armadas ESPE" presentada en el año 2018, que tiene como objetivo el plantear y diseñar un modelo de CSIRT académico basadas en la etapa uno y dos de ITIL, la cual servirá como referencia para el presente proyecto que se basa en la fase tres y cuatro de ITIL que se refiere a la implementación y a la operación del servicio dentro de los laboratorios de la universidad.

Definición de la problemática

La Universidad de las Fuerzas Armadas ESPE cuenta con 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 varios procesos y operaciones que cuentan con el uso de herramientas de red para lograr su funcionamiento y proveer de mejor manera sus servicios. El avance tecnológico ha hecho que la Universidad se adapte a los cambios en tecnología, principalmente de la Internet. Debido al crecimiento tecnológico, el riesgo ante amenazas informáticas en la Universidad ha aumentado siendo este un peligro para la operación regular de la institución.

De acuerdo con la problemática actual de la Universidad, esta no cuenta con un

Equipo de Respuesta ante Incidentes de Seguridad de la Información (CSIRT Académico) formalmente establecido que permita monitorear y dar seguimiento a las alertas o amenazas informáticas presentadas dentro de la institución, teniendo como consecuencia la vulnerabilidad de la red ante ataques cibernéticos internos o externos y la falta del tratamiento de cada uno de los incidentes de seguridad presentados dentro de la institución.

Dada la situación actual de la ESPE y su déficit en cuanto a seguridad informática, es primordial la creación de un Equipo de Respuesta ante Incidentes de Seguridad de la Información (CSIRT Académico) que monitoree la red de la institución y permita estar preparados ante un incidente de seguridad; esta intentará disminuir el riesgo y las consecuencias dadas por un ataque cibernético y que provea los servicios de seguridad a las diferentes áreas de la universidad, tomando en cuenta que la institución posee servidores propios, red interna entre áreas e información confidencial importante.

Justificación

Según (De la Torre Moscoso & Parra Rosero, 2018), en evaluaciones realizadas al Sistema de Información de la ESPE, se ha determinó que no existe un Equipo de Respuesta ante Incidentes Informáticos 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. Se han elaborado varios proyectos de diseño de CSIRT para la Universidad de las Fuerzas Armadas ESPE, pero únicamente se han quedado en el diseño y estrategia del servicio, sin avanzar en la implementación y puesta en marcha del mismo, siendo esta una solución a los incidentes de seguridad de la información.

Las amenazas informáticas son preocupantes en la región, por lo que existen estadísticas alarmantes de ataques a instalaciones tanto públicas como privadas (Securelist, 2019), de las que no se encuentra libre la universidad, se sabe 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. (Organización Internacional de Normalización, 2018)

Existen riesgos a los que está expuesta la Universidad y que deben ser controlados y mitigados mediante una estrategia con el CSIRT (WeLiveSecurity, 2015), a continuación, se listan los riesgos más comunes:

- Infección de computadores dentro de una red
- Infección de servidores
- Conexión con servidores externos maliciosos
- Falta de control en el manejo de la estructura de TI dentro de la institución
- Acceso no autorizado 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 de titulación se enfoca en mitigar estos riesgos en la Universidad de las Fuerzas Armadas ESPE, entregando un CSIRT funcional que se

encuentre en capacidad de monitorear las áreas críticas de la institución y brindar servicios relacionados con la ciberseguridad. Además, permitirá la formación y capacitación de personal docente, administrativo y estudiantes en el área de la seguridad de la información, fomentando buenas prácticas de seguridad y promoviendo a la investigación activa.

Objetivos

Objetivo General

Implementar y poner en marcha un Equipo de respuesta ante incidentes de seguridad informática (CSIRT Académico) en la Universidad de las Fuerzas Armadas ESPE, utilizando el marco de referencia de ITIL para garantizar el control de amenazas y mitigar el riesgo informático dentro de la institución.

Objetivo Especifico

- Realizar una revisión sistemática de literatura de la documentación y proyectos en marcha que existen para la implementación de un CSIRT Académico.
- Investigar y seleccionar las herramientas de seguridad informática más adecuadas para los servicios iniciales que prestará el CSIRT Académico de la ESPE.
- Determinar la comunidad beneficiaria, la infraestructura y diseñar los servicios que serán implementados en el CSIRT Académico.
- Instalar y configurar el hardware y software necesario para el funcionamiento inicial del CSIRT Académico de la ESPE.
- Evaluar y documentar la operación del CSIRT Académico.

Alcance

El presente proyecto plantea como solución a los problemas de seguridad presentados actualmente en la Universidad de las Fuerzas Armadas, implementando un Equipo de Respuesta ante Incidentes, la cual se toma como referencia principal la tercera y cuarta fase de la metodología presentada por (Ron Egas et al., 2017), juntamente con el trabajo de titulación desarrollado por (De la Torre Moscoso & Parra Rosero, 2018) titulado “Estrategia y Diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE”.

En el trabajo de titulación de (De la Torre Moscoso & Parra Rosero, 2018)se menciona la fase I y la fase II de la metodología mencionada anteriormente, pertenecientes al planteamiento estratégico y al diseño de un CSIRT respectivamente. En el presente trabajo de titulación se propone desarrollar la fase III y fase IV definida por (Ron Egas et al., 2017) la cual se toma como referencia para el desarrollo de la presente propuesta la fase uno y dos ya elaborada por (De la Torre Moscoso & Parra Rosero, 2018).

Fase III.- Transición de Servicios

- Planificación y soporte a la transición
- Gestión de cambios
- Gestión de la configuración y activos del servicio
- Gestión de versiones
- Validación y pruebas del servicio

- Evaluación
- Gestión de conocimiento

Fase IV.- Operación del Servicio

- Gestión de eventos
- Gestión de Incidencias
- Gestión de peticiones de servicio
- Gestión de Problemas
- Gestión de Accesos
- Service Desk
- Gestión de Operaciones TI
- Gestión Técnica
- Gestión de Aplicaciones

Capítulo II

Introducción

En este capítulo se detalla la importancia de la ciberseguridad en la actualidad y el valor que tienen los datos dentro de todo tipo de organización, 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 CSIRT académico que le permita tomar acciones ante alguna acción maliciosa o ante un ataque cibernético.

Para el desarrollo del presente proyecto se ha tomado en cuenta investigaciones pasadas del diseño y la estrategia para la implementación de un CSIRT académico en la ESPE; estos servirán para tener un punto de partida para el desarrollo del presente 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 CSIRT académico. Hay que recordar que la ESPE cuenta con propuestas de diseño de un CSIRT, pero no ha llegado a la fase de implementación.

Se ha tomado como indicador el marco de referencia de ITIL para el desarrollo del proyecto, en este capítulo veremos el 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 es basado en la fase I y fase II ya realizada por alumnos de la ESPE, siendo este un referente importante para continuar con la fase III y

fase IV del mismo. Se verá también las herramientas necesarias para el desarrollo del proyecto, tomando en cuenta el hardware y software indispensable para operación exitosa del CSIRT académico de la ESPE, así como el espacio físico, la metodología de implementación y la descripción de cada una de las herramientas seleccionadas.

Antecedentes Investigativos

Los antecedentes investigativos se basan en la revisión de literatura inicial que se presentó en la propuesta del presente trabajo de titulación. De acuerdo con la literatura analizada y con las características proporcionadas en el Capítulo I se realizó una descripción del problema para obtener un contexto de búsqueda en estudios científicos; además se exploró los objetivos para alinear la búsqueda con el problema descrito.

A continuación; se presenta estudios relacionados con el problema descrito en el Capítulo I en donde se obtendrá palabras clave o términos importantes que se asemejen con el presente proyecto de titulación.

Tabla 1.

Antecedentes Investigativos

Título	Cita	Palabras clave
Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos, CSIRT	(Uyana García, 2014). Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos, CSIRT. Maestría en Gerencia de Seguridad y Riesgo. Universidad de las Fuerzas Armadas ESPE. Sede Sangolquí	SEGURIDAD, INFORMÁTICOS, (CSIRT), INFORMÁTICA, FORENSE, Activos, informáticos, Ataques, informáticos
Artículo científico - Diseño y dimensionamiento de un equipo de respuesta ante	Andrade Paredes, Robeto Omar (2013). Diseño y dimensionamiento de un equipo	Incidentes informáticos, Estándares y tecnología,

Título	Cita	Palabras clave
incidentes de seguridad informática (CSIRT) para la Escuela Politécnica del Ejército	de respuesta ante incidentes de seguridad informática (CSIRT) para la Escuela Politécnica del Ejército. Maestría en Gerencia de Redes y Telecomunicaciones.	Emergencias computacionales, Seguridad informática
Dimensional data model for early alerts of malicious activities in a CSIRT	P. Valladares, W. Fuertes, F. Tapia, T. Toulkeridis and E. Pérez, "Dimensional data model for early alerts of malicious activities in a CSIRT," 2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), Seattle, WA, 2017, pp. 1-8.	CSIRT, Data warehousing, BI, Early Warning to Computer Attacks, ETL Process, OLAP cubes, Dimensional Data Model
Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE	De La Torre Moscoso, Hugo Marcelo y Parra Rosero, Mario Andrés (2018). Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería en Sistemas e Informática. Universidad de las Fuerzas Armadas ESPE. Matriz Sangolquí.	Seguridad informática Protección de datos Control de acceso Estándar ITIL v3
Application of business intelligence for analyzing vulnerabilities to increase the security level in an academic CSIRT	F. X. Reyes-Mena, W. M. Fuertes-Díaz, C. E. Guzmán-Jaramillo, E. Pérez-Estévez, P. F. Bernal-Barzallo, and C. J. Villacís-Silva, "Application of business intelligence for analyzing vulnerabilities to increase the security level in an academic CSIRT," Revista Facultad de Ingeniería, vol. 27 (47), pp. 21-29, Jan. 2018	business intelligence; cybersecurity; decision making; early alerts; electronic data processing; ETL; vulnerability analysis

Dadas las siguientes investigaciones se seleccionó los temimos: CSIRT, CERT, cybersecurity, vulnerability, early alerts dando la cadena de búsqueda: csirt + cert + cybersecurity + early alerts + vulnerability

Para afinar la búsqueda, se tomó en cuenta los buscadores más importantes de documentos electrónicos, papers, tesis, publicaciones, etc, en la cual se insertó los términos de búsqueda anteriormente seleccionados. Al usar dichos términos, SpringerLink mostro 21 resultados de los cuales se tomó los de mayor relevancia para el proyecto actual, que servirán para agrandar la visión del presente proyecto.

El artículo presentado por (Reyes et al., 2018) titulado “A BI Solution to Identify Vulnerabilities and Detect Real-Time Cyber-Attacks for an Academic CSIRT” describe sobre la automatización del proceso de difusión de información de un CSIRT o un CERT, donde los autores ilustran un estudio en el cual detectan los riesgos o amenazas informáticas y los ataques en tiempo real. Los autores presentan una evaluación de dos herramientas de análisis de tráfico, Snort y PVS, estas herramientas les sirvió en la recopilación de datos para construir un sistema BI (Inteligencia de Negocios), donde finalmente, les permitió construir una aplicación web que vincula la información obtenida por las herramientas procesadas en el sistema BI con paneles dinámicos, permitiendo generar alertas tempranas, realizar consultas o búsquedas y demostrar que la toma de datos correctos permite automatizar los procesos la institución, y que la data obtenida pueda servir para un proceso de toma de decisiones.

La tesis planteada por (Uyana García, 2014) titulada “Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos, CSIRT” pretende implementar en un CSIRT (Equipos de respuesta ante incidentes) un área que pretenda analizar un delito informático después que suceda, es

decir un área forense. Tenemos que tomar en cuenta que un CSIRT toma en cuenta las amenazas en tiempo real para poder informar y documentar sobre el riesgo de dicha amenaza. El área forense pretende hacer un análisis minucioso cuando ya ocurrió un incidente, después procesa las evidencias con el uso de una cadena de custodia, y finalmente da lugar a que los investigadores puedan mitigar de mejor manera el riesgo informático.

(Andrade et al., 2012) Proponen un estudio sobre el diseño de un CSIRT enfocada para el área administrativa de la Universidad de las Fuerzas Armadas ESPE. Esta se enfocó en el marco de referencia de ITIL para su aplicación. Los autores determinaron que fue positivo y rentable en ese entonces la aplicación de un CSIRT, tratando de realizar un cambio de la cultura dentro de la seguridad informática. En el presente trabajo se realizó pruebas y procesos de simulación para el personal para concientizar al personal para ver la importancia de un CSIRT dentro de la Universidad.

(De la Torre Moscoso & Parra Rosero, 2018) Propone en su tema de tesis "Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE" realizar la fase I y fase II de ITIL para la implementación de un CSIRT académico en la universidad. Los autores se enfocan en el planeamiento estratégico, la cual se comprende de la conformación del equipo inicial del proyecto, definición inicial de trabajo, estudio de la situación actual, definición de la entidad patrocinadora. Para la segunda parte de su tesis de grado proponen el diseño del CSIRT académico de la ESPE, la cual comprende de: Plan estratégico, plan operativo, análisis y gestión de demanda, portafolio de servicios y relación con otros CSIRT. Se ha tomado como referencia esta tesis de grado para la realización del presente proyecto, ya que en base a esta se realizará la fase III y

fase IV del marco de referencia de ITIL para dar continuidad al proyecto y poner en marcha el CSIRT académico de la ESPE.

(Thompson, 2018) En su artículo científico evalúa el programa de respuesta ante incidentes, dando a entender el aprovechamiento del aprendizaje de otros equipos, para un mejor aprovechamiento del conocimiento. Se toma en cuenta como principal el NIST (National Institute of Standards and Technology) donde, este pretender promover la innovación en base a reglas o normas tecnológicas tomando en cuenta como principal la estabilidad económica. El NIST publica varios documentos para la seguridad de la información, la cual sirve como guía para constituir el plan y el equipo de los proyectos tecnológicos (NIST, 2020). El autor de dicho artículo se enfoca en romper los paradigmas que existen entre los proyectos de seguridad informática con la elaboración puramente técnica del desarrollo de los mismos, es decir propone usar métricas como el NIST para concientizar el uso de estándares que permita ver al usuario que no solo existen problemas de ciberseguridad, si no también que estos acarrean problemas comerciales.

Marco de referencia ITIL para seguridad informática

La tecnología se ha convertido en algo esencial para las empresas pequeñas medianas o grandes, también para instituciones financieras, educativas, del gobierno, etc. Donde ha tomado impulso en los últimos años ya que dichas instituciones requieren realizar procesos más eficientes y rápidos, intentan tener obtener mayor información, mejoran la gestión de servicios, mejoran su control de calidad y su vez incrementar sus ganancias.

Servicios de tecnologías de la información.

Los servicios de tecnologías de la información se refieren a la agrupación de

procesos o actividades que se realizan por medio del uso de la tecnología. Estos conjuntos de procesos se realizan con el objetivo de satisfacer la necesidad del usuario o de los clientes de la organización. Actualmente estas instituciones cuentan con servicios o soluciones tecnológicas que entregan de forma constante al cliente o al personal interno de la organización, a su vez constan con personal humano, tecnológico y procesos especializados para el crecimiento del negocio y para el uso correcto de todos sus procedimientos generando un valor agregado a la empresa.

Según (Merino Vásquez, José Christian; Torres Asencios, 2016) las características de los servicios de tecnologías de la información o también llamados servicios TI tienen dos lineamientos desde el punto de vista del usuario-cliente y estos son:

- La utilidad: se refiere al valor que produce el servicio para la institución.
- La garantía: se refiere al respaldo que cuenta la organización para realizar un servicio de forma correcta.
- Fiabilidad: Esto se refiere al tiempo continuo que los servicios tecnológicos han estado funcionando de manera seguida y sin interrupciones.
- Disponibilidad: Se refiere a la continuidad de uso de los usuarios de una manera correcta.
- Escalabilidad: Se refiere a los servicios tecnológicos que están diseñados para que crezcan juntamente con la empresa.

En conclusión, los servicios de TI son importantes en las instituciones, ya que van de la mano con la empresa para su crecimiento, gracias a que este permite adquirir servidores de correo, almacenamiento virtual, herramientas software, gestión de procesos, etc. Los servicios en tecnologías de la información brindan la apertura de ser

adquiridos y utilizados prácticamente por cualquier persona, ayudando a mejorar la calidad de servicios de la organización, mejorando tiempos y recursos.

Hay que tomar en cuenta que los servicios en TI es un proceso distinto a los demás, ya que no apoya en una sola área si no que aporta un valor agregado a los demás procesos de la empresa, es decir provisiona servicios tecnológicos para el cumplimiento de las metas generales de negocio. Las áreas de tecnologías de la información o proveedores de servicios en tecnología de las organizaciones no entregan solamente un producto si no que se basan en una ola de servicios en la cual la empresa busca mejorar la calidad y el trato hacia el cliente mejorando su nivel de satisfacción a través de distintas plataformas de interacción de usuarios y clientes con las empresas y servicios.

Se ha tomado ITIL como marco de referencia para el presente proyecto, ya que se adapta de mejor manera a la situación actual de la Universidad de las Fuerzas Armadas. En la siguiente tabla se observa las ventajas que tiene ITIL frente a otros modelos, tomando en cuenta las necesidades del proyecto.

Tabla 2.

Comparativa de modelos

Aspectos	PMBOK	CMMI	COBIT	ITIL
Enfoque a procesos dentro de la operación del servicio	X	✓	✓	✓
Modelo orientado a procesos	✓	✓	✓	✓
Modelo orientado a Gestión de Procesos	✓	✓	✓	✓

Aspectos	PMBOK	CMMI	COBIT	ITIL
Modelo orientado a desarrollo	✓	✓	✓	--
Modelo orientado a infraestructura de la organización	X	--	--	✓
El modelo se adapta a todo el ciclo de vida del servicio o producto	✓	✓	✓	✓
El modelo gestiona cambios	✓	✓	✓	✓
El modelo gestiona incidencias	--	✓	✓	✓
Se definen métricas en cada proceso	--	✓	✓	✓
Se definen actividades en cada proceso	X	X	--	✓
Permite el seguimiento a los procesos o actividades del servicio	✓	✓	✓	✓
El modelo se orienta a la mejora continua	✓	✓	✓	✓
Permite la certificación de la institución	--	--	--	--
El modelo se puede adaptar a la ISO 9001	✓	✓	✓	✓
El modelo es compatible con la ISO 200000	✓	✓	✓	✓

Definición de ITIL v3

ITIL por sus siglas en ingles se define como Information Technology Infraestructura Library que en español significa Biblioteca de Infraestructura de

Tecnologías de Información donde (Merino Vásquez, José Christian; Torres Asencios, 2016) lo definen como 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 a los servicios de tecnologías de la información.

(De la Torre Moscoso & Parra Rosero, 2018) Define a ITIL como un marco de referencia que contiene buenos procesos o prácticas para la gestión de los servicios en tecnologías de la información. (Ríos, 2014) Se refiere a ITIL como un conjunto de publicaciones que explica de manera sistemática el conjunto 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 útil para cualquier organización, según (Ríos, 2014) ITIL fue creado para empresas públicas británicas en la década de 1980, pero a lo largo del tiempo ha demostrado su eficiencia y ha sido adoptado por empresas privadas adaptándose a las necesidades y objetivos de negocio. (Ríos, 2014) describe que la guía resulto ser tan útil que a lo largo de los años se ha adaptado en el área 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.

(Merino Vásquez, José Christian; Torres Asencios, 2016) resalta la importancia de ITIL al ser este un marco de referencia que intenta garantizar que los procesos y servicios tecnológicos en la organización estén alineados con las necesidades de la empresa y del cliente. Hay que tomar en cuenta que los servicios TI son utilizados por las empresas para tener éxito y crecimiento continuo.

Según (Guedez, 2018) ITIL es un gran referente en el área de la seguridad informática 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 (Guedez, 2018):

- Conecta las tecnologías de la información con las diferentes áreas de negocio,
- Se adapta a los objetivos y metas de la organización,
- Se enfoca en cada uno de los procesos de la organización,
- Es sencilla de aplicar y adaptar en la organización,
- Mejora la comunicación entre usuarios finales, clientes y empleados de la organización
- Fomenta la eficiencia y efectividad del servicio con un impacto positivo en los recursos financieros de la empresa
- Es una guía práctica para el mejoramiento continuo del servicio
- Cuenta con las buenas prácticas necesarias para el levantamiento de nuevos servicios TI

La edición que rige actualmente de ITIL se publicó en el 2011 con el nombre de ITIL v3, la cual cuenta con 5 fases:

- Estrategia del servicio
- Diseño del servicio
- Transición del servicio
- Operación del servicio
- Mejora continua del servicio

ITIL se compone de estas cinco fases intentando describir en cada una de ellas la guía necesaria para la implementación y puesta en marcha de un servicio en TI que tiende a mejorar continuamente. La Estrategia del Servicio y el Diseño del servicio se basan en los requerimientos que necesita la organización antes de implementar un servicio TI; en cambio la Transición del Servicio, la Operación del Servicio y la Mejora continua del Servicio se basan en la producción misma del servicio TI, siendo así una guía completa para la gestión de servicios tecnológicos.

Estrategia del Servicio

Según (Excutive Master Project Management, 2019) la fase de la estrategia de servicio se basa en el eje fundamental para las siguientes fases en la cual trata de puntualizar los objetivos y metas del negocio, conocer el mercado actual y saber qué servicios se entregará en el futuro basados en las necesidades del cliente. (Wikiversity, 2015) resume la fase de Estrategia de Servicio como el propósito que tiene la empresa para precisar los servicios que se prestarán, el segmento de población y el sector del mercado, es decir determina a primera instancia la estrategia para formar los servicios para saber a quién porque y como serán prestados a los clientes.

La fase de Estrategia de Servicio es llamada como el núcleo de negocio ya que es un parte fundamental y estratégica para definir la estructura del servicio a implementar, gracias a esta estructura el servicio permite la mejora continua, agregando

un valor agregado al cliente.

Según (Wikiversity, 2015) la importancia de la Estrategia de servicios se basa en:

- Sirve en la planificación estratégica para la realización correcta de un FODA (Fortalezas, Oportunidades, Debilidades, Amenazas),
- Ayuda en la constitución de los servicios prioritarios,
- Aclara el valor de los servicios,
- Identifica el segmento de mercado,
- Estable un ROI (Retorno sobre la inversión),
- Usa una guía de los servicios que tienes las demás organizaciones.

La Estrategia de Servicio cuenta con 4 P'S, que significan perspectiva, posición, planificación, patrón:

- Perspectiva: Clarificar objetivos, metas y valores que sean alcanzables,
- Posición: Definir los servicios,
- Planificación: Estructurar reglas para el crecimiento futuro,
- Patrón: Congruencia en la toma de decisiones.

Según (Excutive Master Project Management, 2019) los activos ITIL son:

  - Capacidades: se refiere a la capacidad que tiene la empresa para controlar, organizar y entregar recursos según sean necesarios,
  - Recursos: Se refiere a lo que posee la empresa como activos humanos, físicos, técnicos y financieros)
  - Personas: Aportan la capacidad de realizar algo.

Diseño del Servicio

El Diseño de Servicio se refiere a la acción de analizar la factibilidad y viabilidad del posible servicio, es decir intenta encontrar el correcto uso de los recursos humanos, técnicos, físicos y financieros para que el servicio funcione correctamente y satisfacer las necesidades de la empresa. (Merino Vásquez & Torres Asencios, 2016) define el Diseño de Servicio como la estrategia para crear nuevos servicios o de estructurar de mejor manera los servicios ya existentes; esta fase es previa para la creación de catálogos de servicios.

Según (Wikiversity, 2015) el Diseño de Servicio de ITIL son los siguientes:

- **Procesos de negocio:** Intenta precisar los requisitos funcionales del servicio,
- **Servicio:** es la actividad de solventar las necesidades del cliente,
- **Políticas, estrategias, gobierno conformidad:** procesos revisados por la institución para asegurar el correcto funcionamiento del servicio junto con sus objetivos,
- **SLAs/SLRs (Acuerdos a Nivel del Servicio/ Requisitos de Nivel del Servicio):** se refiere al convenio formal con el cliente para alcanzar los objetivos, calidad, alcance del servicio,
- **Infraestructura:** Ser refiere a los activos físicos que se necesitan para operar el servicio en cuestión,
- **Información:** se refiere a la información que necesita el servicio para operar de manera correcta y para tener en claro los procesos del servicio y poder entregar soporte oportuno siempre y cuando sean necesario,

- **Aplicaciones:** Aplicaciones o software necesario para conseguir la meta del servicio y operar los requisitos funcionales previamente encontrados,
- **Soporte de servicios:** se refiere al auxilio técnico que se entregara si alguna operación del servicio falla,
- **Equipos de soporte:** conjunto de personas o componentes capacitados para realizar un auxilio técnico dentro del desarrollo del servicio,
- **Proveedores:** equipo externo que ayuda en el progreso del servicio,
- **Procesos de gestión de servicio:** Se refiere a las actividades que realiza el proveedor para asegurar la operación del servicio.

Transición del Servicio

El actual proyecto tiene como eje fundamental la presente fase que procederemos a estudiar, junto con la fase siguiente que corresponde a la Operación del Servicio, tomando en cuenta que la Estrategia de Servicio y el Diseño de Servicio se realizó previamente en el trabajo de titulación desarrollado por (De la Torre Moscoso & Parra Rosero, 2018) titulado “Estrategia y Diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE”.

Según (Merino Vásquez, José Christian; Torres Asencios, 2016) la Transición de Servicio es el aseguramiento de que los servicios o productos estudiados en la anterior fase puedan integrarse en los procesos activos de la institución, es decir llevarlos a la fase de producción, donde clientes y los usuarios ya los puedan consumir.

Según (Ríos, 2014) la Transición de Servicio se define como la puesta en marcha o la activación del servicio que se estructuro previamente, donde la idea

principal es poner en funcionamiento el hardware y software necesario para que el servicio este operativo. (Ríos, 2014) recalca que gracias a las anteriores fases de ITIL el servicio no debería contar con costes extras por pérdida de tiempo, recursos o problemas de implantación.

La Transición del Servicio tiene como fin resolver las necesidades del cliente que fueron descritas en la fase de Diseño del Servicio, es decir trata de administrar de manera correcta la información obtenida en las anteriores fases para poner en marcha el servicio o producto de una manera beneficiosa para la institución.

El objetivo de la fase de Transición del Servicio según (Excutive Master Project Management, 2019) es garantizar y asegurar la coordinación adecuada de los recursos obtenidos en la fase de Diseño del Servicio para mitigar el riesgo que pueda impedir el desarrollo del producto o servicio. Esta fase también intenta garantizar que los servicios a poner en marcha cumplan con los estándares obtenidos de las fases previas, dando soporte a todo el proceso supervisando cada actividad a realizar.

Según (Universidad Técnica Virtual Tecnologico de Monterrey, 2019) y (Excutive Master Project Management, 2019) la Transición de Servicios cuenta con los siguientes procesos:

- Planificación y soporte a la transición
- Gestión de cambios
- Gestión de la configuración y activos del servicio
- Gestión de versiones
- Validación y pruebas del servicio
- Evaluación

- Gestión de conocimiento

Planificación y Soporte a la Transición. La (Universidad Técnica Virtual Tecnologico de Monterrey, 2019) describe a la Planificación y Soporte de la Transición como la identificación de protocolos, marcos de trabajo, roles definidos, metas, propósitos, requisitos, interesados, socios, proveedores etc., fundamentales para general una visión general del producto y de su desarrollo, para proceder a la instalación o puesta en marcha del servicio.

(Excutive Master Project Management, 2019) por su parte identifica a este proceso como los elementos principales para un correcto servicio al cliente. En esta fase se define productos tangibles, entregables, tiempos de desarrollo, personal implicado en la operación del servicio, control de calidad, reportes, informes, etc.

El propósito de la Planificación y Soporte de la Transición según (Office of Government Commerce, 2010b) es:

- La planificación de recursos y medios adecuados para la construcción, pruebas o test, despliegue, entrega, establecimiento o modificación de un servicio dentro del proceso de producción de una institución.
- Entregar soporte a los usuarios, software y hardware destinados para dicho servicio.
- Planificar los cambios necesarios en la línea de procesos de producción para asegurar la integridad de los recursos de la compañía y de los clientes.
- Coordinar las actividades del proyecto para entregar el software y hardware necesario siempre y cuando sea necesario.

Gestión de Cambios. La Gestión de Cambios según (Excutive Master Project Management, 2019) es evaluar el anterior punto de planificación verificando que el proceso de levantamiento del nuevo servicio se realice de forma eficiente y garantizando la calidad en todo el proceso. La Gestión de Cambios intenta disminuir el número de problemas o incidentes que se presenten en cuestión al cambio, hay que tomar en cuenta que se intenta agregar un nuevo servicio a la línea de producción entonces se debe asegurar que estos cambios tengan el menor impacto negativo dentro de la institución.

(Office of Government Commerce, 2010b) describe la importancia de los cambios como un beneficio que busca la empresa para crecer, reducir costos, mejorar calidad de servicios y sobre todo satisfacer las necesidades del cliente. También estos cambios pueden ser preventivos, ya que la empresa puede intentar mitigar riesgos o prevenir circunstancias externas o internas en las puede haber pérdidas. El propósito de la Gestión de Cambios según (Office of Government Commerce, 2010b) es:

- Que el proceso se realice de una forma eficiente de tal forma que el servicio se levante de una manera óptima y rápida.
- Responder a las necesidades del cliente intentando obtener el máximo de provecho de los activos tangibles e intangibles de la empresa.
- Resolver el cambio de tecnologías que sufrirá la institución de una forma en la cual el nuevo servicio se alinee a los demás de forma tal que no interrumpa la producción de la institución.

Gestión de la Configuración y Activos del Servicio. La Gestión de la

Configuración y Activos del Servicio según (ITIL Foundation, 2015) se refiere al control de actividades en la configuración de los activos que sirven para poner en marcha el proceso, es decir es la gestión de información que se lleva a cabo al configurar la infraestructura TI necesaria para poner en marcha el servicio. Dicha información se la ingresa a un CMDB (Base de Datos de Configuración).

El CMS en con sus siglas en ingles significa Configuration Management System y CMDB significa Configuration Management Database la cual (Wikiversity, 2015) define como un modelo en el cual se almacena información de la infraestructura de TI compuesta por varias Bases de Datos que reflejan la configuración realizada a los activos.

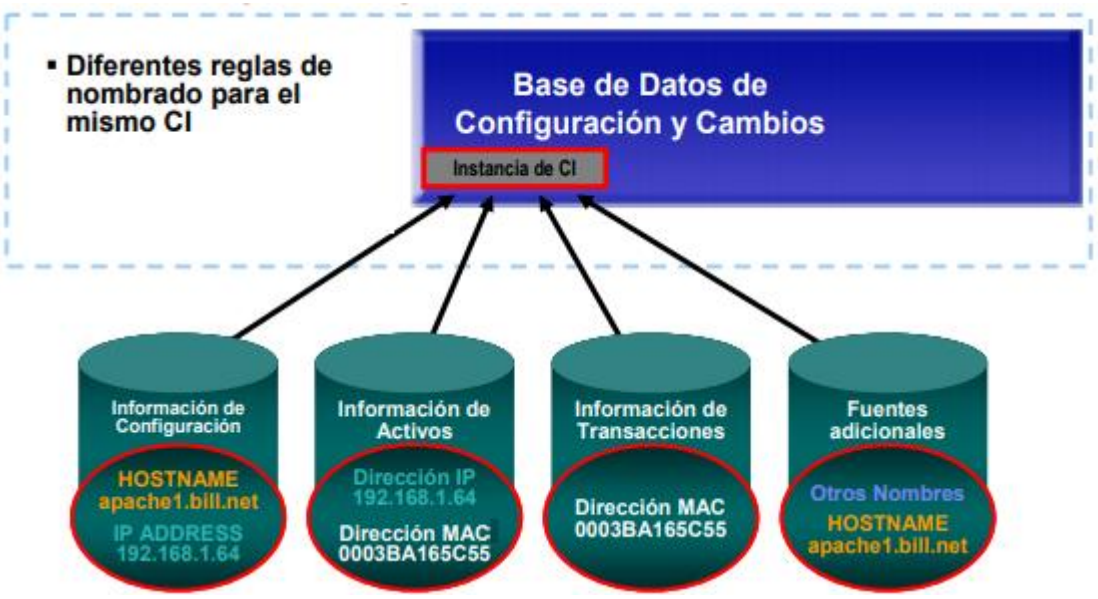
El objetivo de la Gestión de configuración según (Romanos, 2008) es entregar información necesaria a los demás procesos de la empresa para disminuir problemas en los registros de configuración identificando los elementos de la infraestructura necesarios para cada tipo de proceso y servicio.

Cuando hablamos de CIs (Configuration Items) nos referimos a todos los activos tecnológicos que necesita el servicio para poder operar, siendo estos configurados de tal forma que cumplan correctamente con el ciclo de vida del servicio y se saque el mayor provecho de ellos.

La Figura 1 muestra como como el CMDB intenta registrar los diferentes CIs en su base de datos intentando asegurar la integridad de los datos de cada elemento.

Figura 1.

Registro de activos CMDB



Nota. Tomado de *La gestión de la configuración y la gestión de activos como una gestión del conocimiento (p.20)*, por García Romanos, 2009.

El objetivo de gestionar dichos activos en una CMDB es mejorar el valor de herramienta tecnológica y optimizar costos de cada activo; la Gestión de Activos del Servicio intenta garantizar el uso de las herramientas software y hardware dentro del proyecto, esto permite mejorar la toma decisiones y garantizar los estándares legales y corporativos del proyecto. En conclusión, intenta llevar el control del ciclo de vida de los activos que sirven para poner a flote el servicio.

Gestión de versiones. La gestión se versiones se encarga de verificar que las instalaciones de hardware o software estén debidamente autorizadas, tomando en cuenta la calidad del servicio en un entorno de producción.

Según (Ríos, 2014) en su manual de ITIL v3, define a la Gestión de Versiones como el control, entrega y puesta en marcha de las versiones de los activos tecnológicos en un ambiente de producción en donde esta debe planificar cuando y como se deben desplegar las nuevas versiones, asegurar que la instalación del

software y hardware necesario para el correcto funcionamiento del servicio y facilitar la información para el proceso de Gestión del Cambio y Gestión de la Configuración y Activos del Servicio para mantener actualizada a CMDB.

Los principales objetivos de la Gestión de Versiones son:

- Tener una política para la ejecutar nuevas versiones dentro de los activos tecnológicos.
- Implementar las nuevas versiones en los activos tecnológicos verificando la funcionalidad de las mismas disminuyendo el riesgo a fallos.
- Realizar pruebas de versiones.
- Entregar ayuda al proceso de Gestión de Cambios y Configuraciones de Activos de Servicio para que cada cambio sea reflejado en la CMDB correspondiente.
- Mantener actualizado el hardware y software necesario.

Los beneficios de la Gestión de Versiones según (Bravo Campoverde, 2015) se resume en:

- Organizar de mejor manera el cambio para que la calidad de servicio no se vea influenciado.
- Disminuye el riesgo a la incompatibilidad de versiones con otro hardware o software previamente instalado.
- Las pruebas de versiones permiten asegurar que el usuario conozca las nuevas funcionalidades de software o hardware para emitir una opinión sobre su usabilidad.

- Se puede gestionar licencias de software.
- Se reduce la instalación de software ilegales.
- Control de malware asociado a versiones antiguas de software.

Las principales dificultades de la Gestión de Versiones según (Bravo Campoverde, 2015) se resume en:

- No suele haber una persona encargada que haga una revisión continua de versiones dentro de los procesos.
- La organización realiza cambios de versiones cuando hay una necesidad emergente y no preventiva.
- Puede haber cierta resistencia a la implementación de nuevas versiones en los activos tecnológicos de ciertos departamentos o empleados, sobre todo cuando la empresa no tiene una política de actualización de versiones.
- La falta de coordinación de otras áreas puede provocar la resistencia de actualizar las versiones en toda la institución.

Para poder mitigar estos riesgos, la institución debe tener un compromiso con la Gestión de Versiones juntamente con personas responsables y preparas para comunicar al usuario final las ventajas y desventajas del cambio. El control de versiones debería hacerse oportunamente, de acuerdo a como este establecido en las políticas de Gestión de Versiones.

Para poder realizar una Gestión de Versiones correcta se debe entender la clasificación de las versiones según el impacto tecnológico. Encontramos tres clases de versiones:

- **Versiones mayores:** Representan cambios y despliegues relevantes dentro de las herramientas software y hardware insertando modificaciones importantes dentro de la funcionabilidad, usabilidad, técnicas, etc.
- **Versiones menores:** Estas versiones son para la corrección de ciertos errores puntuales de bajo impacto, normalmente son pequeños cambios a implementaciones anteriores.
- **Versiones de emergencia:** Son correcciones a errores de gran impacto, que dan respuesta rápida a errores presentados por la herramienta.

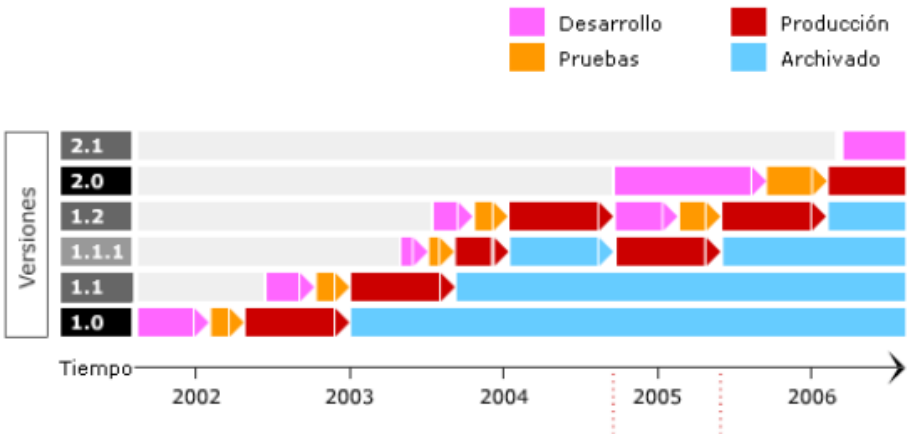
Cada una de estar versiones contiene una referencia para poderlos identificar. El sistema universalmente aprobado es:

- Versiones mayores: 1.0, 2.0, 3.0 etc.
- Versiones menores: 1.1, 1.2, 1.3, etc.
- Versiones de emergencia: 1.1.1, 1.1.2, 1.1.3 etc.

La siguiente figura indica el ciclo de vida de una versión en donde se puede observar los estados en cada fase de desarrollo:

Figura 2.

Ciclo de vida de las versiones



Nota. Tomado *de ITIL: Gestión de Versiones*, por Bravo Campoverde María Eugenia, 2015.

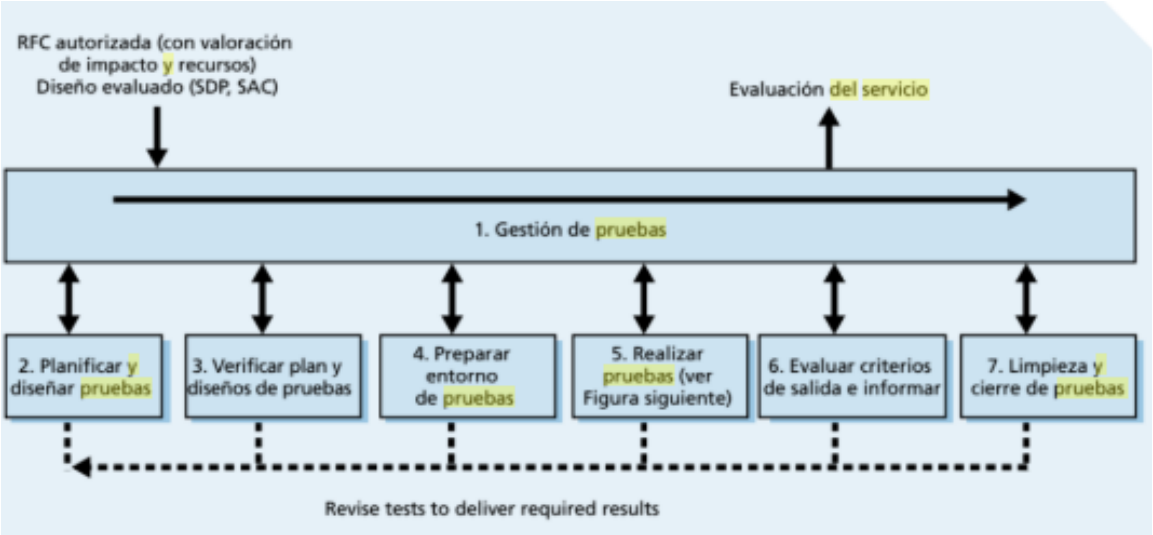
Validación y Pruebas del Servicio. La Validación y Pruebas del Servicio es el que asegura que los servicios tienen lo necesario y cumplan los requisitos establecidos para pasar al ambiente de producción. Este proceso intenta realizar las pruebas pertinentes para dar paso a la implementación y puesta en marcha del servicio.

Los autores (Koltchof et al., 2015) indican que la Validación y Pruebas del Servicio son los test para garantizar que los nuevos servicios o modificaciones están alineados con el propósito y la utilidad prevista en las anteriores fases. El objetivo de Validación y Pruebas de Servicio es realizar pruebas para garantizar que los procesos cuenten con la calidad esperada disminuyendo riesgos, costes y problemas en la línea de producción.

En la siguiente figura observamos los pasos a seguir para realizar una Validación y Pruebas de Servicio exitosa.

Figura 3.

Pasos para la Validación y Pruebas del Servicio



Nota. Tomado de *Gestión de Servicio de TI basada en ITIL V3 Guia de Bolsillo* por Koltchof Axel; Pieper Mike y Tjassing Ruby, 2015, Van Haren Publishing.

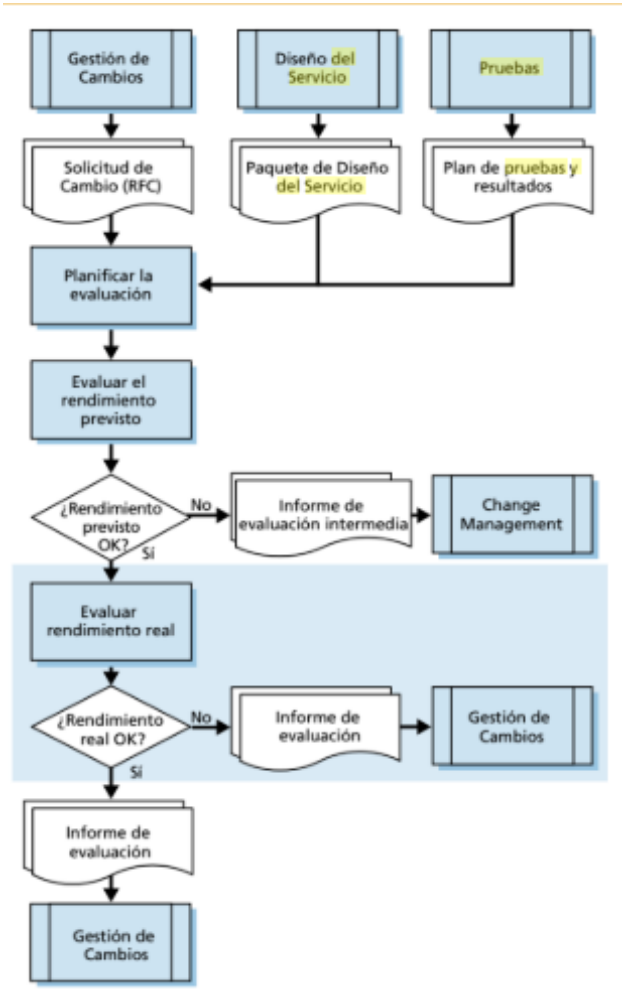
Evaluación. La Evaluación se lleva a cabo con el objetivo de verificar si un servicio está realizando debidamente sus procesos, es decir si tiene un rendimiento aceptable, si su relación costo-beneficio es adecuada o si el servicio lo utilizara la institución.

Según (Ríos, 2014) la Evaluación es la medición de los indicadores de los procesos del servicio, esta información sirve para tener un panorama más completo del servicio y determinar qué aspectos o que procesos son los más válidos para la línea de producción.

La Evaluación permite entender de mejor manera los aspectos que el negocio necesita y también proporciona información para la Mejora Continua del Servicio (CSI). La siguiente figura indica los pasos de la Evaluación:

Figura 4.

Evaluación (Transición del Servicio)



Nota. Tomado de *Gestión de Servicio de TI basada en ITIL V3 Guía de Bolsillo* por Koltchof Axel; Pieper Mike y Tjassing Ruby, 2015, Van Haren Publishing.

Gestión del conocimiento. El objetivo de la Gestión del Conocimiento es entregar información detallada y fiable para la mejora la toma de decisiones que necesite el servicio dentro de su ciclo de vida.

Este intenta recoger, examinar, guardar y compartir información dentro de la

organización. Para compartir la información eficazmente se realiza una SKMS (Sistema de Gestión del Conocimiento del Servicio), la cual debe estar a la mano de las áreas interesadas. La base de datos CMDB trabaja juntamente con la SKMS facilitando información para la mejora del proceso de toma de decisiones.

La diferencia de la SKMS con la CMDB se basa principalmente en que la CMDB trata únicamente de activos tecnológicos, en cambio la SKMS podemos encontrar datos como conocimientos del personal, comportamiento de los usuarios ante algún proceso, rendimiento del servicio, requisitos de los proveedores asociados.

Operación del Servicio

La Operación del Servicio en ITIL es el conjunto de buenas prácticas que permite a la institución garantizar que los servicios implementados se realizan eficaz y eficientemente.

Esta fase intenta gestionar los requisitos y peticiones de los usuarios, dar soluciones a errores que se presenten en el ciclo de vida del servicio, gestionar los problemas y realizar actividades en la línea de producción en contacto con el cliente.

Según (Office of Government Commerce, 2010a) la Operación del Servicio dentro del ciclo de vida del mismo es el responsable de ejecutar los requisitos previos obtenidos en las anteriores fases de ITIL. Como parte de la institución, será el responsable de cumplir y alinear las metas u objetivos de negocio juntamente con la operación del servicio. También es el responsable de gestionar todos los activos tecnológicos para que funcionen de una manera eficaz dentro de todos los procesos.

La Operación del Servicio cuenta con varias sub fases para su correcta implementación:

- Gestión de eventos
- Gestión de Incidencias
- Gestión de peticiones
- Gestión de Problemas
- Gestión de Accesos
- Service Desk
- Gestión de Operaciones TI
- Gestión Técnica
- Gestión de Aplicaciones

Gestión de eventos. Los Eventos son acontecimientos que influencian a los activos tecnológicos o infraestructura TI, es decir los eventos son considerados cambios importantes dentro de un elemento de configuración (CI) o de un servicio.

El objetivo de la Gestión de Eventos es monitorear los CIs de la institución, verificar las licencias vigentes de cada activo tecnológico, monitorear el flujo normal del ciclo de vida del servicio.

El servicio debe identificar cada tipo de evento y el proceso que se llevará a cabo según su importancia. Para un correcto manejo de eventos la institución debe responder las siguientes preguntas:

- ¿Cómo se origina cada evento?
- ¿Cómo se va a clasificar cada evento?
- ¿Cómo se va a comunicar y documentar cada evento?
- ¿Qué datos se va a documentar en cada evento?

- ¿Dónde se guardará los informes de eventos?

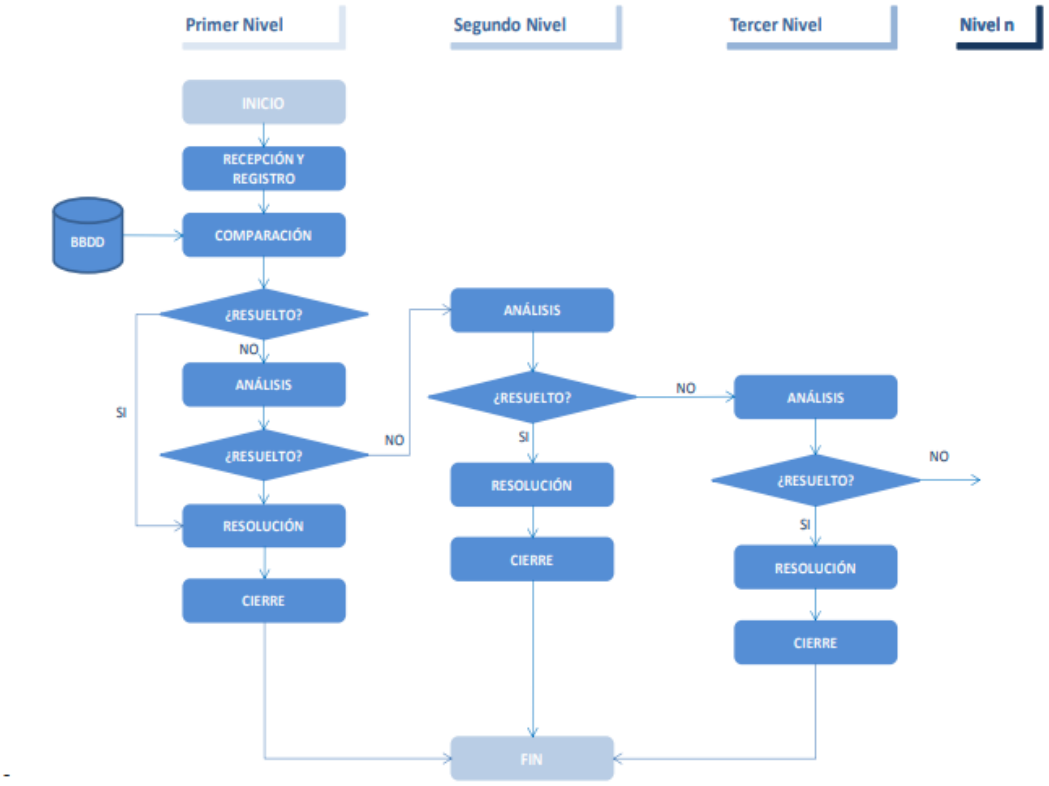
Gestión de Incidencias. La Gestión de Incidencias se basa en la pronta respuesta ante un incidente, intentando mitigar el riesgo y reduciendo el impacto negativo en la institución.

Un incidente de define como un o varios eventos clasificado como emergentes que puede interrumpir los procesos o reducir la calidad del servicio comprometiendo a un proceso en particular o a la institución. La Gestión de Incidentes según (Wikiversity, 2015) puede contener varios subprocesos:

- **Soporte en la gestión de incidentes:** Se refiere a provisión de herramientas, personal, capacidad y guías para un manejo oportuno del incidente.
- **Categorizar Incidente:** Clasificar prioridad o tipo de incidente de acuerdo al impacto.
- **Registro de Incidentes:** Registrar y entregar soluciones de manera eficiente e inmediata.
- **Resolver incidentes (Primera línea):** Resolución de incidente con un límite de tiempo; si la resolución del incidente se excede del tiempo establecido será transferido a la resolución de incidentes de segunda línea.
- **Resolver incidentes (Segunda línea):** Intenta resolver de manera eficiente el incidente. En caso de que se requiera, puede involucrarse personal externo o soporte especial para la resolución del incidente. Si este no es solucionado se escala hasta n niveles. Si el incidente persiste se envía un informe del problema y se transfiere a Gestión de Problemas.

Figura 5.

Escalado para resolución de incidencias



Nota. Tomado de *Manual de ITIL v3 por Ríos Huércano, 2017.*

- **Monitorear el Incidente:** Revisar el estado del incidente después de ser reportado, este debe ser atendido inmediatamente para disminuir el impacto y que no peligre el ciclo de vida del Servicio.
- **Cierre del incidente:** Se refiere a llevar un control de cada incidente informado, garantizando la solución del mismo. Para hacer el cierre del incidente se debe documentar con detalle la solución, esta será útil para resolver de problemas futuros.
- **Informar a los usuarios:** Se debe informar al personal del incidente para

poder realizar ajustes al proceso normal y evitar las interrupciones en el servicio.

Gestión de peticiones. La Gestión de peticiones según (ITIL Foundation, 2015) es el que atiende las necesidades de los usuarios entregando información o atendiendo a las peticiones oportunamente. Las peticiones se refieren a todo tipo de solicitudes que haga el usuario para pedir consejo, información, cambios, acceso a servicios TI.

El objetivo de la Gestión de Peticiones en la institución es:

- Proporcionar accesos rápidos a los servicios de Tecnologías de la Información mejorando la productividad de los servicios en la línea de producción.
- Reducir la burocracia que se puede crear al realizar una petición en los servicios.
- Centraliza el acceso a los servicios.
- Reduce costes de soporte.

Gestión de Problemas. La Gestión de Problemas intenta encontrar las razones del porque se suscita un inconveniente, investigando las posibles causas que repercute en el ciclo normal del servicio para plantear soluciones y garantizar que en un futuro ya no se repitan.

Las funciones de la Gestión de Problemas según (Ríos Huércano, 2017) son las siguientes:

- Reconocer, documentar y analizar los problemas para evitar la repetición de los mismos.

- Dar soluciones ante el problema encontrado.
- Documentar soluciones válidas.
- Proponer cambios en la RFC en el caso de que sea necesario.
- Realizar un seguimiento después de la solución para garantizar el correcto funcionamiento.
- Realizar informes de la condición de la infraestructura TI

La Gestión de Problemas intenta trabajar de dos formas, proactiva y reactivamente, en donde la proactiva se define como el análisis de preventivo a la infraestructura TI mientras que la reactiva se realiza cuando un incidente repetitivo ya se presentó y debe ser solucionado.

Figura 6.

Gestión de un problema

Nota. Tomado de *Proactivanet por* Tecnologías con Clase Mundial, 2016.

Gestión de Accesos. La Gestión de Accesos se refiere a los permisos que se da al personal para manejar cierta infraestructura TI, intentando proteger los activos tecnológicos brindando confidencialidad, integridad y disponibilidad de las herramientas. El objetivo de la Gestión de Accesos es identificar al personal autorizado para manejar cierta infraestructura para garantizar que solo ellos puedan modificarlo o usarlo.

Los propósitos de la Gestión de Accesos son los siguientes:

- Gestionar los accesos al personal basados en políticas definidas por la

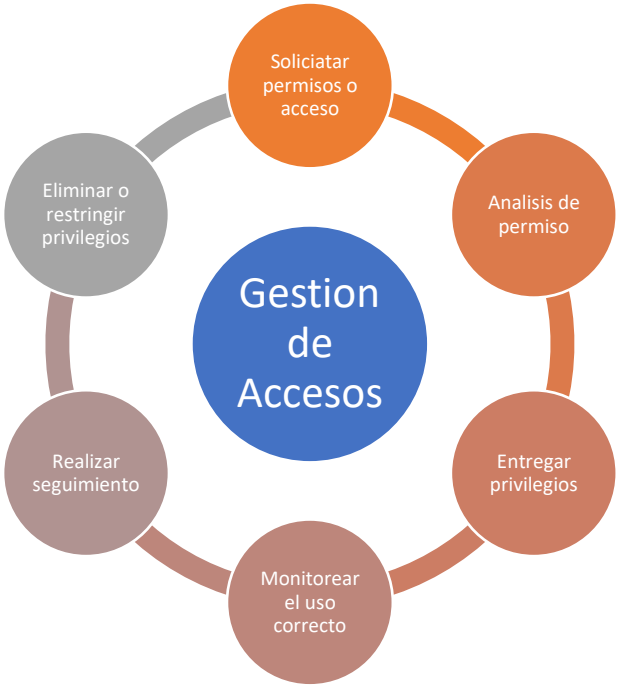
institución.

- Contestar peticiones oportunamente sobre accesos del personal a cierta infraestructura TI
- Gestionar cambios o restricciones de accesos cuando sea necesario.
- Gestionar los distintos niveles de privilegios que tiene cada usuario con la finalidad de proteger la información de la institución.

En la siguiente figura se describe las actividades de la Gestión de Accesos:

Figura 7.

Actividades de Gestión de Accesos



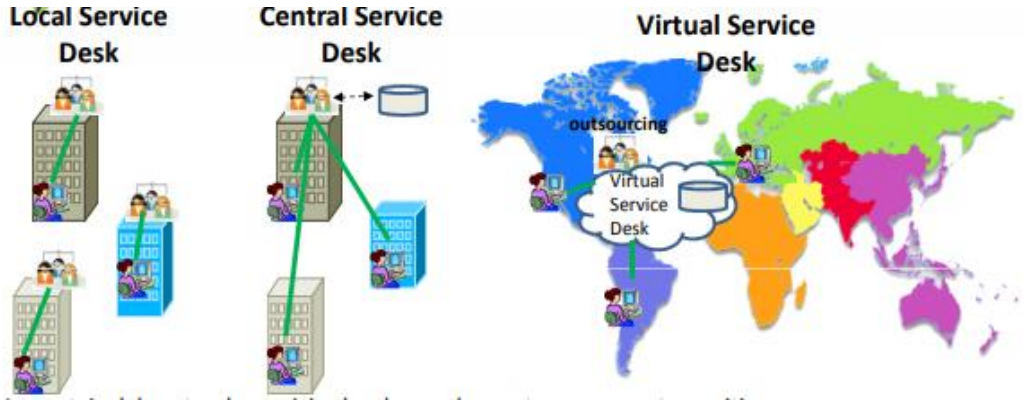
Nota. *Elaboración Propia*

Service Desk. El Service Desk es el punto de ayuda a los usuarios la cual intenta dar servicio, soporte y ayuda a los clientes. El autor (Ríos Huércano, 2017) indica que antes de implementar un Service Desk hay que tomar en cuenta cual es el tipo de servicio y el tipo de organización para que este centro provea realmente un apoyo a la institución. Hay que tomar en cuenta que el Service Desk va muy de la mano con la calidad de servicio y con la satisfacción a los usuarios, es importante realizar un análisis previo a los usuarios y establecer procesos en base a los objetivos de la institución. Si el proceso previo se realiza correctamente, se abre una brecha de satisfacción con los usuarios permitiendo ofrecerles nuevos servicios en un futuro.

En la siguiente figura observamos los distintos tipos de Service Desk que existen:

Figura 8.

Tipos de Service Desk



Nota. Tomado de *Proactivanet* por Tecnologías con Clase Mundial, 2016.

Service Desk Local: Este centro de servicio útil en instituciones o servicios con

necesidad local o pequeños, en donde tienen centralizado su infraestructura TI en un solo lugar.

Service Desk Centralizado: La ventaja de tener un Service Desk Centralizado es gestionar de un mismo luar a varias sedes lo cual significa menos costos, mejor aprovechamiento de recursos, mayor coordinación con todos los procesos TI.

Service Desk Virtual: Este Service Desk se caracteriza por ser la unión de las dos anteriores, es centralizado, pero tiene la ventaja de atender a varias sedes no solamente en la misma localidad sino incluso en varios países.

Gestión de Operaciones TI. La Gestión de Operaciones se define como el monitoreo y el control de los activos tecnológicos, está a cargo de los componentes, soporte, mantenimiento, mejoras etc.

Para los autores (Fernández-Baladrón, 2007) la Gestión de Operaciones se resume en el personal a cargo de que la ejecución de las actividades y procesos del ciclo normal del servicio. Esta fase garantiza que la infraestructura TI funcione correctamente y de forma continua.

Las Gestión de Operaciones como su nombre lo menciona se encarga de la operación del servicio, sus actividades son las siguientes:

- Registro de actividades realizadas en la infraestructura.
- Copias de seguridad y restauración.
- Control y gestión de eventos en la infraestructura de TI
- Hospedar equipos
- Administración de red
- Acceso físico al personal

- Administración de energía.

Gestión Técnica. La Gestión Técnica se refiere a la entrega de recursos necesarios para que el servicio funcione de forma correcta. Esta fase intenta dar soporte y ayuda a los servicios, garantizando el uso correcto de los recursos y entregando las herramientas necesarias para que el servicio funcione de manera óptima.

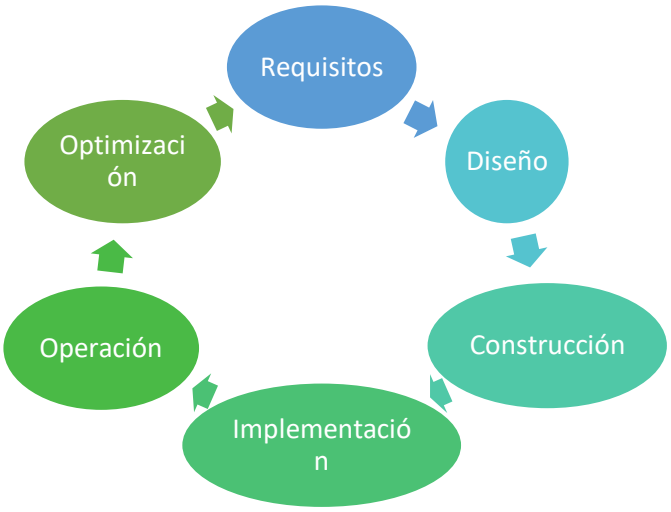
La Gestión Técnica intenta aprovechar los recursos de una manera óptima, por ejemplo, analiza el personal a cargo de ciertos recursos y verifica que la infraestructura se esté utilizando de manera que se aproveche todas sus capacidades.

Gestión de Aplicaciones. La Gestión de Aplicaciones se refiere al control, soporte, mejoramiento, pruebas etc. del software o aplicaciones que necesita el servicio en todo su ciclo de vida.

La Gestión de Aplicaciones tiene el conocimiento técnico del software para poder gestionarlas optimizando los servicios e identificando las mejores herramientas para distribuirlos en toda la organización; también identifica la disponibilidad de las aplicaciones en cada fase del ciclo de vida garantizando que se use adecuadamente la herramienta. Según (Fernández-Baladrón, 2007) la función de la Gestión de Aplicaciones vienen dadas en el siguiente ciclo:

Figura 9.

Funciones de la Gestión de Aplicaciones



Nota. Elaboración Propia

Los objetivos de esta fase son los siguientes:

- Entregar soporte al ciclo de vida del servicio.
- Ayudar en el diseño, transición, operación y mejora.
- Garantizar que los requisitos funcionales sean aptos para las metas de la institución.
- Mantener las aplicaciones en funcionamiento.
- Llevar documentación técnica o manuales para dar una pronta solución ante alguna falla.
- Evaluar el rendimiento del software.
- Desarrollar soluciones.

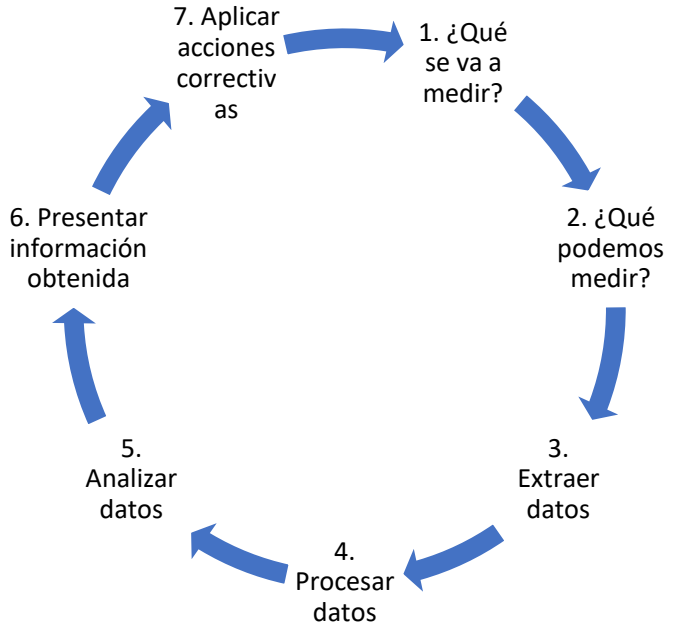
Mejora Continua del Servicio

La Mejora Continua del Servicio pone en marcha una serie de mejoras en el servicio. Cada parte del ciclo de vida y sus procesos son analizados para ser optimizados con el objetivo de tener eficiencia y calidad en fase del servicio.

ITIL menciona siete pasos para la mejora continua las cuales vamos a ver en la siguiente figura:

Figura 10.

Pasos mejora continua del servicio



Nota. Elaboración Propia

- **1. ¿Qué se va a medir?:** En la fase de diseño y estrategia del servicio se debe definir los procesos que se ejecutan siempre.
- **2. ¿Qué podemos medir?:** Se puede medir cada proceso y sus nuevos requisitos, centrándonos en las oportunidades de mejora de calidad, costes, procedimientos, etc.
- **3. Extraer datos:** Extraer datos de nuevos requisitos y compararlos con los objetivos y metas trazadas.
- **4. Procesar datos:** Procesar los datos obtenidos transformándolo a

formatos legibles para el público que requiera la información.

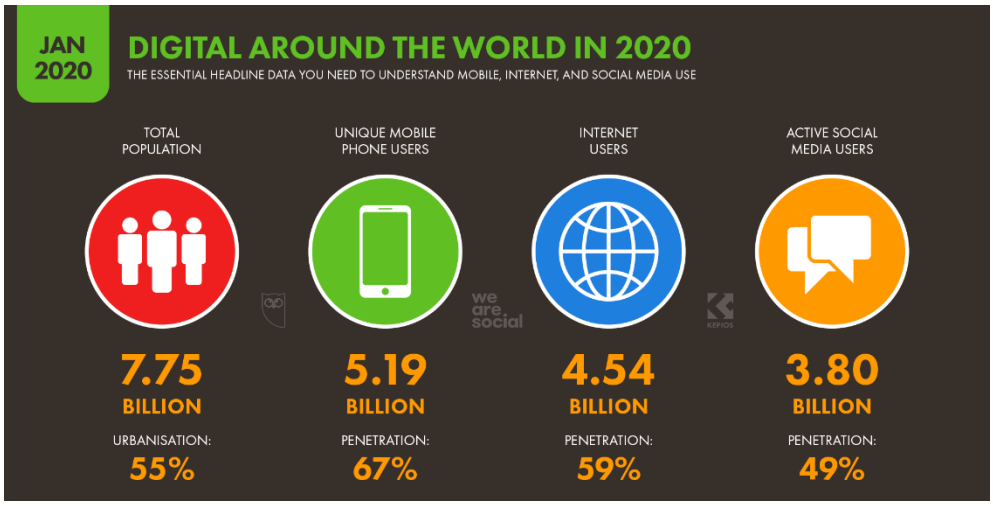
- **5. Analizar datos:** Convertir datos procesados en información y metas a ser cumplidas.
- **6. Presentar información obtenida:** Indicar a todos los interesados las propuestas de mejora.
- **7. Aplicar acciones correctivas:** Poner en marcha los procesos de mejora.

Seguridad de la Información

La red de comunicación interconectados entre sí (internet) se ha hecho parte fundamental del uso cotidiano de todas las personas. Según (Kemp, 2020) en su reporte digital del 2020 nos cuenta que más de 4.5 billones de personas usan internet, donde 3.8 billones de estas usan redes sociales, es decir alrededor del 70% de la población mundial. Según (Kemp, 2020) el crecimiento del uso del internet tomando en cuenta al del año pasado, es de 4.54 mil millones, es decir un aumento del 7%. En cuestión de las redes sociales, esta ha crecido un 9% desde el año pasado y finalmente el uso de dispositivos móviles ha crecido a 5.19 billones de usuarios en el presente año.

Figura 11.

Datos del uso del Internet año 2020

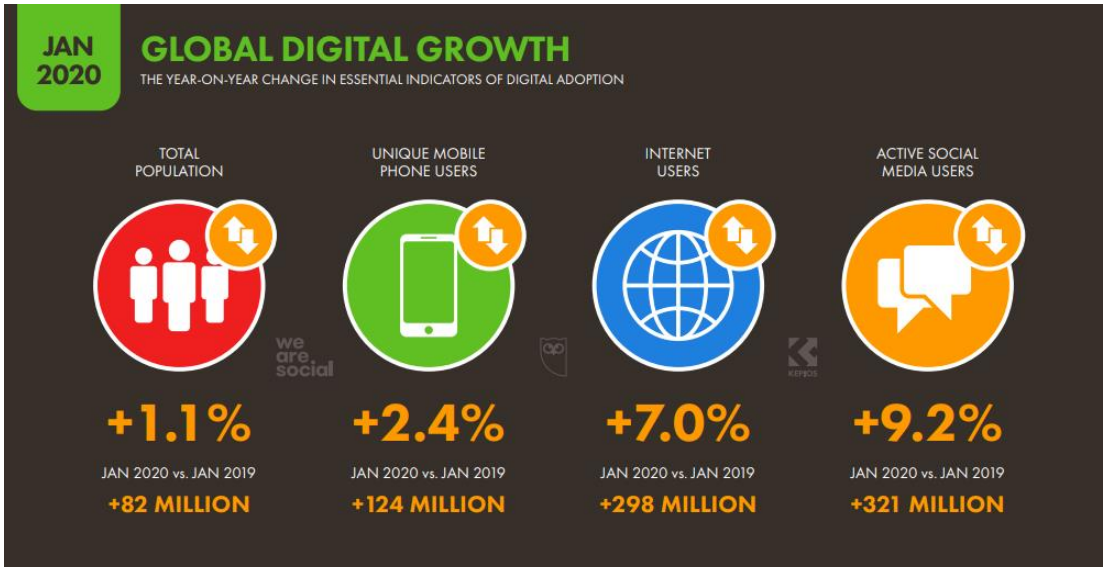


Nota. Tomado de *We Are Social* por Kemp Simon, 2020

A continuación, observaremos el crecimiento de internet en base a enero del 2019.

Figura 12.

Crecimiento del internet en base a enero del 2019



Nota. Tomado de *We Are Social* por Kemp Simon, 2020.

Como podemos observar el mundo tiende al crecimiento en el uso del internet, estamos en una era digital en la cual la mayoría de los dispositivos cuentan con una

conexión a internet. En el caso de Ecuador según un estudio que hizo (Kemp, 2020) 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 13.

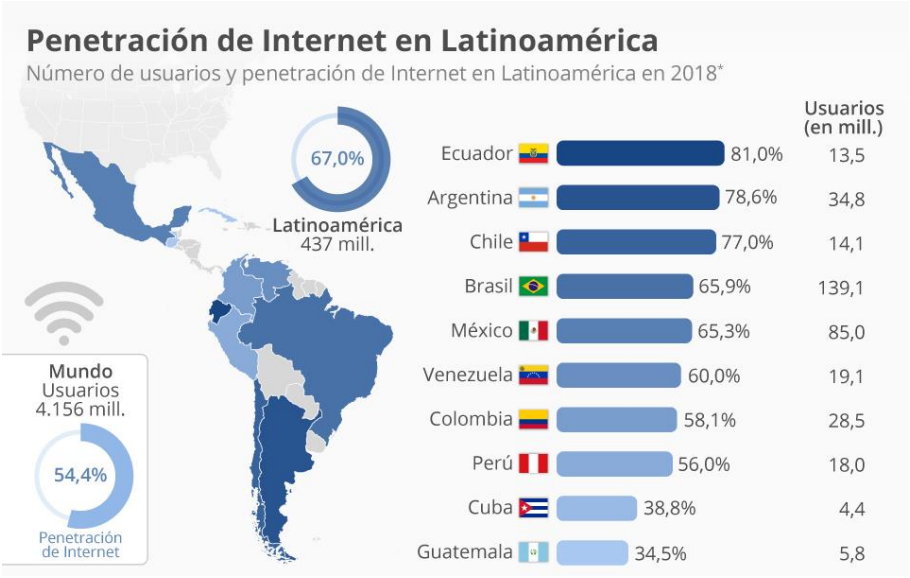
Uso de internet en Ecuador

Nota. Tomado de *We Are Social* por Kemp Simon, 2020.

Según cifras de (Internet World Stats, 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 14.

Penetración de Internet en Latinoamérica



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

En referencia a la figura, podemos observar que el internet se ha hecho 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 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.

(Cisco Networking Academy, 2020) 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 conjunto de procesos o herramientas que tienen como objetivo la protección de la información, tomando en cuenta que la seguridad informática es un proceso en la cual participan diversas personas, sistemas, herramientas, etc, tratando de crear conciencia de su importancia antes de alguna amenaza critica.

Importancia de los Datos

(Cisco Networking Academy, 2020) intenta concientizar la protección de los datos dando a entender la exposición de los usuarios al registrar gran cantidad de información en línea. La pregunta que sugieren es, ¿Dónde están los datos del usuario? Hay que recordar que las personas al usar internet dejan gran cantidad de datos solo al dar un clic en alguna página web. Incluso hay páginas web que piden información personal como nombre, correo electrónico, numero celular, etc, o instituciones que cuentan con información de seguros, cuentas bancarias, fotos, tarjetas de crédito, etc del usuario. Es decir, vivimos en un mundo globalizado que tiene nuestros datos sin tener la certeza de que están seguros en línea.

Los instrumentos electrónicos actualmente también entran a la lista de dispositivos en internet, recordemos que ahora son llamados dispositivos inteligentes. La información no solo se almacena en el computador o un smartphone, si no que existe actualmente una tecnología llamada (IoT) o Internet de las Cosas, la cual es definida como una serie de tecnologías o sensores conectados entre sí a varios dispositivos electrónicos con la capacidad de conectarse a internet para el envío y recepción de datos.

En conclusión, los datos son importantes no solamente para una organización si no para los usuarios comunes, ahora estamos en una era digital donde nuestra vida común ha cambiado para dar acceso a las facilidades que nos brinda el internet. Las empresas o servicios deben estar conscientes de la importancia de los datos; hay que entender que si una empresa levanta un servicio TI es muy importante entregar garantías para que el cliente se sienta seguro al realizar todas sus actividades en la infraestructura TI que la institución levante.

Análisis de un ciberataque

Un ciberataque se refiere a los métodos que usa un atacante cibernético para aprovechar brechas de seguridad digital y obtener algún beneficio como robo de dinero, suplantación de identidad, espionaje, robo de datos, inhabilitar servidores, robo de contraseñas, etc. Los ciberataques pueden estar dirigidos a usuarios comunes, servidores o sistemas de red para dañar las instituciones, personas o gobiernos.

Los atacantes son personas con cierto conocimiento que intentan aprovechar vulnerabilidades de algún sistema para conseguir un beneficio. Según (Cisco Networking Academy, 2020) los atacantes se pueden clasificar de la siguiente manera:

- **Aficionados (Script Kiddies):** Son los que tienen poco o nada de conocimientos sobre ataques cibernéticos, pero utilizan instrumentos que encuentran en el internet para realizar algún daño. Puede que instrumentos básicos, pero aun así pueden ser letales para una organización.
- **Hackers:** Los hackers se caracterizan por tener los conocimientos necesarios para vulnerar algún sistema y tener accesos. Este tipo de atacantes se dividen en tres según la intención del atacante, ya que no todos los hackers vulneran sistemas por un interés malvado.

  - **Hackers de Sombrero Blanco:** Se caracterizan por tener la autorización para vulnerar redes y ver sus debilidades con la intención de encontrar problemas y solucionarlos, mejorando la seguridad en la institución.
  - **Hackers de Sombrero Gris:** Se caracterizan por encontrar vulnerabilidades, pero no aprovecharlas, es decir no realizan la acción maliciosa, pero pueden publicar en internet las fallas de dicho sistema para que otros hackers la aprovechen.
  - **Hackers de Sombrero Negro:** Se caracterizan por usar sus conocimientos para realizar acciones mal intencionadas al vulnerar sistemas. Este tipo de atacante tienen la intención de aprovechar las vulnerabilidades para beneficio propio o de una organización.

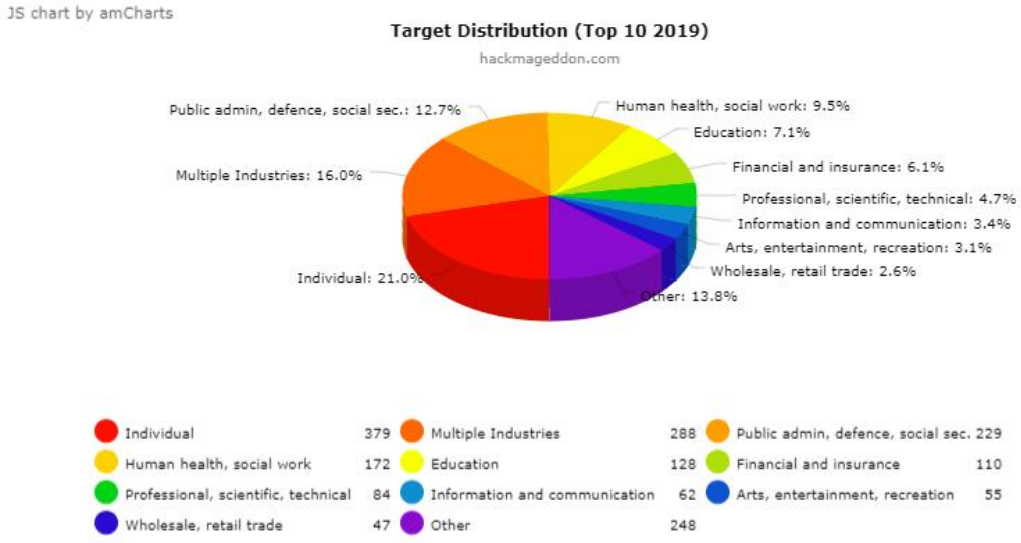
- **Hackers organizados:** Este tipo de atacantes se caracteriza por ser una organización de delincuentes cibernéticos con un mismo interés. Estos pueden ser divididos de la siguiente manera:
  - **Ciberterroristas:** Son atacantes cuyo interés es desestabilizar un país, suelen afectar servicios básicos, comunicaciones, infraestructura, etc.
  - **Hacktivistas:** Son atacantes cuyo interés es político o social, este tipo de delincuentes intentan concienciar sobre problemas que son de interés de ellos. Es común que realicen ataques en nombre de una posición social que ellos defienden.
  - **Hackers patrocinados por un gobierno:** Este tipo de atacantes se caracteriza por estar altamente equipados y financiados por un estado que intenta realizar ataques que beneficien a su propio

gobierno.

El autor (Hackmageddon & Passeri, 2020) indica estadísticas mundiales sobre los ataques cibernéticos mes a mes, en donde al finalizar el 2019 las estadísticas de a quien fue dirigidos los ataques quedaron de la siguiente forma (ver Figura 15):

Figura 15.

Distribución objetivo de ataques en 2019



Nota. Tomado de *Hackmageddon* por Passeri Paolo, 2020.

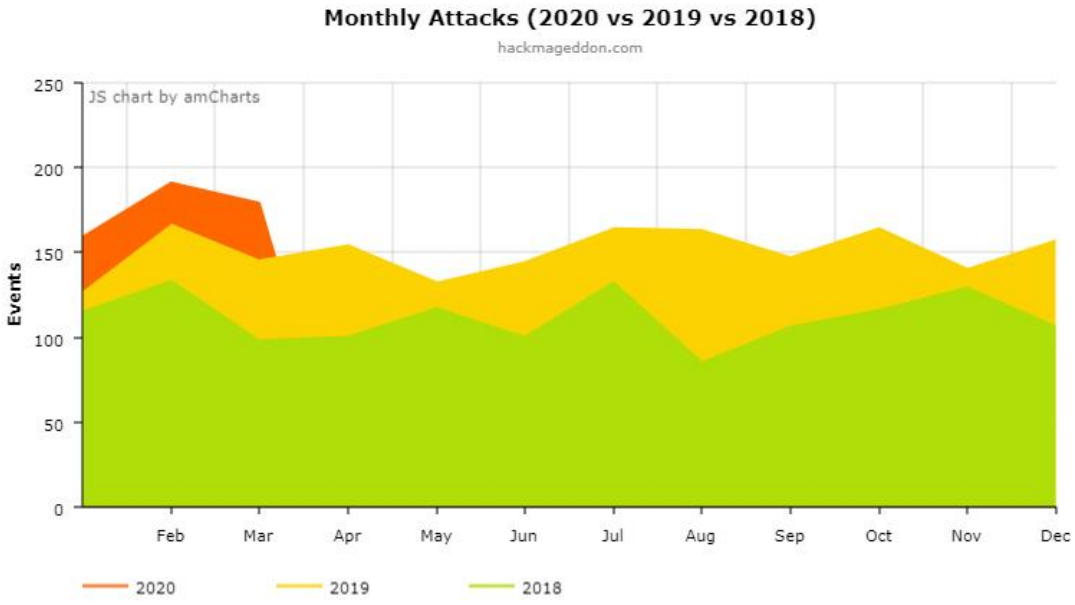
Como podemos observar, para el año 2019 los sectores de Educación (7.1%) y Profesional, Científico, Técnico (4.7%) suman un total 11.8% de ataques, los cuales significan que de 100 ataques 12 son dirigidos a estos sectores. La Universidad de las Fuerzas Armadas ESPE al ser una institución educativa y profesional entraría en los sectores descritos anteriormente lo cual significa un gran riesgo para la institución ya que no se cuenta con un grupo de seguridad informática propiamente establecido.

En lo que va del año 2020 los ataques se han elevado en comparación a los

años anteriores, significa que conforme el mundo se va digitalizando, la seguridad de la información es mucho más importante ya que cada día aparecen más sistemas y dispositivos que deben ser protegidos. La siguiente figura describe el crecimiento de ataques hasta marzo del 2020 comparándolos con dos años anteriores:

Figura 16.

Ataques mensuales 2020 vs 2019 vs 2018

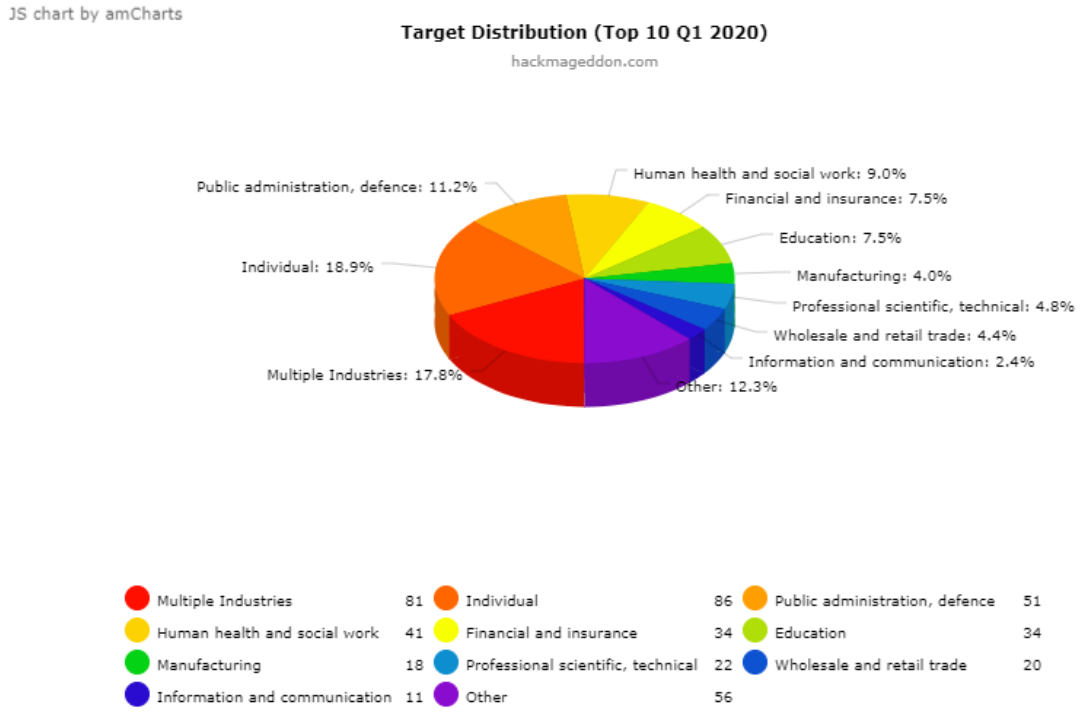


Nota. Tomado de *Hackmageddon* por Passeri Paolo, 2020.

En la Figura 16 se observa un aumento considerable de ataques cibernéticos a lo que va de marzo del 2020; las estadísticas por distribución de objetivo también han cambiado, en donde el sector de Educación y Profesional, Científico, Técnico han aumentado dejando en claro que hay que focalizar los esfuerzos en tener un equipo de Seguridad de la Información que permita disminuir los riesgos de ataques cibernéticos (Ver Figura 17).

Figura 17.

Distribución Objetivo de ataques hasta marzo de 2020



Nota. Tomado de *Hackmageddon* por Passeri Paolo, 2020.

Vulnerabilidades de Seguridad

Las vulnerabilidades de Seguridad ser refieren a todo tipo de fallo o error en el software o hardware que usuarios malintencionados intentar aprovechar para explotarla. El aprovechamiento de estas vulnerabilidades se conoce como ataque y este intenta tener acceso no autorizado a recursos específicos. Hay dos tipos de vulnerabilidades:

- **Vulnerabilidad de software:** Se refieren a los errores en las aplicaciones o sistemas operativos en donde las empresas tratan de corregirlos por medio de actualizaciones o nuevas versiones.

- **Vulnerabilidad de hardware:** Estas se refieren a errores de diseño en el hardware, por ejemplo, fallas en la memoria RAM, fallas en procesadores, etc.

Las vulnerabilidades se pueden explotar con varias técnicas, una de ellas son el uso de Malware que significa (Malicious Software). Este tipo de software es un código que aprovecha las vulnerabilidades de un sistema y puede robar, espiar, conceder accesos, etc. Los tipos más comunes de malware según (Cisco Networking Academy, 2019) son los siguientes:

- **Spyware:** Diseñado para espiar, rastrear actividades o conocer la ubicación del usuario, por lo general este tipo de malware contiene keylogger que son un tipo de spyware de captura de pulsaciones de teclado.
- **Adware:** Diseñado para entregar al usuario publicidad automáticamente, este malware intenta invadir al usuario con publicidad no deseada. Es común que este tipo de malware venga también con un spyware.
- **Bot:** Este malware se caracteriza por ser silencioso; al ser una especie de robot, esta espera realizar acciones automáticas o también ordenadas por el atacante.
- **Ransomware:** Este tipo de malware secuestra al computador de la víctima cifrando la información del disco duro. Para liberar la información el atacante pide cierta cantidad de dinero para quitar el cifrado a los archivos. Algunas versiones de ransomware tienen la capacidad de bloquear al sistema operativo entero.
- **Scareware:** Este tipo de malware intenta persuadir al usuario mediante el miedo, es decir falsifica que el computador está en riesgo o que puede perder información si no instala software específico (la realidad es que el

equipo no está en riesgo). El usuario al ser persuadido puede instalar el software malicioso que perjudique aún más su computador.

- **Rootkit:** El Rootkit es un tipo de malware que tiene la capacidad de escalar privilegios, dando la oportunidad al atacante que entre remotamente al computador. Este tipo de malware explota vulnerabilidades en los Sistemas Operativos y crea puertas traseras para su acceso. Este tipo de malware es muy difícil de controlarlo ya que escaló toda la seguridad del sistema.
- **Virus:** El virus se refiere a un código malicioso con líneas de comando que puede ejecutar el sistema. En su mayoría estos códigos necesitan ser ejecutados por el usuario. Los virus pueden ser inofensivos como presentar solamente cuadros de dialogo o tan peligrosos como borrar datos o dañar sistemas.
- **Gusanos:** Los gusanos son códigos que tienen la capacidad de clonarse o replicarse en una red, es decir tiene la capacidad de pasar de computador en computador automáticamente, infectando a toda la organización. Este tipo de malware tiene como característica principal que no necesita la activación del usuario para ejecutarse, si no que puede infectar a la red con códigos automáticos de propagación y activación.
- **Troyano:** El Troyano engaña al usuario haciéndose pasar por un software legítimo, es decir, el usuario accede a instalar o descargar cierto archivo pensando que es el correcto, sin darse cuenta que al interior contiene códigos maliciosos que perjudica el funcionamiento del computador.
- **MitM:** también llamado Hombre en el Medio, este tipo de malware se coloca en la red interceptando la información del usuario cuando quiere acceder a cualquier sitio web. Este tipo de ataque es más común para robar

información bancaria, credenciales, etc.

Tipos de ataques

Conociendo los tipos de malware, los atacantes han inventado varios métodos o estrategias para que los sistemas sean vulnerados o que los usuarios caigan en dichas tácticas para comprometer su seguridad. Hay que tomar en cuenta que no todos los métodos son iguales, pero existen algunos tipos de ataques conocidos que los criminales intentan sacar provecho.

- **Ingeniería Social:** Intentan manipular al usuario con información falsa para que realicen actividades o divulguen información. Un ejemplo muy común es cuando al usuario le llega un correo expresando que ganó la lotería; el usuario es engañado y accede a entregar sus datos bancarios, o a realizar pagos para que se realice el canje de su premio.
- **Fuerza Bruta:** El atacante para ingresar a las cuentas de la víctima usa combinaciones de datos o dígitos hasta dar con la contraseña del usuario. Hay que tomar en cuenta que las computadoras pueden procesar estas combinaciones de manera rápida, disminuyendo el tiempo para encontrar las claves de acceso.
- **Phishing:** Se refiere a cuando el atacante toma la identidad de una red social, entidad bancaria, escuelas, páginas del gobierno, etc, para encaminar al usuario a paginas falsas o entregue información privada. Un ejemplo es cuando llega correos falsos haciéndose pasar por una red social, el atacante le pide al usuario que ingrese a una página fraudulenta en donde será víctima de robo de información. La probabilidad que el usuario caiga en la trampa es alta ya que las paginas fraudulentas son exactamente igual a

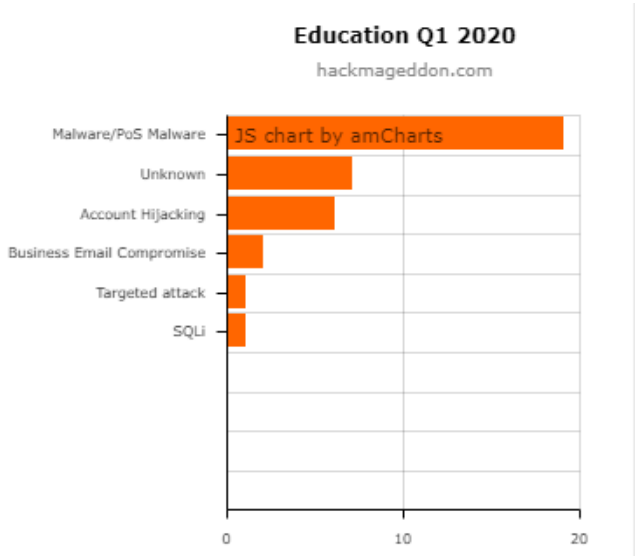
las oficiales.

- **Inyección SQL:** Este tipo de ataque es insertar un código malicioso a un servidor de base de datos, en donde el atacante inyecta un código que le permite robar datos e información.
- **DoS:** El atacante envía una cantidad abrumadora de tráfico a los servidores con el objetivo de interrumpir el servicio y dejar sin servicio a las instituciones.
- **DDoS:** El DDoS es una variable del ataque DoS, este ataque se realiza con la ayuda de botnets, las cuales mandan tráfico a un mismo servidor desde varias localidades, a diferencia del DoS que se envía de una sola localidad. Una botnet es una serie de bots infectados en varias partes del mundo y controladas por el mismo atacante.
- **Envenamiento SEO:** Este ataque se realiza a los motores de búsqueda como google, en donde el atacante posiciona una página web maliciosa en los primeros lugares de búsqueda.

Conociendo los tipos de ataques, el delincuente puede aprovechar de estas técnicas para vulnerar algún sistema; hay que recordar que puede realizar ataques combinados para lograr su objetivo. En las figuras siguientes observaremos las técnicas y motivación de los atacantes para vulnerar una institución educativa hasta marzo del 2020:

Figura 18.

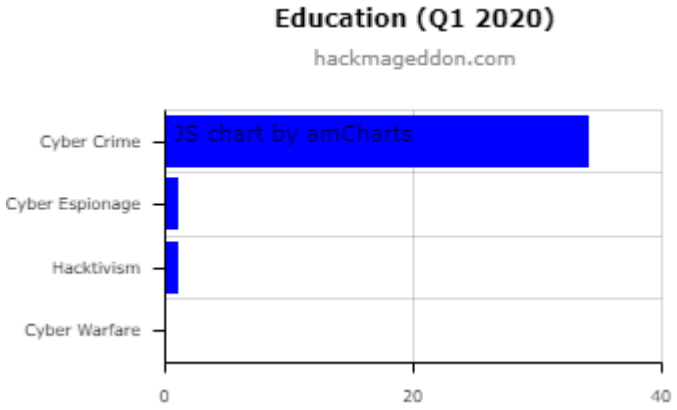
Desglose de técnicas de ataque para el sector educativo



Nota. Tomado de *Hackmageddon p*or Passeri Paolo, 2020.

Figura 19.

Desglose de motivaciones para el sector educativo



Nota. Tomado de *Hackmageddon* por Passeri Paolo, 2020.

Proceso de ataque

En ciberseguridad existe un término llamado la Cadena de Eliminación o Kill Chain, que indica la serie de pasos que sigue un atacante para vulnerar algún sistema. La cadena de eliminación tiene los siguientes pasos:

- **Etapa 1. Reconocer:** Estudia el objetivo y su infraestructura, puede utilizar escaneo de puertos, whois, información de contacto, etc.
- **Etapa 2. Preparar:** Crea el ataque perfecto para su objetivo, este ataque puede ser combinado con varios métodos.
- **Etapa 3. Distribuir:** Envía el ataque o el malware por diferentes métodos.
- Etapa 4. Explotación: Se ejecuta el ataque.
- **Etapa 5. Instalación:** Se ejecuta el malware o las estrategias enviadas instalando puertas traseras dentro de la infraestructura TI del objetivo.
- **Etapa 6. Mando y Control:** Se toma el control de la infraestructura de la víctima.
- **Etapa 7. Acción sobre la víctima:** En este punto el atacante ya tiene el control. Aquí roba información, instala malware, infecta nuevos dispositivos, etc.

Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT)

El continuo crecimiento de la infraestructura TI en todo el mundo y el aumento de incidentes de seguridad informática han sido razón para que las empresas y usuarios pongan más empeño en el cuidado de sus dispositivos ante un ataque informático. Gracias a esta necesidad nacen los CSIRT, por sus siglas en inglés “Computer Security Incident Response Team”, aunque internacionalmente también es conocido como CERT.

Descripción conceptual

Según (Enisa, 2006), el nacimiento de los CERT (Computer Emergency Response Team) fue en los años ochenta cuando la infraestructura mundial fue

comprometida por un gusano llamado Morris, el cual se propago rápidamente infectado varios sistemas en el mundo. Este incidente abrió la brecha para que varios administradores tomen importancia a los incidentes de seguridad informática y creen algún tipo de solución que les permita cooperar entre varias instituciones con el fin de enfrentar este tipo de ataques.

Cuando hablamos de un CERT hablamos también de un CSIRT, la diferencia es que el término CERT es una marca registrada. Varias instituciones han optado por llamar a su Equipo de Seguridad Informática CSIRT, siendo este un término genérico que pueden utilizar sin ningún tipo de restricción. Otros tipos de términos usados son los de IRT (Incident Response Team), CIRT (Computer Incident Response Team), SERT (Security Emergency Response Team). En el presente proyecto tomaremos el nombre de CSIRT ya que es el más común en todo el mundo y esto permite una mejor comprensión de los servicios que prestara a la institución.

Un CSIRT es un equipo de profesionales que responden con una solución ante incidentes de seguridad informática dentro de una institución, permitiendo también la colaboración con otros centros de cualquier localidad. Los CSIRT se ocupan de los incidentes y ayuda a los usuarios a recuperarse ante una alguna falla y los capacita para que en el futuro tengan mejores prácticas en el uso de la infraestructura TI.

Los autores (Ron Egas et al., 2017) describen a un CSIRT como un Equipo de Respuesta a Incidentes de Seguridad Informática responsable de prevenir, reconocer y dar solución a incidentes informáticos. Los CSIRT cuenta con varios servicios según la necesidad de la institución, pero el más importante es el ayudar en la mitigación de riesgos relacionados con ataques de la infraestructura TI y dar soporte oportuno para proteger los mismos. En resumen, los CSIRT gestionan los incidentes de seguridad de

la información protegiendo a la comunidad a la que se brinda el servicio y planifica estrategias para recuperarse en el caso de que un incidente ya haya afectado a la organización.

Las funciones de un CSIRT según (Enisa, 2006) son las siguientes:

- Centralizar las soluciones en cuanto a seguridad de la información se refiere dentro de la institución.
- Analizar los incidentes y gestionarlos en un área centralizada, esto permite tener una mejor coordinación y documentación de los incidentes dentro de la empresa.
- Definir el proceso a llevar a cabo para gestionar incidentes.
- Dar servicios de seguridad de la información a la institución.
- Manejo correcto de la información ante algún evento perjudicial.
- Investigar soluciones ante algún incidente.
- Dar soluciones para que la institución se recupere de un incidente.
- Tener los conocimientos técnicos necesarios para dar soporte a los usuarios afectados.
- Hacer un seguimiento de los incidentes presentados.
- Fomentar la cooperación con otros centros nacionales e internacionales.

Para la implementación de un CSIRT hay que tomar en cuenta el tipo de institución y cuál es su forma de negocio; al tener un CSIRT varios servicios es importante analizar las necesidades y los objetivos de la institución para entender de forma clara la necesidad de los clientes y de qué forma se enfocará los servicios. Hay

varios tipos de CSIRT según los sectores de negocio:

- **CSIRT Académico:** CSIRT que brinda servicios a una comunidad estudiantil, los clientes son los alumnos, profesores y personal administrativo.
- **CSIRT Comercial:** Este tipo de CSIRT son por contratación, es decir los clientes compran el servicio para su organización. Este tipo de CSIRT llega a acuerdos con el cliente para dar servicios específicos según el tipo de institución.
- **CSIRT Militar:** Este CSIRT presta servicios a instituciones militares y otras entidades que estén relacionadas con esta, entregando protección a la infraestructura TI diseñadas con fines de defensa.
- **CSIRT Nacional:** Este CSIRT tiene como beneficiarios a todo el país ya que puede coordinar todos los sectores del mismo. Este tipo de centro funciona más como el punto de contacto y coordinación con otros CSIRT de la misma localidad.
- **CSIRT para pequeña y media empresa (PYME):** Ya que el tamaño de estas empresas no es grande, este tipo de CSIRT es la unión de varias organizaciones con la intención de trabajar en conjunto y dar soporte a todas las organizaciones.
- **CSIRT Gubernamental:** Este tipo de CSIRT tiene la característica de ser financiados por el estado para la protección de su gobierno, este tipo de CSIRT suele tener como clientes a varios organismos y administraciones públicas.
- **CSIRT de Soporte:** Este tipo de CSIRT se centra en dar soporte a

productos específicos. Al igual que un CSIRT Nacional, este coordina y resuelve posibles fallos en los sectores que cuenten son sus productos.

- **CSIRT Internos:** Entregan servicios a su propia organización.

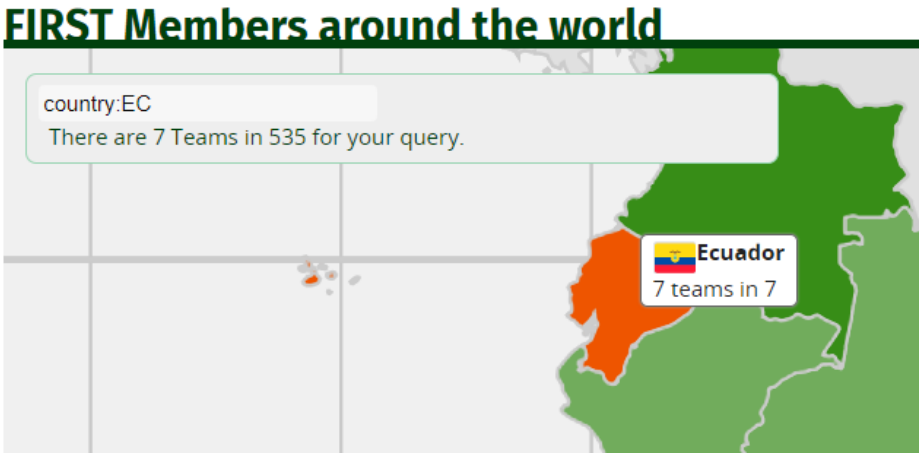
FIRST

FIRST por sus siglas en ingles significa (Forum for Incident Response and Security Teams) la cual tiene como objetivo el fomentar la comunicación y cooperación de varios centros certificados por ellos y crear una comunidad activa entre varias localidades. La visión que tiene (FIRST, 2018) es reunir a varios equipos de respuesta ante incidentes de seguridad en todas las localidades del mundo para garantizar el uso del internet seguro para todo usuario.

Actualmente FIRST tiene 535 equipos en 96 países diferentes. La ventaja de pertenecer a FIRST es la cooperación entre todos los equipos que son miembros, fomentando el aprendizaje y eficiencia a la hora de detectar algún incidente. Según la página oficial de (FIRST, 2018), actualmente en Ecuador existe siete Equipos miembros:

Figura 20.

Equipos miembros de FIRST en Ecuador



Fuente: (FIRST, 2020)

Nota. Tomado de *First Improving Security Together* por FIRST, 2020.

- BLUE HAT CERT (Blue Hat Cyber Security Incident Response Team),
- CERT Radical (CERT RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA. LTDA.),
- CSIRT Telconet (Centro de Respuesta a Incidentes de Ciberseguridad de Telconet),
- CSIRT-CEDIA (CSIRT-CEDIA),
- CSIRT-EPN (CSIRT-EPN),
- EcuCERT (Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones),
- MAINTLATAM CSIRT (MAINTLATAM CSIRT).

Los beneficios de ser miembros de FIRST son los siguientes:

- Cuenta con un foro para comunicarse con otros equipos de seguridad en todo el mundo.
- FIRST realiza una conferencia anual sobre incidentes de seguridad informática, esta conferencia es reconocida mundialmente ya que incluye investigación actual sobre cómo responder y prevenir incidentes.
- Se comparte coloquios técnicos con información como vulnerabilidades, software y hardware, técnicas, incidentes entre otros.
- Se benefician con herramientas técnicas como Malware Information Sharin Plataform que es un servicio web de intercambio de información.

Servicios de un CSIRT.

Según la (Organización de los Estados Americanos, 2016) en su informe de Buenas Prácticas para Establecer un CSIRT nacional, señala que los servicios de un CSIRT se pueden diferenciar en tres grupos: reactivos, proactivos y de valor agregado los cuales se definen de la siguiente manera:

- **Servicios reactivos:** Estos son los servicios más importantes dentro de un CSIRT de cualquier organización, estos se encargan de responder activamente los incidentes, eventos o requerimientos de seguridad que se presentan en el momento.
- **Servicios Proactivos:** Se refiere a la prevención de incidentes, este servicio intenta cuidar a la institución y su infraestructura TI con información e investigación que ayude a anticiparse a los ataques futuros.
- **Servicios de valor agregado:** Este tipo de servicio se basa más en el mejoramiento de la calidad que se brinda como CSIRT.

En la siguiente tabla observamos los sub-servicios que tiene cada literal descrito anteriormente:

Tabla 3.

Servicios de un CSIRT

Servicios reactivos	Servicios proactivos	Manejo de instancias
• **Alertas y advertencias** • **Tratamiento de incidentes** • **Análisis de incidentes** • **Apoyo a la respuesta a incidentes** • **Coordinación de la respuesta a incidentes** • Respuesta a incidentes *in situ* • Tratamiento de la vulnerabilidad • Análisis de la vulnerabilidad • Respuesta a la vulnerabilidad • Coordinación de la respuesta a la vulnerabilidad	• Comunicados • Observatorio de tecnología • Evaluaciones o auditorías de la seguridad • Configuración y mantenimiento de la seguridad • Desarrollo de herramientas de seguridad • Servicios de detección de intrusos • Difusión de información relacionada con la seguridad	• *Análisis de instancias* • *Respuesta a las instancias* • *Coordinación de la respuesta a las instancias* ***Gestión de la calidad de la seguridad*** • *Análisis de riesgos* • *Continuidad del negocio y recuperación tras un desastre* • *Consultoría de seguridad* • *Sensibilización* • *Educación / Formación* • *Evaluación o certificación de productos*

Nota. Tomado de *Cómo crear un CSIRT paso a paso* por Enisa, 2006

Cabe recalcar que los servicios de un CSIRT van a depender de la organización, ya que hasta la fecha no existe un CSIRT que provea todos los servicios descritos anteriormente. Cada servicio se acopla a las metas y objetivos trazados por la institución, aunque para ser considerado un CSIRT los servicios básicos que deben ser los siguientes:

- Alertas y advertencias,
- Tratamiento de incidentes,
- Análisis de incidentes,
- Apoyo en la respuesta de incidentes,
- Coordinación de la respuesta a incidentes.

Metodología de implementación

La metodología de implementación para el presente proyecto se da con la ayuda del marco de referencia de ITIL v3 descrita anteriormente, ya que tiene una estructura

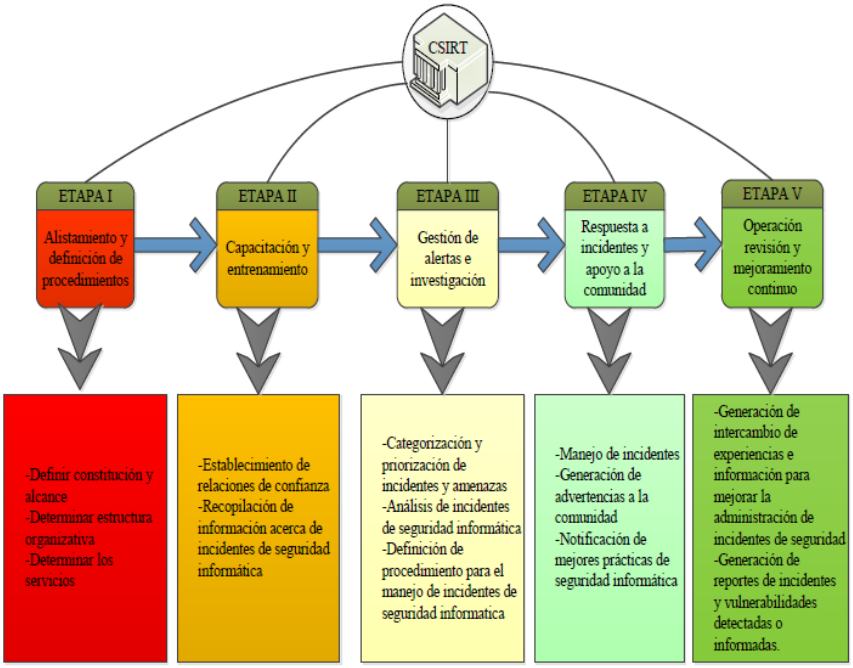
lógica que permite levantar procesos y servicios de manera ordenada y optima, también cuenta con flexibilidad, información, niveles de servicio, adaptabilidad y manejo correcto de incidentes.

También para la implementación se tomará en cuenta la metodología propuesta por (Andrade et al., 2012) diseñada para le Universidad de las Fuerzas Armadas ESPE, en donde cuenta con cinco etapas:

- Etapa 1. Alistamiento y definición de procedimientos.
- Etapa 2. Capacitación y entrenamiento.
- Etapa 3. Gestión de alertas e investigación.
- Etapa 4. Respuesta a incidentes y apoyo a la comunidad.
- Etapa 5. Operación, revisión y mejoramiento continuo.

Figura 21.

Etapas para la implementación de un CSIRT



Nota. Tomado de *Diseño y dimensionamiento de un equipo de un equipo de respuesta ante incidentes de seguridad informática (CSIRT). Caso de estudio: ESPE* por Andrade Roberto; Fuertes Walter, 2013.

Herramientas de monitoreo de red

Actualmente existen varias herramientas que ayudan a evaluar, informar, gestionar, monitorear y explotar vulnerabilidades para verificar que la infraestructura TI de nuestra institución esté debidamente protegida. Existen herramientas gratuitas y de paga que ofrecen varias funcionalidades según la actividad que se realice. Cabe recalcar que para escoger una herramienta se debe poseer conocimientos del negocio para escogerlas según sea la necesidad de la institución.

Para realizar una correcta decisión de herramientas, estas deben tener ciertas características que ayudaran en la instalación y puesta en marcha del servicio, las características son listadas a continuación:

- **Visibilidad:** La herramienta debe contar con el sustento correspondiente mediante informes generados por su proveedor o usuarios a fin de que la herramienta sea entendible para los usuarios. Hay que evitar herramientas que ocultan características o información con fines de marketing.
- **Extensibilidad:** La herramienta debe ser capaz de adaptarse a la organización y a sus procesos, esta debe tener la característica de poderse personalizar según sea la necesidad de la institución. Por ejemplo, que permita personalizar reglas, adaptar plugins, cambiar configuraciones etc.
- **Configurabilidad:** Debe permitir configurarse con facilidad.
- **Documentación:** Debe contar con la documentación necesaria, manuales o guías de uso para aprovechar de mejor manera la herramienta.

Las herramientas para el CSIRT Académico de la ESPE dependerá de los servicios que se quieran implementar y del presupuesto que la institución provea para el proyecto. Para la puesta en marcha inicial se tomará como referencia los servicios básicos de un CSIRT, es decir se necesitará herramientas como:

- **Escáneres de puertos:** recoge información sobre los puertos, los hosts, sistema operativo, servicios de una o varias IP asignadas.

- **Herramientas de análisis de vulnerabilidad:** Generan informes sobre fallas de seguridad de una red explotando vulnerabilidades conocidas.

- **Herramientas de Alertas y reportes:** Funcionan dando alertas si un peligro potencial entro a la red, de esta manera permite que los administradores de red tomen decisiones para que la infraestructura TI no sea vulnerada.

- **Herramientas Forenses:** Ayudan en la investigación de un suceso después de haber ocurrido o colaboran validando la integridad de la información.

- **Feeds:** Recopila información necesaria en varias páginas webs, sobretodo en blogs permitiendo resolver de mejor manera los incidentes.

Capítulo III

Introducción

El presente capitulo trata sobre la Transición del Servicio Basado en ITIL en donde se describirá el proceso de puesta en marcha de un CSIRT Académico en los laboratorios del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE, siendo la idea principal el poner en funcionamiento el hardware y software necesario para que el servicio este operativo y resuelva las necesidades descritas en la fase de Diseño del Servicio realizada por (De la Torre Moscoso & Parra Rosero, 2018). Para el presente proyecto se analizó la situación actual de la Universidad dando solución o realizando cambios pertinentes para que el proyecto sea un éxito tomando en cuenta que la Estrategia y el Diseño del Servicio fueron realizados en el 2018.

Situación actual del proyecto CSIRT ESPE

La Universidad de las Fuerzas Armadas ESPE no cuenta actualmente con un CERT/CSIRT/SOC académico que entregue garantías en los niveles de seguridad dentro de la institución, solamente cuenta con una área de seguridad informática en la Unidad de Tecnologías de la Información y Comunicaciones UTIC pero no existe un modelo o departamento que cuente con un modelo organizacional, roles y responsables dedicados a la gestión de respuesta ante incidentes informáticos propiamente establecido, dando como consecuencia los bajos niveles de seguridad de la información dentro de la ESPE y la preocupación del personal ante tal situación.

Ante la necesidad y preocupación del personal, ha habido varios proyectos que intentan dar solución a los problemas de seguridad de la información de la ESPE, entre los más importantes están:

- “Estrategia y Diseño de un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) Académico para la Universidad de las Fuerzas Armadas ESPE” (realizada en el 2018).

- “Modelo de Análisis y selección de Herramientas de Ciberseguridad para un CSIRT Académico: Caso CSIRT-ESPE” (realizada en el 2018).

- “Diseño e Implementación del sistema de gestión de servicios e infraestructura de TI para el CSIRT/CERT Académico de la ESPE” (en ejecución).

Para la base de este trabajo de titulación se tomó en cuenta la tesis de grado de los autores (De la Torre Moscoso & Parra Rosero, 2018) ya que describe la Fase I y Fase II de ITIL que sirvió de guía para la elaboración de la Fase III y Fase IV en el presente proyecto ubicando al CSIRT Académico de la ESPE dentro del Departamento de Ciencias de la Computación.

También se tomó en cuenta el proyecto que se encuentra en fase inicial titulado “Diseño e Implementación del sistema de gestión de servicios e infraestructura de TI para el CSIRT/CERT Académico de la ESPE” elaborada por (Fuertes et al., 2020), donde el presente trabajo de titulación aporta en la marcha inicial de implementación de un CSIRT Académico que beneficiará a toda la comunidad universitaria.

Planificación y soporte a la transición

El presente literal describe el personal y roles, metas, interesados, proveedores, y la planificación de actividades que se necesitó para la puesta en marcha inicial del servicio.

Tabla 4.

Personal a cargo y roles

Rol	Nombre completo	Departamento al que pertenece	Contacto	Responsabilidades
Director General/Capacitador/ Analista de servicios	Mario Bernabé Ron Egas.	Departamento de ciencias de la computación	3989400. Ext. 1902. mbron@espe.edu.ec	- Organizar al equipo - Realizar reuniones - Aprobar actividades en la creación del CSIRT - Gestionar tiempos - Acercamiento con las demás áreas interesadas - Informes y reportes Análisis de hardware y software - Localizar posibles vulnerabilidades - Identificar riesgos de un incidente de seguridad y su alcance - Elaborar informes - Capacitación al personal - Ejecución de talleres y cursos - Búsqueda de socios para capacitar al personal - Investigar nuevos hardware y software - Control de capacitaciones
Miembro del Comité de Tecnología / Investigador	Enrique Vinicio Enrique Carrera PhD en Ingeniería de Sistemas y Computación	Departamento de Eléctrica y Electrónica	3989400, Ext. 1880.	- Asesorar la planificación . Recomendar lineamientos para la puesta en marcha del CSIRT - Valorar el avance - Recomendar planes correctivos - Asesorar reporte de riesgos
Miembro del Comité de Tecnología	Manuel Sánchez Rubio (Doctor por la Universidad de Alcalá e Ingeniero en Informática)	Director del Master de Seguridad Informática en Universidad Internacional de la Rioja, España	manuel.sanchezrubio@unir.net	- Asesorar la planificación . Recomendar lineamientos para la puesta en marcha del CSIRT - Valorar el avance - Recomendar planes correctivos - Asesorar reporte de riesgos
Miembro del Comité de Tecnología	Freddy Mauricio Tapia León	Departamento de Ciencias de la Computación	3989400, Ext. 1934;	- Asesorar la planificación . Recomendar lineamientos para la

Rol	Nombre completo	Departamento al que pertenece	Contacto	Responsabilidades
	Máster en Investigación e Innovación en TIC's		fmtapia@espe.edu.ec	puesta en marcha del CSIRT - Valorar el avance - Recomendar planes correctivos - Asesorar reporte de riesgos
Investigador	Recalde Herrera Luis Lenin (Magíster en Evaluación y Auditoría de Sistemas Tecnológicos)	Departamento de Seguridad y Defensa	3989400, Ext. 2562 llrecalde@espe.edu.ec	- Diseñar proyectos de investigación - Reportar avance de tareas - Difusión de proyectos - Elaborar publicaciones periódicas
Investigador	Alberto Daniel Núñez Agurto (Magister en Gerencia de Sistemas)	Departamento de Ciencias de la Computación,	3989400, Ext. 4940 adnunez1@espe.edu.ec	- Diseñar proyectos de investigación - Reportar avance de tareas - Difusión de proyectos - Elaborar publicaciones periódicas
Investigador	Walter Fuertes	Departamento de Ciencias de la Computación	3989400, Ext. 1906. wmfuertes@espe.edu.ec	- Diseñar proyectos de investigación - Reportar avance de tareas - Difusión de proyectos - Elaborar publicaciones periódicas
Investigador	Dr. Henry Omar Cruz Carrillo	Departamento de Ciencias de la Energía y Mecánica	3989400 Ext, 2510, hocruz@espe.edu.ec	- Diseñar proyectos de investigación - Reportar avance de tareas - Difusión de proyectos - Elaborar publicaciones periódicas
Analista de servicios / Monitor de redes / Implementador	Jonathan Francisco Benavides Cabascango Autor del presente proyecto	Departamento de Ciencias de la Computación	jfbenavides@espe.edu.ec	- Implementar y configurar software y hardware necesario - Soporte a hardware y software - Buscar vulnerabilidades de red - Reportar vulnerabilidades a los administradores - Resguardar información - Gestionar incidentes - Realizar procesos operativos a fin de monitorear la red - Análisis de hardware y software

Rol	Nombre completo	Departamento al que pertenece	Contacto	Responsabilidades
				- Localizar posibles vulnerabilidades - Identificar riesgos de un incidente de seguridad y su alcance - Elaborar informes
Director UTICs ESPE	Rommel Asitimbay	Director UTICs ESPE	rdasitimbay@espe.edu.ec	- Administrar red de la ESPE - Delegar responsabilidades y casos - Responder las solicitudes al monitor en redes - Mantener comunicación continua con el CSIRT Académico.

La planificación de actividades y metas a alcanzar están descritas en la siguiente tabla:

Tabla 5.

Planificación y metas para la puesta en marcha inicial del CSIRT

Actividad	Personal a cargo	Meta / Objetivo
Revisión de proyectos anteriores y estado del arte	Todos los cargos	Tomar en cuenta proyectos anteriores que sirvan para la elaboración del presente trabajo y compararlo con la realidad actual de la ESPE y realizar los cambios pertinentes
Diseñar e implementar servicios básicos	Todos los cargos	Encontrar la comunidad objetivo e implementar los servicios básicos tanto proactivos y reactivos de un CSIRT Académico

Actividad	Personal a cargo	Meta / Objetivo
Test de prototipos de herramientas	Implementador / analista de servicios	Implementar y probar herramientas para mitigar incidentes de seguridad de la información.
Implementar la infraestructura básica de TI	Implementador	Analizar infraestructura como laboratorios, equipos, software y hardware para la implementación del CSIRT Académico
Licenciamiento	Director General / Implementador	Coordinar con los socios y proveedores para el licenciamiento o compra de software
Diseñar procedimientos y políticas de seguridad asociados a la gestión de incidentes	Director General / Analista de servicios / Monitor de redes	Diseño de la gestión de incidentes y políticas del CSIRT Académico
Diseñar procedimientos del funcionamiento del CSIRT académico	Todos los cargos	Elaborar los procesos de cada servicio
Establecer contactos y relaciones publicas	Director General	Conseguir convenios, colaboración, acercamientos, etc., con otros Equipos de Respuesta ante Incidentes.
Capacitaciones	Capacitador	Crear convenios con empresas para la capacitación del personal
Operación del servicio	Todos los cargos	Operar el servicio con el fin de mejorar la calidad y proveer más servicios en el futuro.

Los interesados del proyecto son el personal de la comunidad universitaria,

personal docente, administrativo y alumnos. En cuanto a proveedores y acercamientos con otros Equipos de Respuesta ante Incidentes se ha logrado establecer comunicación con los siguientes:

- Nicolás Macías, Coordinador Técnico del CERT Académico de la Universidad Nacional de la Plata.
- José María Gómez de la Torre, Técnico Operativo de EcuCERT.
- Liliana Córdova, Coordinadora del CSIRT-EPN.
- Ernesto Pérez, Coordinador CSIRT CEDIA (Proveedor de licencia de software específico para escaneo de vulnerabilidades)

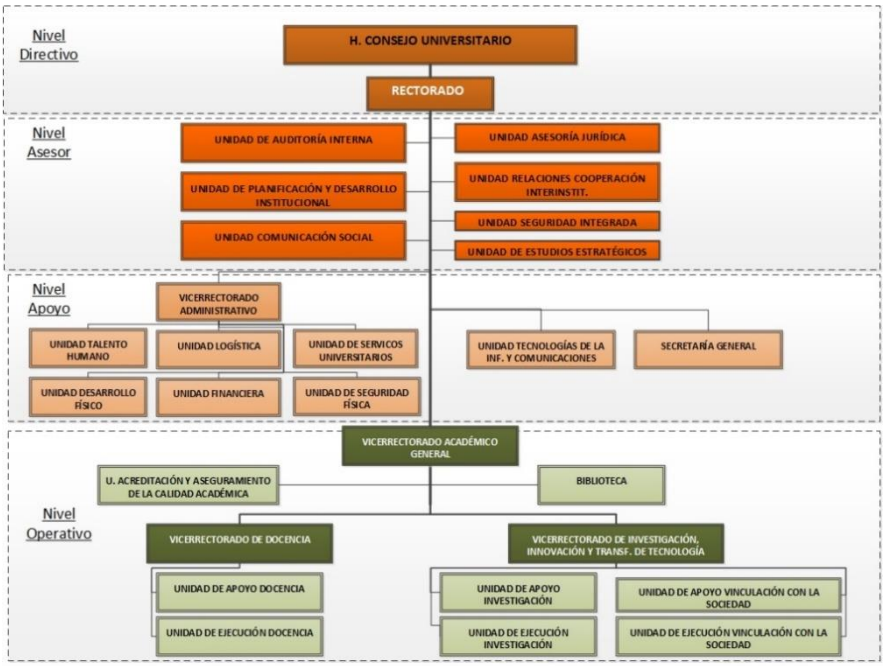
Gestión de cambios

El presente literal describe la forma en que se levantó el servicio, el lugar, las tecnologías a implementar y todos los cambios realizados en la institución de tal forma que no interrumpa los demás procesos y asegurar que los cambios tengan el menor impacto negativo dentro de la línea de producción.

A continuación, observamos la estructura organizacional de la Universidad la cual sirvió para entender la ubicación del CSIRT propuesta por los autores (De la Torre Moscoso & Parra Rosero, 2018):

Figura 22.

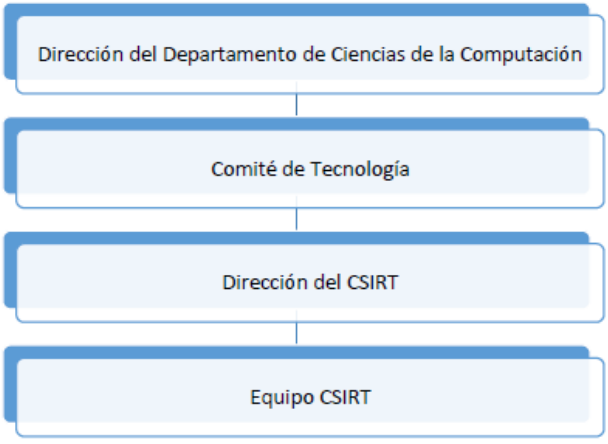
Estructura Organizacional de la ESPE



Nota. Tomado de *ESPE* por Universidad de las Fuerzas Armadas ESPE, 2020.

Figura 23.

Propuesta de ubicación jerárquica del CSIRT



Nota. Tomado de *Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas*

ESPE por De la Torre Moscoso Hugo Marcelo; Parra Rosero Mario Andrés, 2018.

En base a la propuesta jerárquica de ubicación del CSIRT, la infraestructura TI necesaria para levantar el servicio se instaló en el laboratorio H-402, misma que servirá como centro de operaciones ya que cuenta con los equipos computacionales, seguridad e infraestructura necesaria para que el CSIRT Académico pueda funcionar correctamente. Se optó por utilizar dicho laboratorio para no interrumpir con las actividades que realizadas por las UTICs y para que el servicio cause el menor impacto en la línea de producción.

Los riesgos que involucran el cambio en la puesta en marcha del CSIRT Académico viene dado por la siguiente matriz, en donde la probabilidad es calificada por: 1. No sucede, 2. Raramente sucede, 3. Es posible, 4. Casi seguro que sucede y 5. Muy probable. Mientras que el impacto es calificado de la siguiente manera 1. Insignificante, 2. Pequeño, 3. Moderado, 4. Grande y 5. Desmedido.

La calificación del riesgo es sobre 100 siendo de 0 a 25 bajo, 26 a 50 medio, 51 a 75 alto y de 76 a 100 muy alto.

Tabla 6.

Matriz de riesgo para la Gestión de cambios

No	Objetivo / Actividad	Descripción del Riesgo	Probabilidad	Impacto	Calificación	Acciones
1	Realizar una revisión sistemática de literatura de la documentación y proyectos en marcha que existen para la implementación de un CSIRT Académico.	Las propuestas realizadas en anteriores proyectos ya no son válidas con la realidad actual de la ESPE	3. Es posible	2. Pequeño	24/100 Bajo	Analizar las propuestas anteriores y realizar modificaciones para adaptarlas a la realidad actual de la ESPE.

No	Objetivo / Actividad	Descripción del Riesgo	Probabilidad	Impacto	Calificación	Acciones
2	Investigar y seleccionar las herramientas de seguridad informática más adecuadas para los servicios iniciales que prestará el CSIRT Académico de la ESPE.	Falta de recursos y financiamiento para la compra de software y hardware.	3. Es posible	3. Moderado	36/100 Medio	Utilizar servidores existentes en el laboratorio juntamente con herramientas sin costo para disminuir la necesidad de recursos.
3	Determinar la comunidad beneficiaria, la infraestructura y diseñar los servicios que serán implementados en el CSIRT Académico.	Permisos para operar en toda la infraestructura de red de la comunidad universitaria.	4.Casi seguro que sucede	4. Grande	64/100 Alto	Sacar los permisos pertinentes para que las UTICs permita el acceso la red de la ESPE
4	Instalar y configurar el hardware y software necesario para el funcionamiento inicial del CSIRT Académico de la ESPE.	Versión de Sistema operativo de los servidores	3. Es posible	2. Pequeño	24/100 Bajo	Actualizar servidores y equipos.
5	Evaluar y documentar la operación del CSIRT Académico.	No lograr evaluar el 100% de la capacidad del proyecto por la pandemia de Covid-19 actual.	5.Muy probable	4. Grande	80/100 Muy Alto	Configurar los equipos y la infraestructura para poder trabajar desde casa

Gracias a la valoración y a la evaluación de riesgos analizados, el Ingeniero Mario Ron, persona a cargo del laboratorio H-402 autoriza la Gestión del cambio y se procede a la implementación del servicio.

Gestión de la Configuración y Activos del Servicio

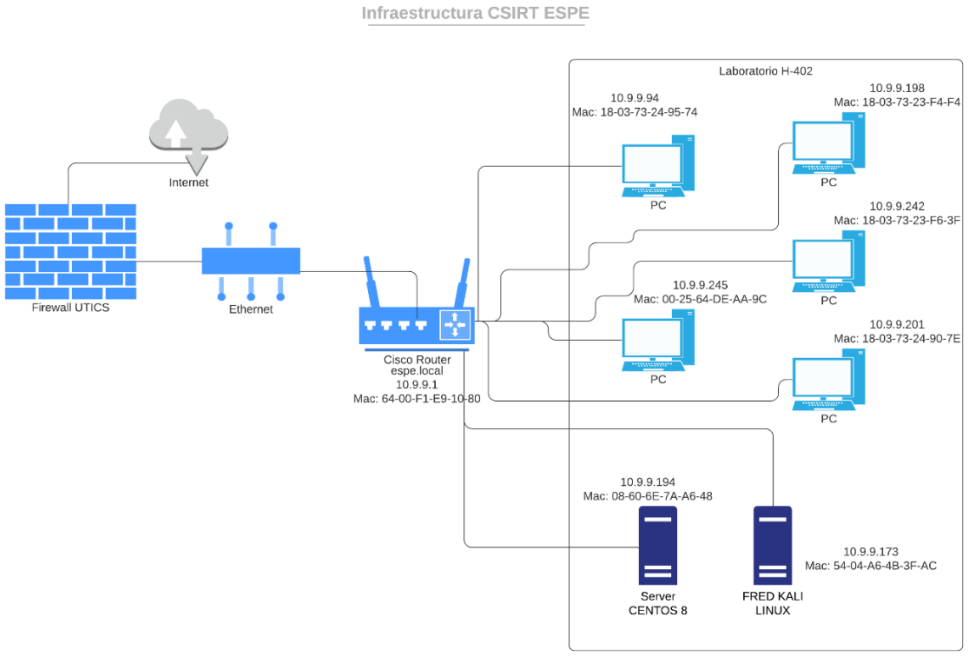
El presente literal describe la información de la infraestructura TI necesaria para

poner en marcha el servicio, donde se usó una CMDB para guardar la información de la configuración realizada en cada activo.

Para la implementación y configuración de los activos se hizo una revisión de la infraestructura del laboratorio H-402, tomando en cuenta el espacio físico, cubículos de docentes y estado de los equipos a ser configurados, los cuales para la operación del servicio se usó cinco equipos computacionales y dos servidores. En la siguiente figura se observa el diseño de red del aula y de los equipos a ser utilizados para la operación del servicio:

Figura 24.

Infraestructura CSIRT ESPE



Nota. El Grafico representa la estructura de red del laboratorio H-402 adaptada para el CSIRT-ESPE

La siguiente tabla describe los CIs que se encuentra en el laboratorio, tomando

en cuenta que no todos son necesarios para la puesta en marcha del servicio ya que algunos activos son de uso de docentes.

Tabla 7.

CMDB de los activos del CSIRT Académico

Cls	**Descripción**	**Código del activo**	**Condición**	**Dirección IP / MAC**	**S.O**	**Uso**
Video proyector EPSON	Video proyector 3200 lúmenes incluye maleta, control remoto, cable de poder, cable de video.	4543170	Bueno	-	-	Exposiciones, Capacitaciones, Reuniones, Visualización de monitoreo a toda el área.
Teléfono digital 3com	Teléfono digital.	4543721	Regular	-	-	Recibir llamadas.
CPU Dell de escritorio	CPU CORE I 7 3.40 Ghz 500 Gb DVD RW	4591585	Bueno	IP: 10.9.9.94 Mac:18-03-73-24-95-74	Windows 10 y Kali Linux	Monitoreo de red, herramientas forenses, elaboración de informes.
CPU Dell de escritorio	CPU CORE I 7 3.40 Ghz 500 Gb DVD RW	4591586	Bueno	IP: 10.9.9.245 Mac: 00-25-64-DE-AA-9C	Windows 10 y Kali Linux	Monitoreo de red, herramientas forenses, elaboración de informes.
CPU Dell de escritorio	CPU CORE I 7 3.40 Ghz 500 Gb DVD RW	4591587	Bueno	IP: 10.9.9.198 Mac: 18-03-73-23-F4-F4	Windows 10 y Kali Linux	Monitoreo de red, herramientas forenses, elaboración de informes.
CPU Dell de escritorio	CPU CORE I 7 3.40 Ghz 500 Gb DVD RW	4591588	Bueno	IP: 10.9.9.242 Mac: 18-03-73-23-F6-3F	Windows 10 y Kali Linux	Monitoreo de red, herramientas forenses, elaboración de informes.
CPU Dell de escritorio	CPU CORE I 7 3.40 Ghz 500 Gb DVD RW	4591589	Bueno	IP: 10.9.9.201	Windows 10 y Kali Linux	Monitoreo de red, herramientas forenses,

Cls	Descripción	Código del activo	Condición	Dirección IP / MAC	S.O	Uso
				Mac: 18-03-73-24-90-7E		elaboración de informes.
CPU Dell de escritorio	CPU CORE I 7 3.40 Ghz 500 Gb DVD RW	4591590	Bueno	-	Windows 10	Equipo de docente
CPU Dell de escritorio	CPU CORE I 7 3.40 Ghz 500 Gb DVD RW	4591591	Bueno	-	Windows 10	Equipos de docente
CPU Dell de escritorio	CPU CORE I 7 3.40 Ghz 500 Gb DVD RW	4591592	Bueno	-	Windows 10	Equipo de docente
Servidor Asus	ASUS DUAL INTEL 2.4 GHZ 12 GB RAM 2HDD DE 300 GB Y 2.0 TB	4591565	Bueno	IP: 10.9.9.173 Mac: 54-04-A6-4B-3F-AC	Windows 10 y Kali Linux	Herramientas de forense.
Servidor Asus	ASUS INTEL X79 16 GB RAM 1TB HDD - 120 GB HDD	4592181	Bueno	IP: 10.9.9.194 Mac: 08-60-6E-7A-A6-48	Centos 8	Alojamiento de servicios
Monitor Dell	MONITOR LCD 19"	4596019	Bueno	-	-	Accesorio de CPU
Monitor Dell	MONITOR LCD 19"	4596020	Bueno	-	-	Accesorio de CPU
Monitor Dell	MONITOR LCD 19"	4596021	Bueno	-	-	Accesorio de CPU
Monitor Dell	MONITOR LCD 19"	4596022	Bueno	-	-	Accesorio de CPU
Monitor Dell	MONITOR LCD 19"	4596023	Bueno	-	-	Accesorio de CPU
Monitor Dell	MONITOR LCD 19"	4596024	Bueno	-	-	Accesorio de CPU
Monitor Dell	MONITOR LCD 19"	4596025	Bueno	-	-	Accesorio de CPU

Cls	Descripción	Código del activo	Condición	Dirección IP / MAC	S.O	Uso
Monitor Dell	MONITOR LCD 19"	4596026	Bueno	-	-	Accesorio de CPU
Monitor LG	MONITOR LCD 19"	4596099	Bueno	-	-	Accesorio de CPU

Para poner en marcha el CSIRT Académico, se realizó una selección de hardware y software que satisfagan las necesidades iniciales y sean óptimos para el ciclo de vida del servicio. En la siguiente tabla se explica los criterios que se utilizó para escoger de manera correcta las herramientas, en donde Portabilidad se refiere a la capacidad de la aplicación en ser multiplataforma y pueda brindar servicios con otras aplicaciones; Documentación se refiere a la información y manuales que se encuentra en línea para la configuración y Fiabilidad se refiere a la madurez de la aplicación para entregar datos confiables.

Tabla 8.

Selección de software para el CSIRT Académico ESPE

Herramienta	Portabilidad	Documentación	Fiabilidad	Precio	Observaciones
Nessus	✓	✓	✓	$3190	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.

Herramienta	Portabilidad	Documentación	Fiabilidad	Precio	Observaciones
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.
AnyDesk	✓	✓	✓	Gratuito	Software de acceso remoto.

Gracias a todas sus características y observaciones, finalmente el software que se escogió para la puesta en marcha del CSIRT Académico fue Nessus, Nmap, FortiAnalyzer (FortiGate), FreshDesk, AnyDesk y Shodan, los cuales servirán para brindar los servicios básicos iniciales del CSIRT.

Tabla 9.

Software seleccionado para el CSIRT Académico de la ESPE

Herramienta	Descripción	Versión	Observaciones
Nessus	Herramienta de análisis de vulnerabilidades y amenazas en tiempo real. Es considerado uno de los mejores del mundo ya que tiene una gran precisión y evita informar falsos positivos	8.10.1	El software se encuentra trabajando en perfectas condiciones con la IP local 10.9.9.194
Nmap	Herramienta de escaneo de puertos donde se revisa los equipos conectados a una red, puertos abiertos, aplicaciones que se ejecutan etc.	7.80-1	Para la utilización de este software en particular no es necesario instalarlo dentro del servidor ya que puede ser utilizado en cada estación individual de trabajo.
FortiAnalyzer	Herramienta que analiza logs y eventos de red, también cuenta con herramientas de análisis forense, análisis de	-	Se escogió el FortiAnalyzer de Fortinet ya que la universidad cuenta con esos equipos.

Herramienta	Descripción	Versión	Observaciones
	vulnerabilidades y escaneo de red. IDS		
Shodan	Motor de búsqueda enfocado a encontrar sistemas y servicios conectados a internet.	-	Servicio web para monitoreo en tiempo real de amenazas https://www.shodan.io/
AnyDesk	Software para trabajo remoto, donde le permite al usuario trabajar desde otra localidad.	**5.5.6**	La instalación de AnyDesk fue necesaria para poder gestionar y configurar el servidor desde casa, por la situación actual de la pandemia de Covid-19
Freshdesk	Servicio de gestión de tickets	**-**	Para la correcta gestión de incidentes es importante implementar una aplicación de gestión de tickets para tramitar cada incidente ordenadamente.

Configuración de Nessus

Los requerimientos mínimos para la instalación de Nessus son las siguientes:

- CPU: 4 2GHz cores
- Memory: 4 GB RAM (8 GB RAM recommended)
- Disk space: 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:

- ASUS INTEL X79
- 16 GB RAM
- 1TB HDD - 120 GB HDD

- Intel® Core™ i7-3930K CPU @ 3.20GHz × 12 cores

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

- El licenciamiento se realizará por un Security Center autorizado por Tenable (CSIRT-CEDIA).
- 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 UTICs 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.

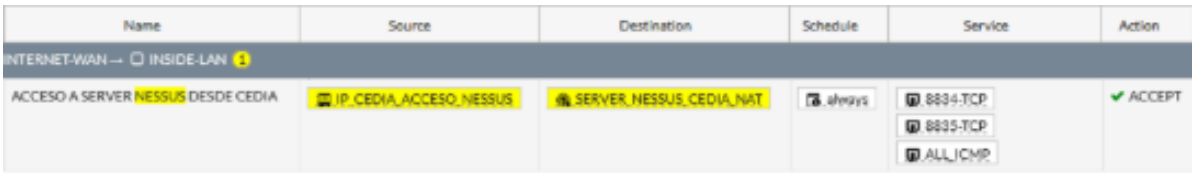
Figura 25.

NAT de IP pública a IP local

Nota. Configuración de las UTICs para el servidor Nessus.

Figura 26.

Permisos de puertos a IP local



Nota. Configuración de las UTICs para el servidor Nessus.

Gracias a los requerimientos resueltos por las UTICs CEDIA procedió al licenciamiento respectivo de la herramienta Nessus.

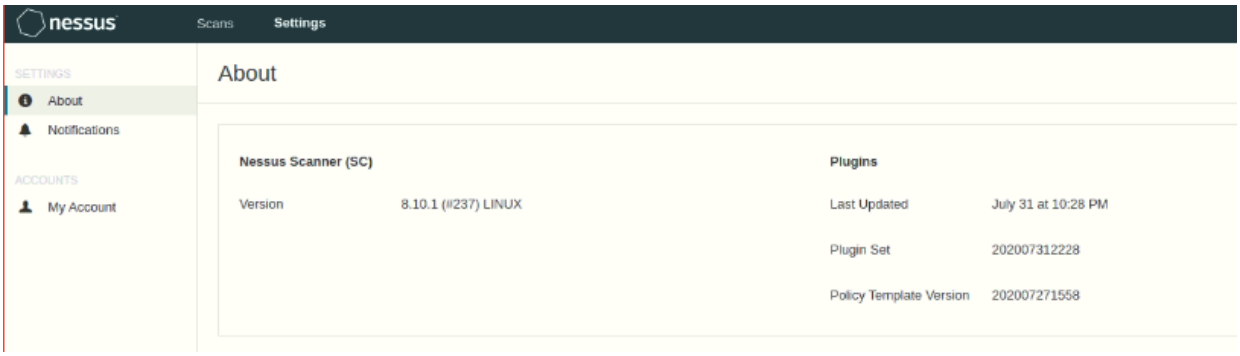
Figura 27.

Dashboard de CEDIA (Licenciamiento de Nessus)

Nota. El grafico representa el dashboard de CEDIA indicando que el licenciamiento es un éxito.

Figura 28.

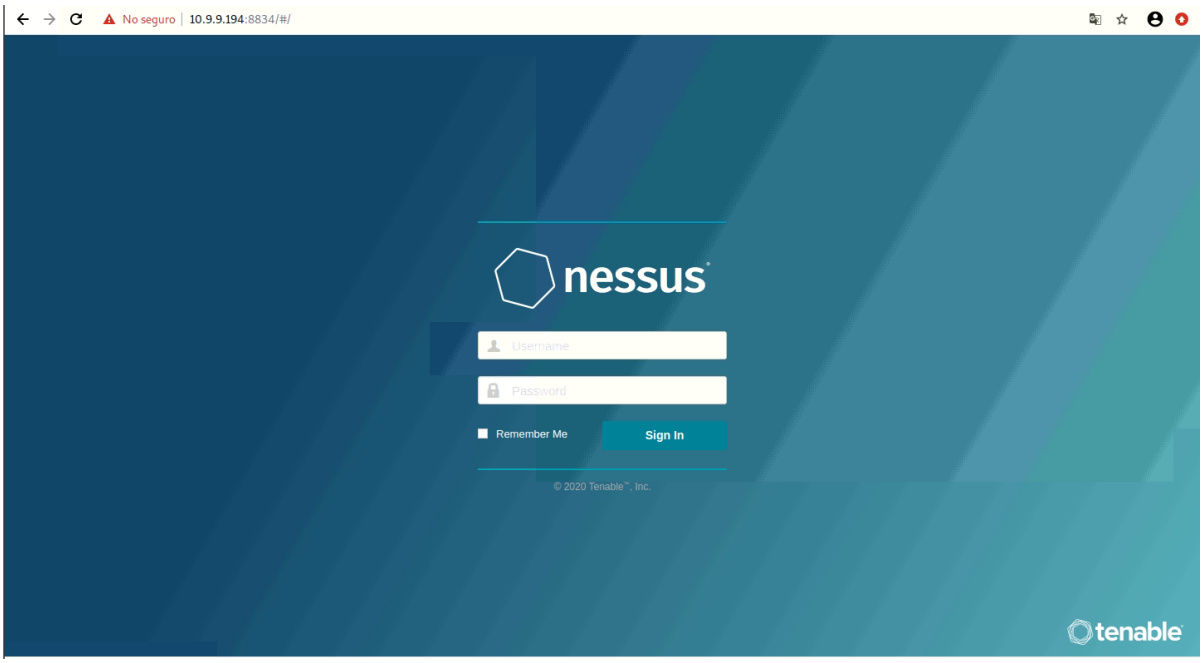
Licenciamiento de Nessus versión 8.10.1 CSIRT ESPE



Nota. El grafico indica que el licenciamiento de la herramienta fue un éxito.

Figura 29.

Operación de Nessus versión 8.10.1



Nota. El grafico representa el funcionamiento de Nessus en el servidor 10.9.9.194.

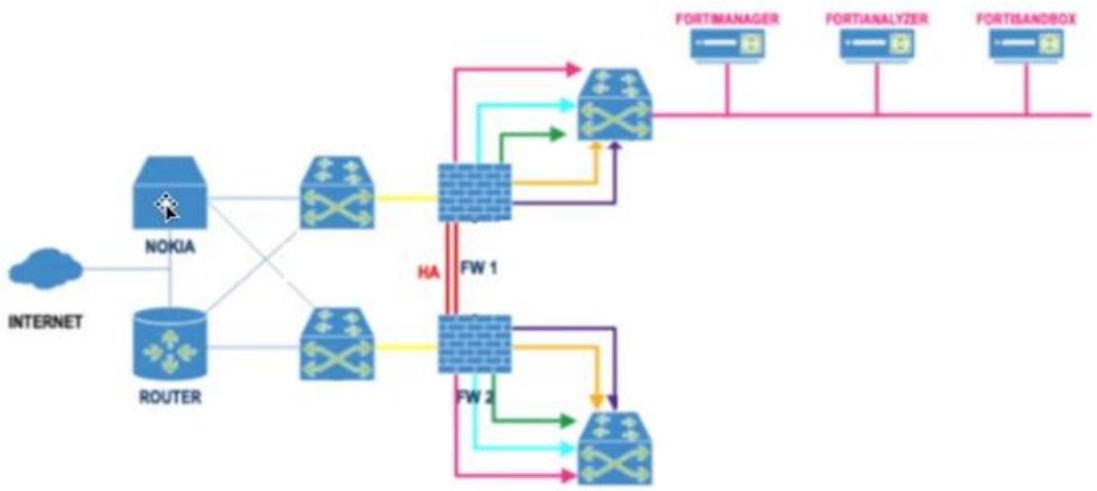
Configuración FortiAnalyzer

FortiAnalyzer es un producto de Fortinet que permite monitorear el tráfico de red de una institución mediante la unión de componentes como un firewall. FortiAnalyzer permite al usuario llevar un control de tráfico, aplicaciones usadas, host comprometidos, análisis de eventos, IPS, análisis de amenazas y búsqueda de vulnerabilidades.

La Universidad de las Fuerzas Armadas ESPE cuenta con dichos equipos configurados de la siguiente manera:

Figura 30.

Diagrama de red y configuración de FortiAnalyzer

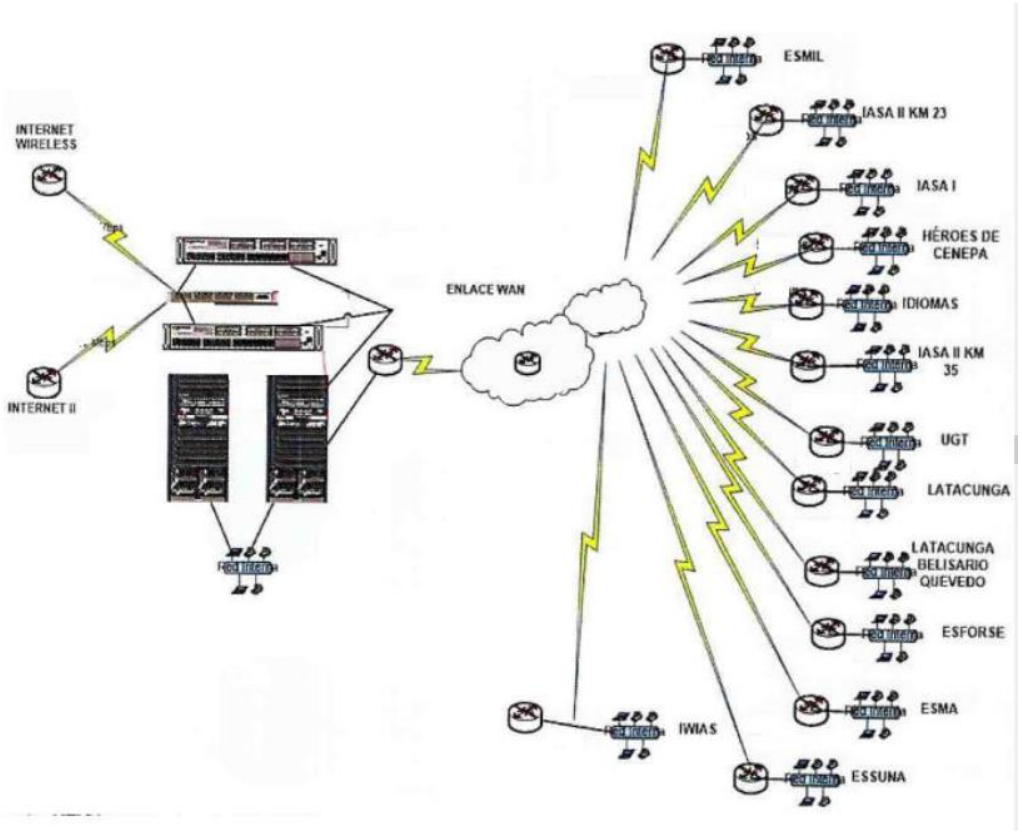


Nota. La figura indica el lugar dentro de la infraestructura de red de la instalación del FortiAnalyzer.

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 31.

Diagrama de red de la Universidad de las Fuerzas Armadas ESPE

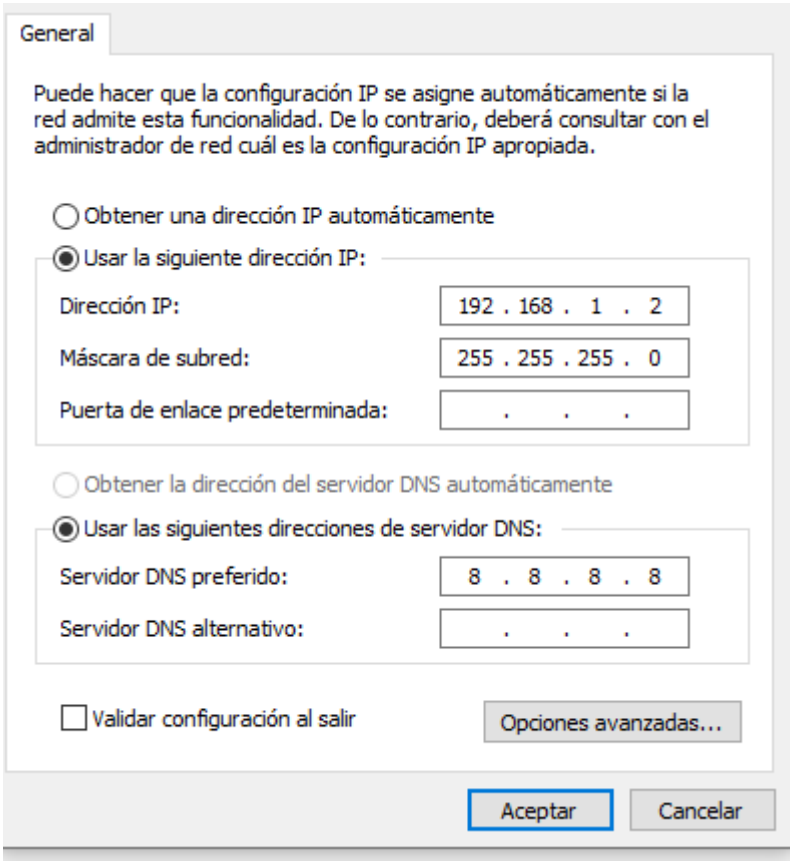


Nota. Tomado del *Plan Estratégico de Tecnologías de la Información y Comunicaciones* por UTIC ESPE, 2015.

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 32.

Configuración manual FortiAnalyzer



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

Figura 33.

Ingreso a FortiAnalyzer de forma manual.

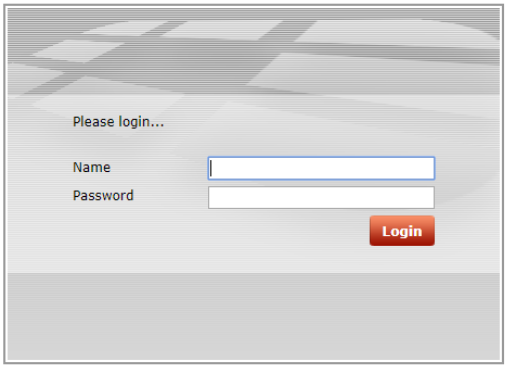
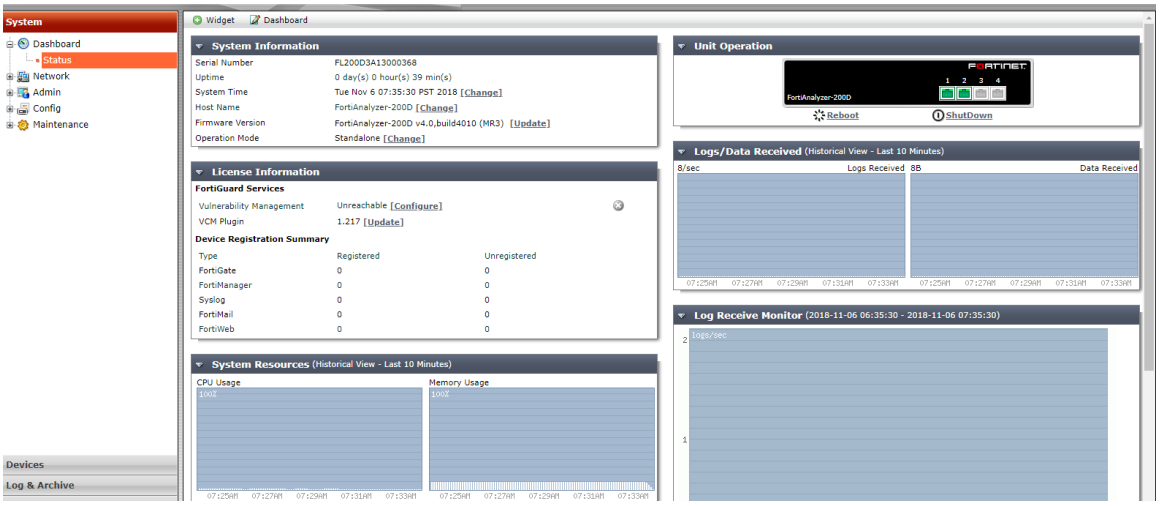


Figura 34.

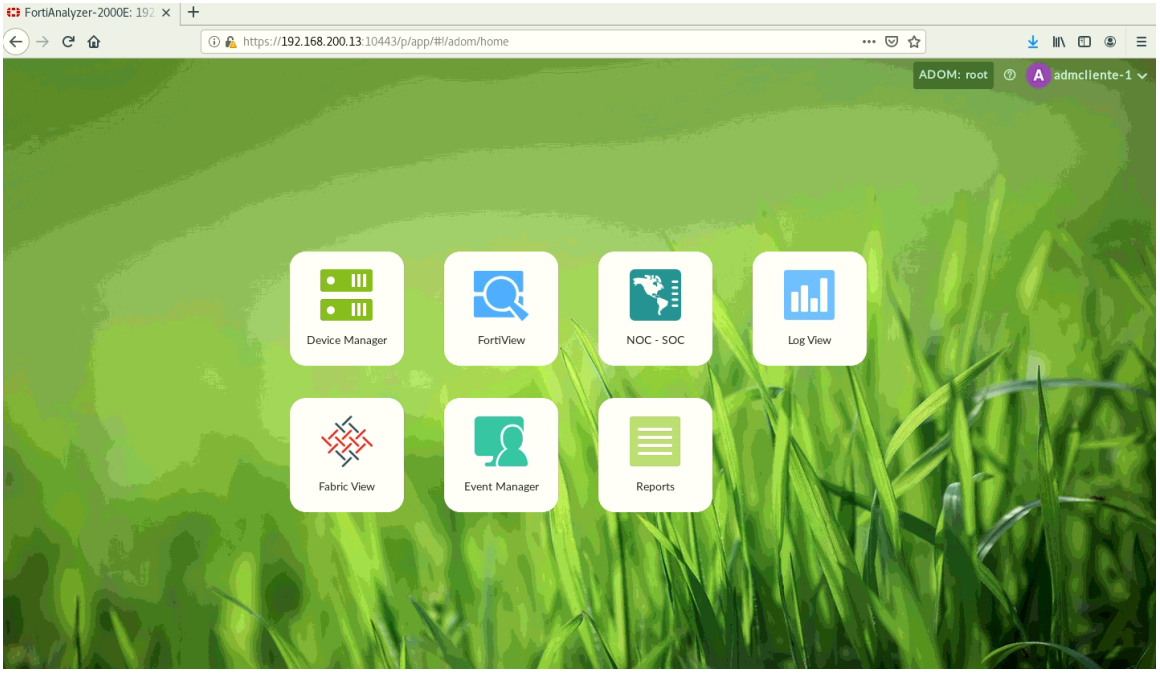
Dashboard de configuración de FortiAnalyzer



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 del CSIRT-ESPE a la visualización del dispositivo y monitorear eventos.

Figura 35.

FortiAnalyzer centralizado ESPE

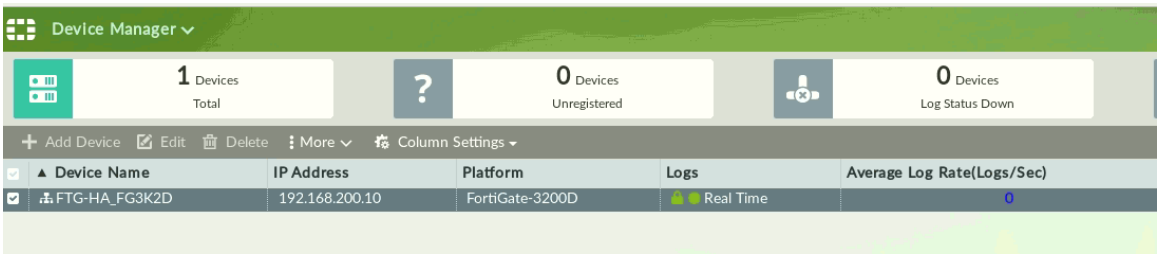


Nota. La figura representa el dashboard principal para gestionar el FortiAnalyzer de la institución.

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

Figura 36.

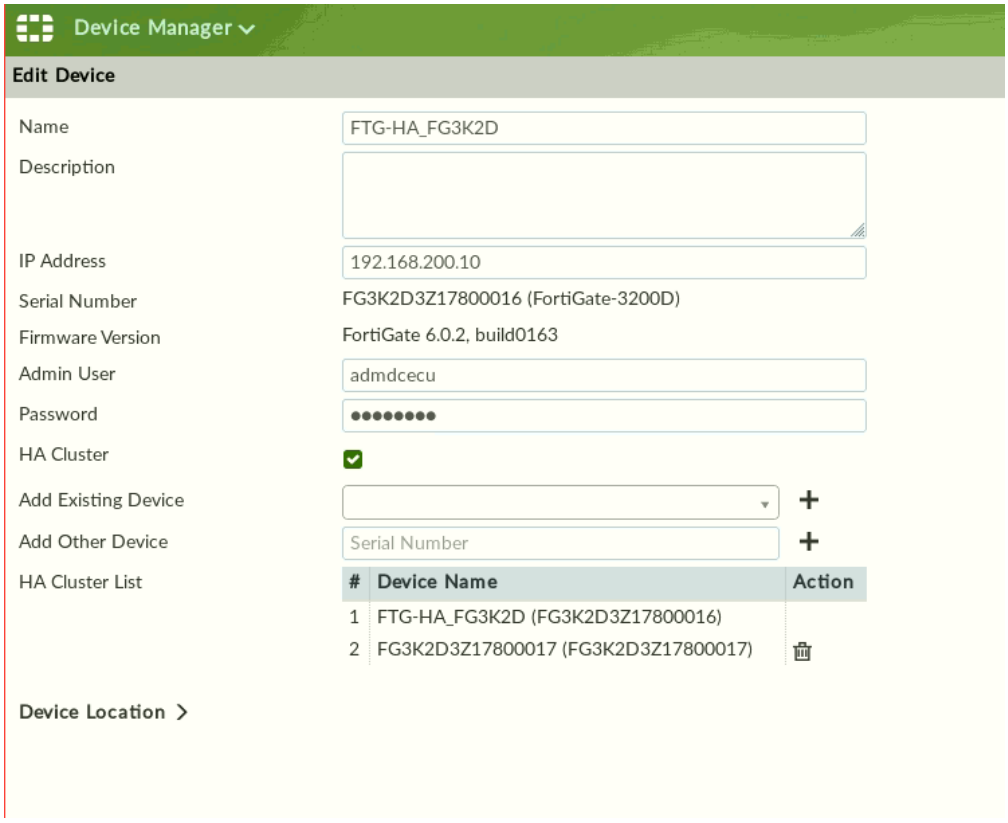
Configuración de dispositivos en FortiAnalyzer



Nota. La figura representa los dispositivos agregados para analizar tráfico por el FortiAnalyzer.

Figura 37.

Ingreso de firewall a FortiAnalyzer



Nota. La figura representa los datos del dispositivo agregado para que el FortiAnalyzer analice el tráfico.

Configuración Shodan

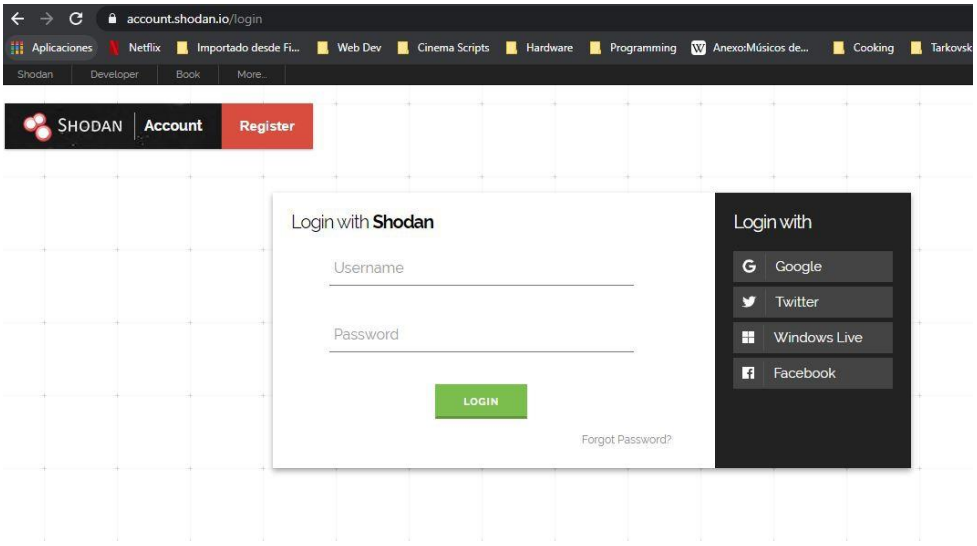
Shodan es un motor de búsqueda de dispositivos conectados a internet que sirve para recaudar información de servicios, puertos, vulnerabilidades y amenazas de los dispositivos conectados en todo el mundo. El acceso a Shodan se hace mediante su página web shodan.io y dispone de varios servicios como el de motor de búsqueda, monitoreo en tiempo real, APIs para servicios, reportes, búsqueda de exploits y mapas.

Uno de los servicios a entregar del CSIRT Académico ESPE es el de alertas de

incidentes, lo cual se necesitó los servicios de Shodan Monitor. La configuración se realizó de la siguiente manera.

Figura 38.

Registro Shodan.

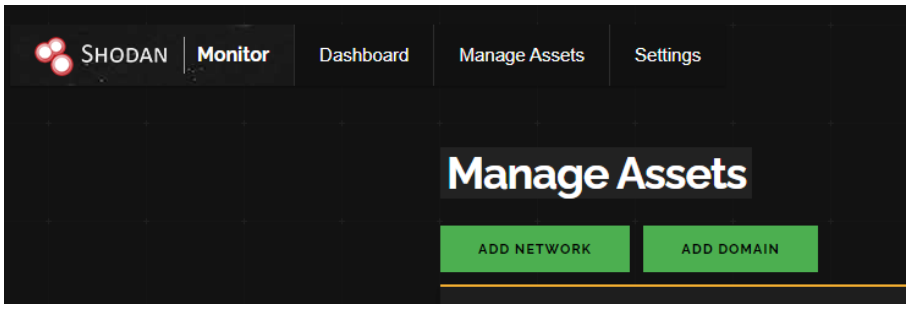


Nota. *Tomado de la web* Shodan.io *por Shodan, 2020.*

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 39.

Formas de registro de IP para monitoreo.

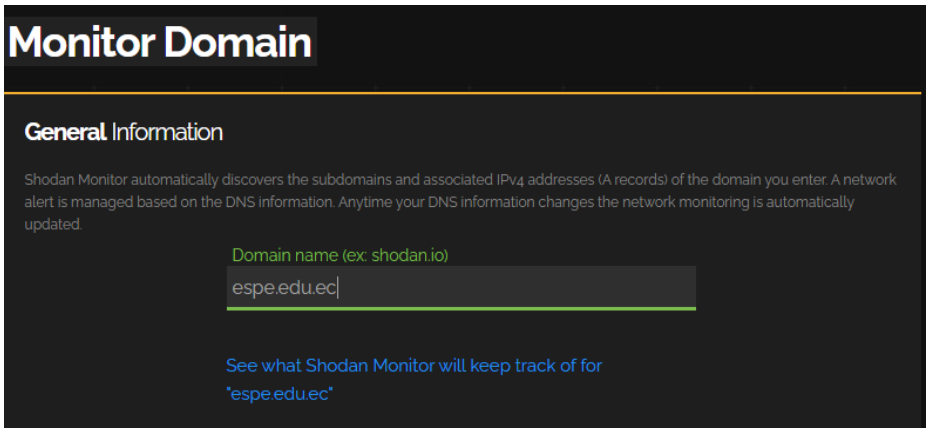


Nota. Tomado de la web *Shodan.io* por Shodan, 2020.

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

Figura 40.

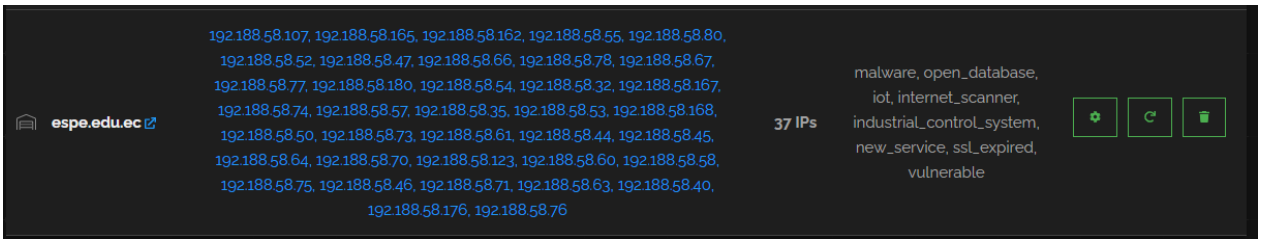
Registro del dominio ESPE en Shodan Monitor



Nota. Tomado de la web *Shodan.io* por Shodan, 2020.

Figura 41.

IP correspondientes al dominio espe.edu.ec

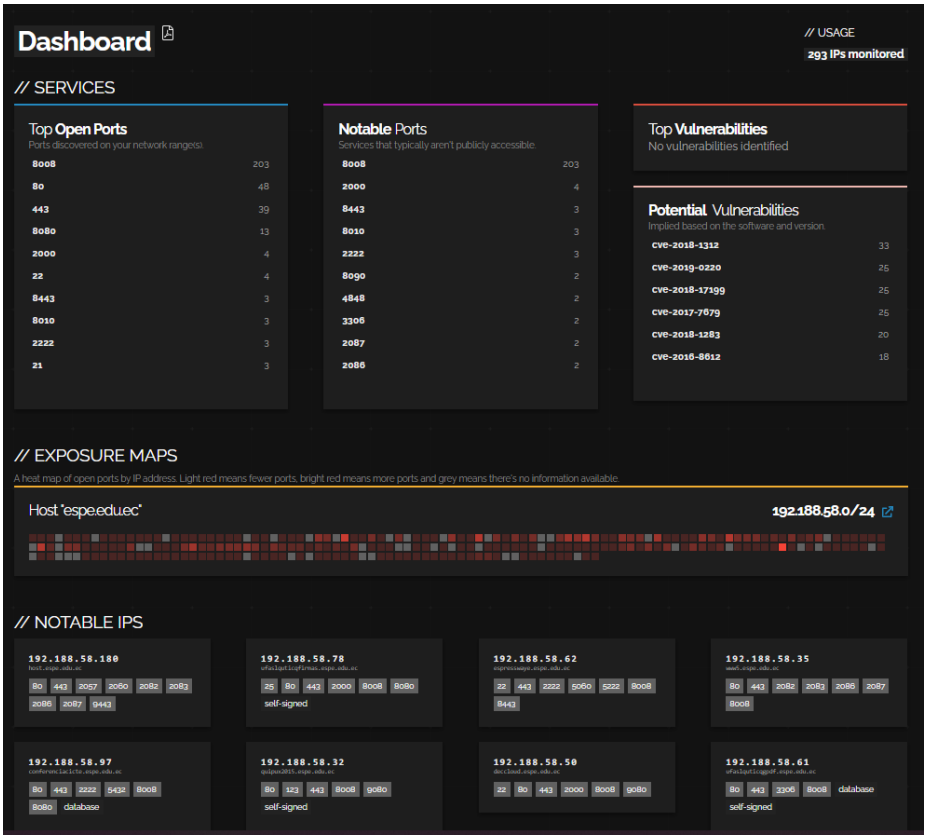


Nota. Tomado de la web *Shodan.io* por Shodan, 2020.

Después de la configuración de las IP de la ESPE, el Dashboard de monitoreo queda de la siguiente manera, en donde resalta las IP más importantes, los puertos abiertos más comunes, y las vulnerabilidades de dichos dispositivos.

Figura 42.

Dashboard de monitoreo Shodan

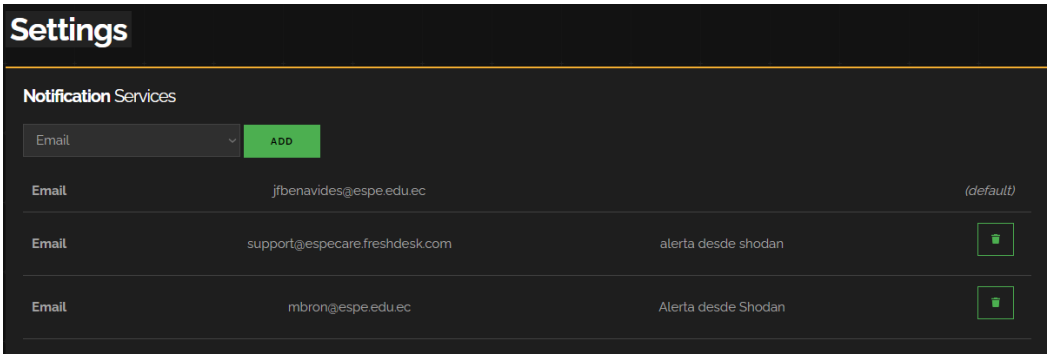


Nota. Tomado de la web *Shodan.io* por Shodan, 2020.

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

Figura 43.

Configuración al correo electrónico.



Nota. Tomado de la web *Shodan.io* por Shodan, 2020.

Configuración Freshdesk

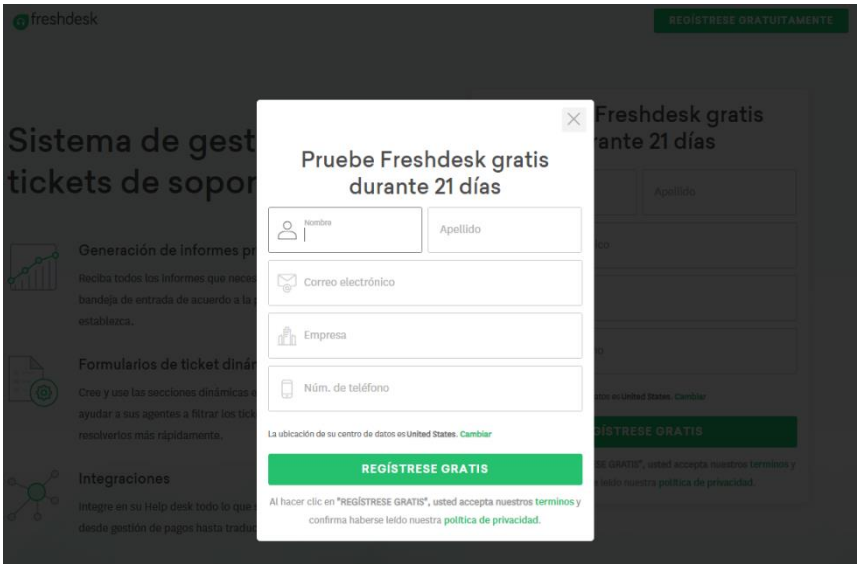
Freshdesk es un servicio web de gestión de tickets, lo cual sirve para la generación tickets o turnos dinámicos que ayuda al equipo de trabajo a solucionar los problemas de los clientes de una forma más ordenada y activa. Estos tickets pueden ser categorizados según su importancia, también asignar a al personal a cargo y generar reportes que servirán de documentación para analizar la operación de servicio y realizar mejoras a futuro.

El servicio web de Freshdesk ayuda al CSIRT Académico de la ESPE a la gestión de incidentes ya que permite asignar al personal a cargo de la resolución del mismo y priorizar los eventos. Cada incidente es tratado de inicio a fin y es registrado en el dashboard permitiendo hacer un seguimiento en el caso de que algún evento no sea resuelto.

A continuación, se describe la configuración de Freskdesk adaptado a las necesidades del CSIRT Académico ESPE.

Figura 44.

Registro Freshdesk

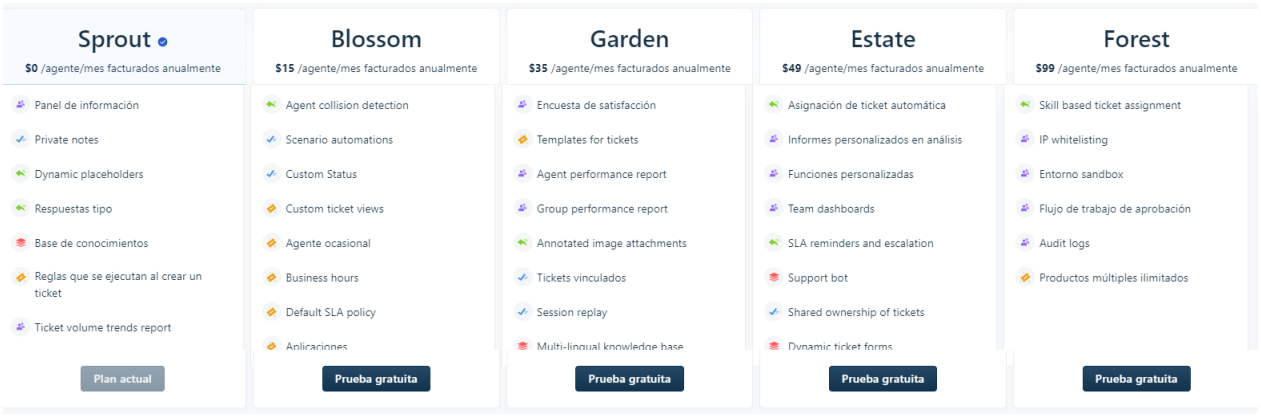


Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2020

Freshdesk dispone de varios planes que aportan servicios a las empresas; para el caso de este proyecto y la puesta en marcha inicial del CSIRT Académico 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 45.

Planes del servicio Freshdesk

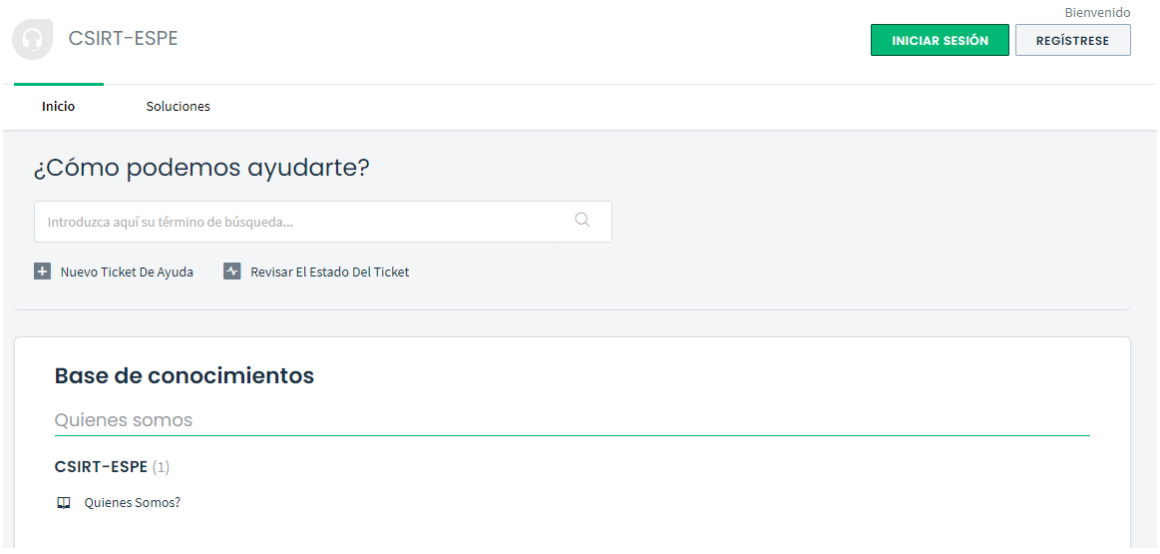


Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2020

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

Figura 46.

Portal servicio al cliente CSIRT-ESPE



Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2020

Figura 47.

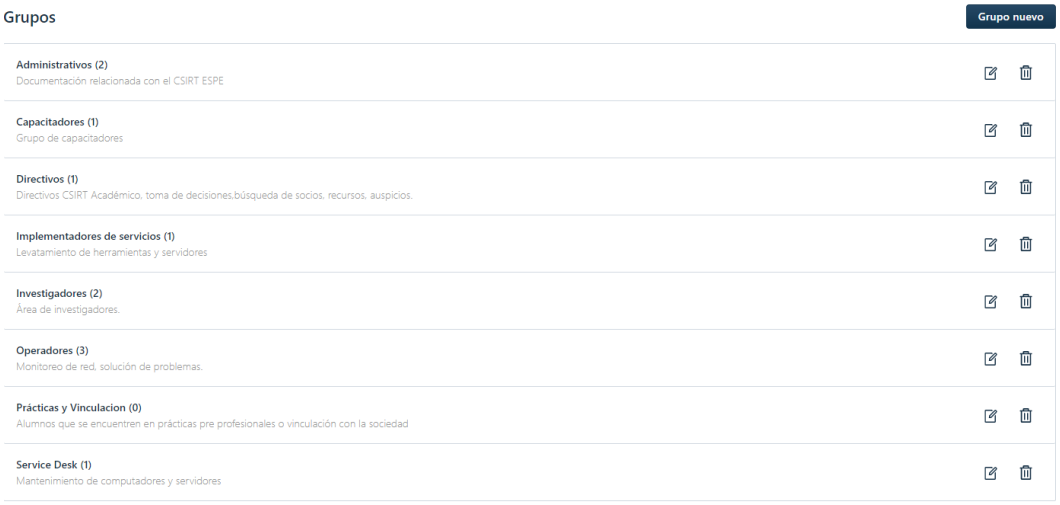
Configuración del correo de soporte CSIRT-ESPE

Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2020

Freshdesk también cuenta con la configuración de grupos que sirve para categorizar a cada agente y distinguir las funcionalidades de cada uno de ellos, esto sirve para gestionar de mejor manera los eventos de a cuerdos a los roles designados.

Figura 48.

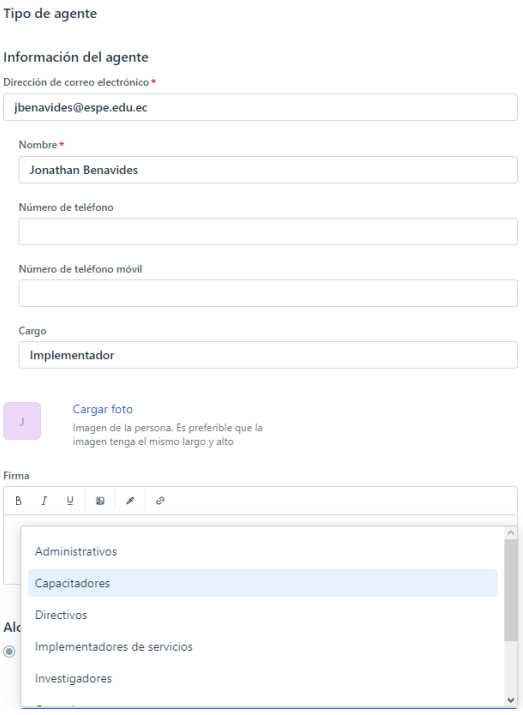
Grupos de trabajo CSIRT-ESPE



Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2020

Figura 49.

Registro de agentes CSIRT-ESPE

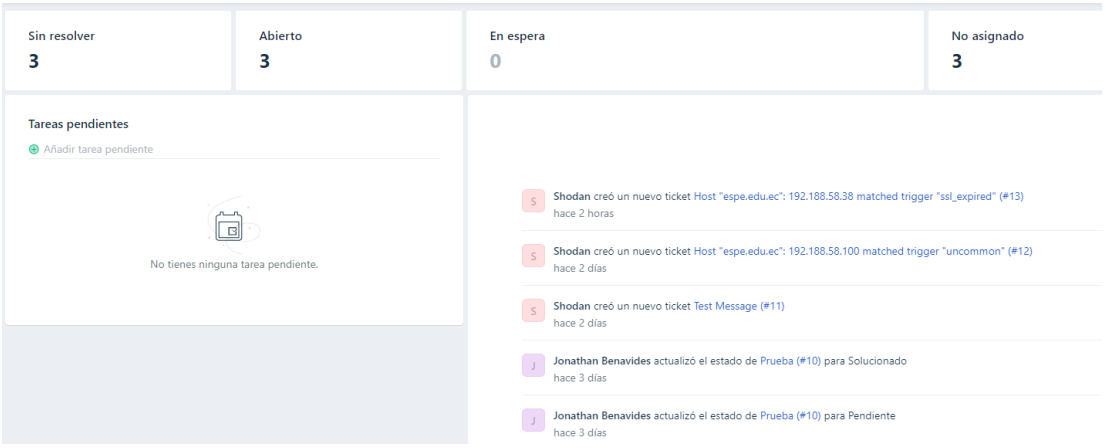


Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2020

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 50.

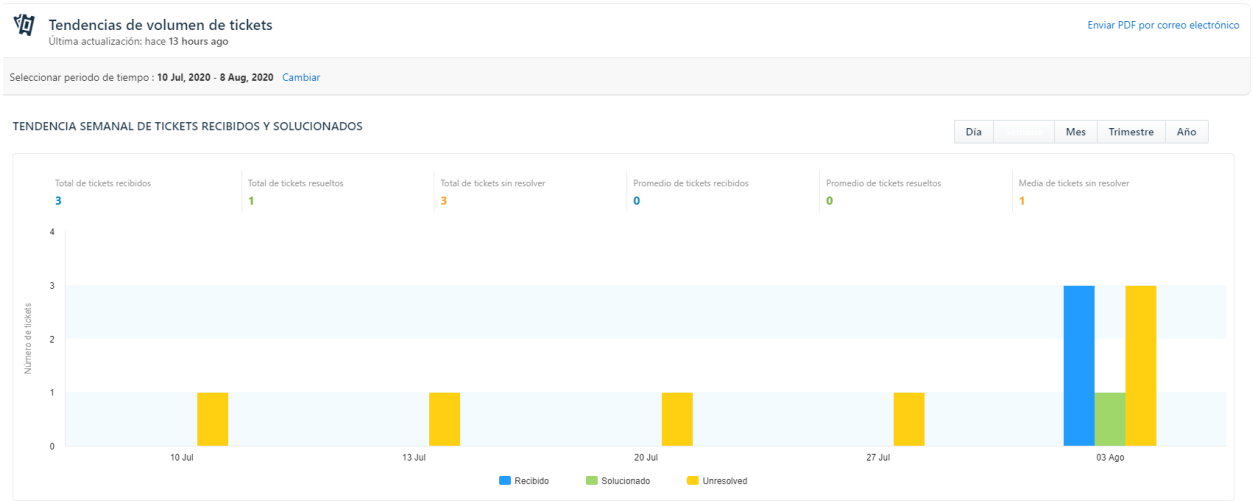
Dashboard principal de la gestión de tickets



Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2020

Figura 51.

Tendencia de volumen de solicitudes CSIRT-ESPE



Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2020.

Finalmente se configuro los contactos, proveedores y empresas que trabajan junto al CSIRT-ESPE.

Figura 52.

Contactos y empresas socias del CSIRT-ESPE

Contacto	Título	Empresa	Dirección de correo electrónico	Teléfono del trabajo
Andrés Castillo Changuán	Operador UTICs ESPE	UTICs ESPE	adcastillo@espe.edu.ec	- -
Enrique López	Especialista servidores	CSIRT-CEDIA	enrique.lopez@cedia.org.ec	- -
Ernesto Pérez	Coordinador CSIRT-CEDIA	CSIRT-CEDIA	ernesto.perez@cedia.org.ec	- -
Jonathan Benavides	- -	- -	jonabenavides91@hotmail.com	- -
Rommel Asitimbay Morales	Director Tecnologías de la Información y Comunicaciones.	UTICs ESPE	rdasitimbay@espe.edu.ec	- -
Shodan	Alertas Shodan	Shodan	no-reply@mg.shodan.io	- -

Nota. Tomado de *la web Freshdesk.com* por Freshdesk, 2020.

Gestión de versiones

El presente literal describe el historial de versiones de software que se usó en

los activos para que el servicio funcione correctamente (la tabla representa las versiones de los activos propios del aula H-402 más no de los servicios como Shodan y Freshdesk por ser servicios web).

Tabla 10.

Gestión de Versiones de Equipos

CIs	**Serie**	**Historial de Versiones**	**Fecha**	**Observaciones**
CPU Dell de escritorio	4591585	Kali Linux versión 2018.2	04-may-2020	Equipo sin mantenimiento
		Kali Linux versión 2018.2	05-may-2020	Actualización de lista de paquetes (apt-get update) e instalación de nuevas versiones de paquetes (apt-get upgrade).
		Instalación AnyDesk 5.5.6	05-may-2020	Se instaló AnyDesk para trabajar desde casa por causa de la pandemia del Covid-19.
CPU Dell de escritorio	4591586	Kali Linux versión 2018.2	04-may-2020	Equipo sin mantenimiento
		Kali Linux versión 2018.2	05-may-2020	Actualización de lista de paquetes (apt-get update) e instalación de nuevas versiones de paquetes (apt-get upgrade).
		Instalación AnyDesk 5.5.6	05-may-2020	Se instaló AnyDesk para trabajar desde casa por causa de la pandemia del Covid-19.
CPU Dell de escritorio	4591587	Kali Linux versión 2018.2	04-may-2020	Equipo sin mantenimiento
		Kali Linux versión 2018.2	05-may-2020	Actualización de lista de paquetes (apt-get update) e instalación de nuevas versiones de paquetes (apt-get upgrade).
		Instalación AnyDesk 5.5.6	05-may-2020	Se instaló AnyDesk para trabajar desde casa por causa de la pandemia del Covid-19.

CIs	Serie	Historial de Versiones	Fecha	Observaciones
CPU Dell de escritorio	4591588	Kali Linux versión 2018.2	04-may-2020	Equipo sin mantenimiento
		Kali Linux versión 2018.2	05-may-2020	Actualización de lista de paquetes (apt-get update) e instalación de nuevas versiones de paquetes (apt-get upgrade).
Servidor Asus	4592181	Partición Windows 10 con Kali Linux versión 2017.3	04-may-2020	Equipo dañado las particiones (sin mantenimiento)
		Actualización Kali Linux versión 2020.2	06-may-2020	Partición funcionando
		Instalación de Snort versión 3.0	07-may-2020	Instalación fallida por falta de soporte para Kali Linux 2020
		Formateo e instalación de Windows 10 en partición de 300GB	10-may-2020	Se reinstalo el sistema operativo por fallas en las particiones, se encontró excesivas particiones de disco duro
		Formateo e instalación de Centos 8 en partición de 700GB	15-may-2020	Se analizó instalar Centos 8 ya que cuenta con una interfaz gráfica que permite trabajar remotamente desde casa por causa de la pandemia del Covid-19

Validación y pruebas del servicio

El presente literal asegura que la configuración de la infraestructura 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 trazados en la puesta en marcha del nuevo servicio.

Para proceder a la validación y pruebas es necesario entender los servicios que Los servicios iniciales que prestará el CSIRT Académico de la ESPE los cuales se representan en la siguiente tabla:

Tabla 11.

Servicios iniciales CSIRT ESPE

Servicio	**Funciones**
Alertas y advertencias	Reportar incidente informático, sea una vulnerabilidad, malware o intrusión, entregando información detallada para que el administrador pueda corregir la falla.
Tratamiento de incidentes	Recomendar al administrador tomar acciones entregando soluciones. Seguimiento al incidente hasta ser resuelto
Análisis de incidentes	Analizar incidente y clasificarlos según su impacto e identificar su alcance y su naturaleza para dar soluciones. Entrega informe para dar soluciones.
Apoyo en la respuesta de incidentes	Entrega una guía remota o personal en la infraestructura afectada.
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 CSIRT para pedir soporte.

En la siguiente tabla se observa la validación de los activos según los servicios del CSIRT Académico; para cada servicio se valida las herramientas implementadas verificando si sus componentes son suficientes para dar solución y aportar al proceso.

Tabla 12.

Validación de herramientas.

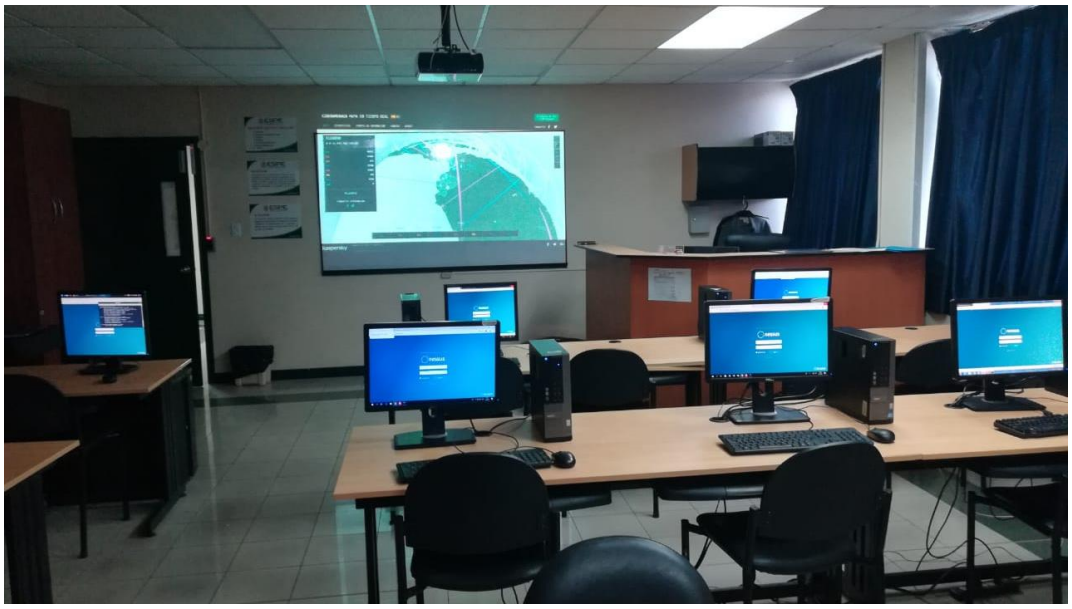
Servicio	Herramientas						Funciones de las herramientas
	Nessus	Nmap	FortiAnalizer	Shodan	AnyDesk	Freshdesk	
Alertas y advertencias	✓	✓	✓	✓	✓		Monitorear incidentes de seguridad
Tratamiento de incidentes					✓	✓	Gracias a software de tickets se puede gestionar el incidente hasta se resuelto
Análisis 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. También se evaluó el lugar físico para que este en óptimas condiciones para la siguiente fase de operación del servicio. En las siguientes figuras se observa la infraestructura adaptada

para el funcionamiento del CSIRT Académico ESPE.

Figura 53.

Infraestructura física CSIRT ESPE



Nota. *Laboratorio H-402 adaptado para operar el CSIRT-ESPE*

Figura 54.

Equipos de trabajo y monitoreo

Nota. Laboratorio H-402 adaptado para operar el CSIRT-ESPE (Área de equipos de operación)

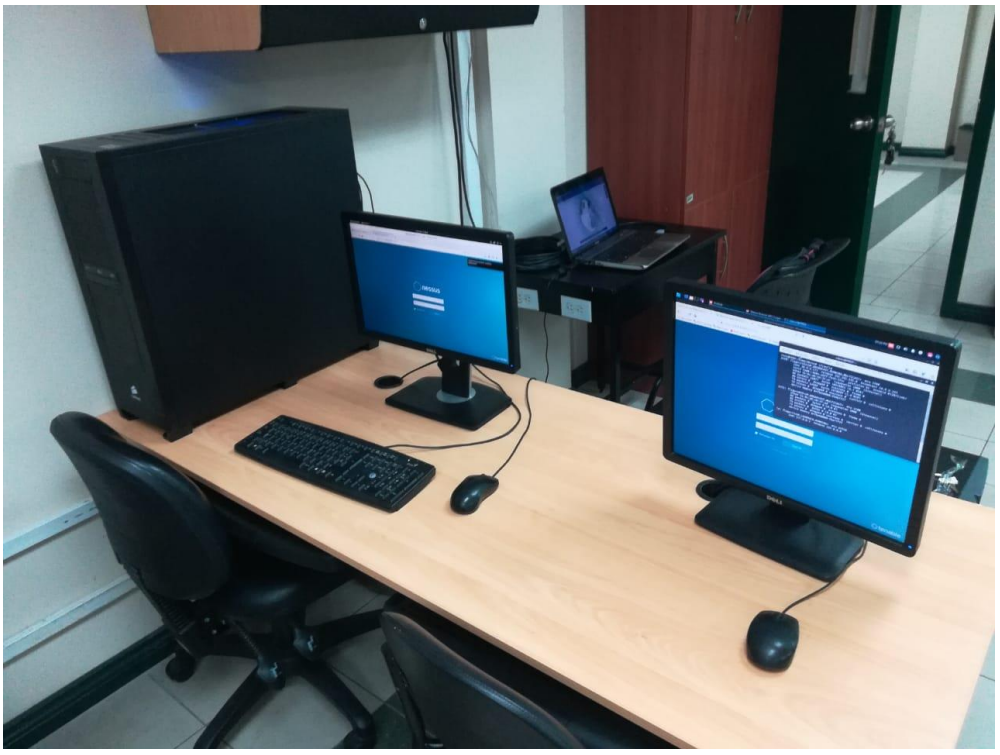
Figura 55.

Mesa de reuniones CSIRT ESPE

Nota. Laboratorio H-402 adaptado para operar el CSIRT-ESPE (Área de mesa de reuniones)

Figura 56.

Operación de servidores CSIRT ESPE



Nota. *Laboratorio H-402 adaptado para operar el CSIRT-ESPE (Área de servidores)*

Gestión de conocimiento

El presente literal 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 cerrada por la pandemia del Covid-19, por lo tanto, el personal deberá trabajar desde casa.

Tabla 13.

Personal	Equipo designado	Contacto	Rol
Mario Bernabe Ron Egas,	ID Anydesk: 670 633 572 IP: 10.9.9.198	3989400. Ext. 1902. **mbron@espe.edu.ec**	Director Capacitador, analista de incidentes y vulnerabilidades, gestión de proveedores, encargado de infraestructura, monitoreo de red.
Enrique Vinicio Enrique Carrera	ID Anydesk: 792 015 915 IP:10.9.9.94	3989400, Ext. 1880.	Monitoreo de vulnerabilidades y creación de informes, investigación.
Freddy Mauricio Tapia León	ID Anydesk: 578 194 526 IP: 10.9.9.242	3989400, Ext. 1934; fmtapia@espe.edu.ec	Monitoreo de vulnerabilidades y creación de informes, investigación
Recalde Herrera Luis Lenin	ID Anydesk: 728 537 443 IP: 10.9.9.201	3989400, Ext. 2562 llrecalde@espe.edu.ec	Monitoreo de vulnerabilidades y creación de informes, investigación
Alberto Daniel Núñez Agurto	-	3989400, Ext. 4940 adnunez1@espe.edu.ec	No es necesario designar un equipo ya que su rol es de investigador.
Walter Marcelo Fuertes Díaz	ID Anydesk: 484 765 549 IP:10.9.9.245	3989400, Ext. 1906. wmfuertes@espe.edu.ec	Gestión del CSIRT, Administrativo, Investigador.
Dr. Henry Omar Cruz Carrillo		3989400 Ext, 2510, hocruz@espe.edu.ec	No es necesario designar un equipo ya que su rol es de investigador.
Jonathan Francisco Benavides Cabascango	ID Anydesk: 195 505 247 IP: 10.9.9.194 ID Anydesk: 228 694 666 IP:10.9.9.173	jfbenavides@espe.edu.ec	Implementador de servicios, analista de incidentes, monitoreo de red, gestión de equipos e infraestructura, manejo de servidores.
Rommel Asitimbay	-	rdasitimbay@espe.edu.ec	Director UTICs ESPE

Capítulo IV

Introducción

Después de la configuración y puesta en marcha de las herramientas e infraestructura necesaria para dar inicio a la operación del servicio; el presente capitulo describe los procesos, lineamientos y políticas que sigue el CSIRT Académico ESPE para su operación, garantizando a los usuarios la protección de sus sistemas gracias a la combinación de herramientas, procesos y personal calificado para prevenir incidentes de seguridad de la información y disminuir riesgos.

Gestión de eventos

La definición de un evento hablando sobre la seguridad de la información es cualquier hecho u ocurrencia relacionada con algún dispositivo que puede o no comprometer sus niveles de riesgo. Para el caso de un CSIRT, los eventos deben ser categorizados según su importancia ya que no todos pueden presentar un problema a la institución. Para gestionar un evento el CSIRT Académico ESPE 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

La herramienta Nessus entrega información de forma pasiva, es decir es necesario que el usuario realice un escaneo a la red para que entregue logs e información sobre las ocurrencias que han pasado en los sistemas. El usuario puede escoger entre varios tipos de escaneo que proporciona Nessus entre los cuales están:

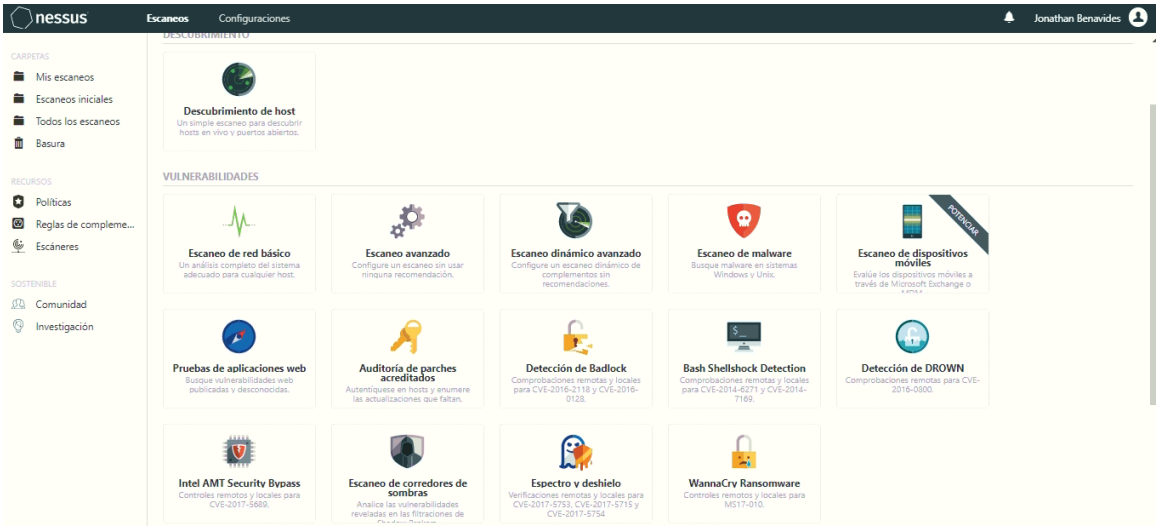
- Descubrimiento de host: Un simple escaneo para descubrir hosts en vivo y puertos abiertos.

- Escaneo de red básico: Un análisis completo del sistema adecuado para cualquier host.
- Escaneo avanzado: configuración avanzada de escaneo sin guía y recomendaciones.
- Escaneo dinámico avanzado: escaneo dinámico de complementos.
- Escaneo de malware: Busque malware en sistemas Windows y Unix.
- Escaneo de dispositivos móviles: Evaluación a través de Microsoft Exchange o MDM.
- Pruebas de aplicaciones web: Buscar vulnerabilidades web publicadas y desconocidas.
- Auditoría de parches acreditados: Búsqueda de actualizaciones importantes
- Bash Shellshock Detection: Comprobaciones remotas y locales para CVE-2014-6271 y CVE-2014-7169.
- Detección de DROWN: 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: Controles remotos y locales para MS17-010.
- Auditoría de la infraestructura de la nube: Auditar la configuración de servicios en la nube de terceros.
- Escaneo interno de red PCI: Realice un análisis de vulnerabilidades interno de PCI DSS (11.2.1).
- Auditoría de configuración de MDM: Auditar la configuración de los administradores de dispositivos móviles.

- Auditoría de configuración sin conexión: Auditar la configuración de dispositivos de red.

Figura 57.

Tipos de escaneo en Nessus.

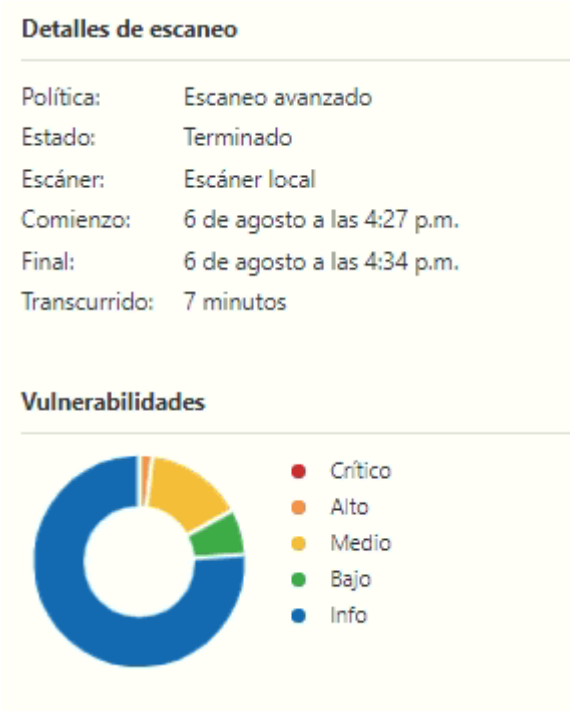


Nota. Dashboard para un escaneo en Nessus.

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

Figura 58.

Resultados de escaneo Nessus

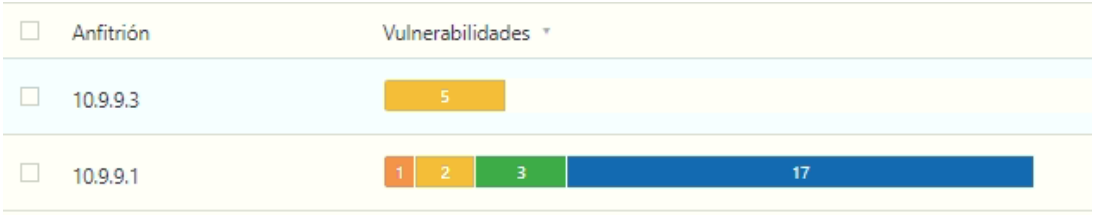


Nota. *Detalles de escaneo en Nessus.*

La herramienta también divide los escaneos según los hosts encontrados, categorizando los resultados en crítico, alto, medio, bajo e informativo, indicando información detallada para que el operador pueda analizar y determinar si se trata de un incidente o un evento sin riesgo para la institución.

Figura 59.

Resultados de escaneo según el host



Nota. Resultados del escaneo divido por host encontrados.

Figura 60.

Detalles del escaneo por host

Nota. Detalles de vulnerabilidades encontradas en un host.

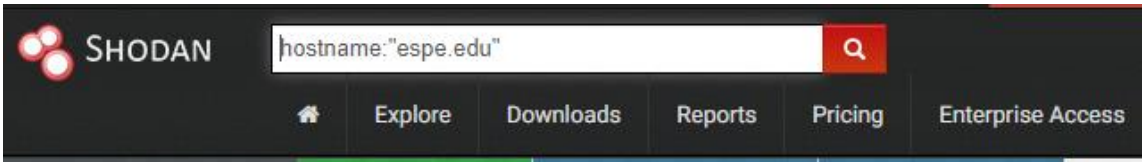
Eventos de Shodan

Shodan es un buscador de dispositivos que se encuentran conectados a internet en todas partes del mundo, se pueden encontrar servidores, cámaras, computadoras, dispositivos médicos, IoT, y todo aparato que pueda conectarse a internet. Los tipos de eventos que recopila dicha herramienta son pasivos y activos; pasivos gracias al buscador que permite revisar los servicios y vulnerabilidades de los dispositivos, y activos al monitorear en tiempo real las vulnerabilidades de los equipos que el usuario determino previamente.

El CSIRT Académico ESPE usa este tipo de eventos para determinar riesgos en la institución y entregar una solución oportuna ante algún fallo de seguridad. En el caso del buscador el usuario tiene que ingresar filtros y cadenas de caracteres para encontrar sus objetivos:

Figura 61.

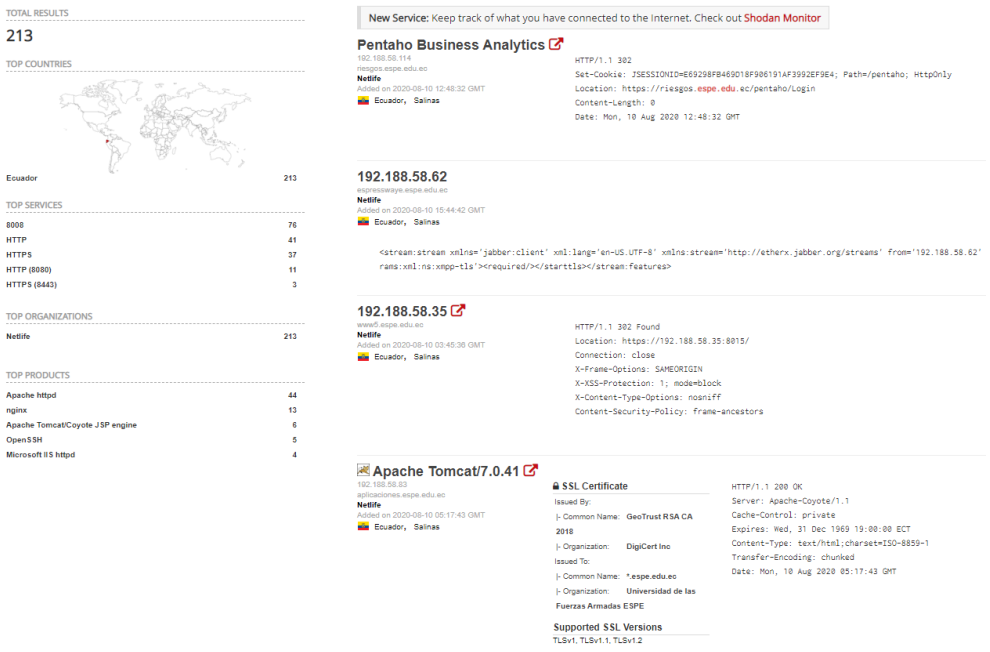
Ejemplo de búsqueda en Shodan



Nota. Tomado de *shodan.io* por Shodan, 2020.

Figura 62.

Resultado de búsqueda en Shodan

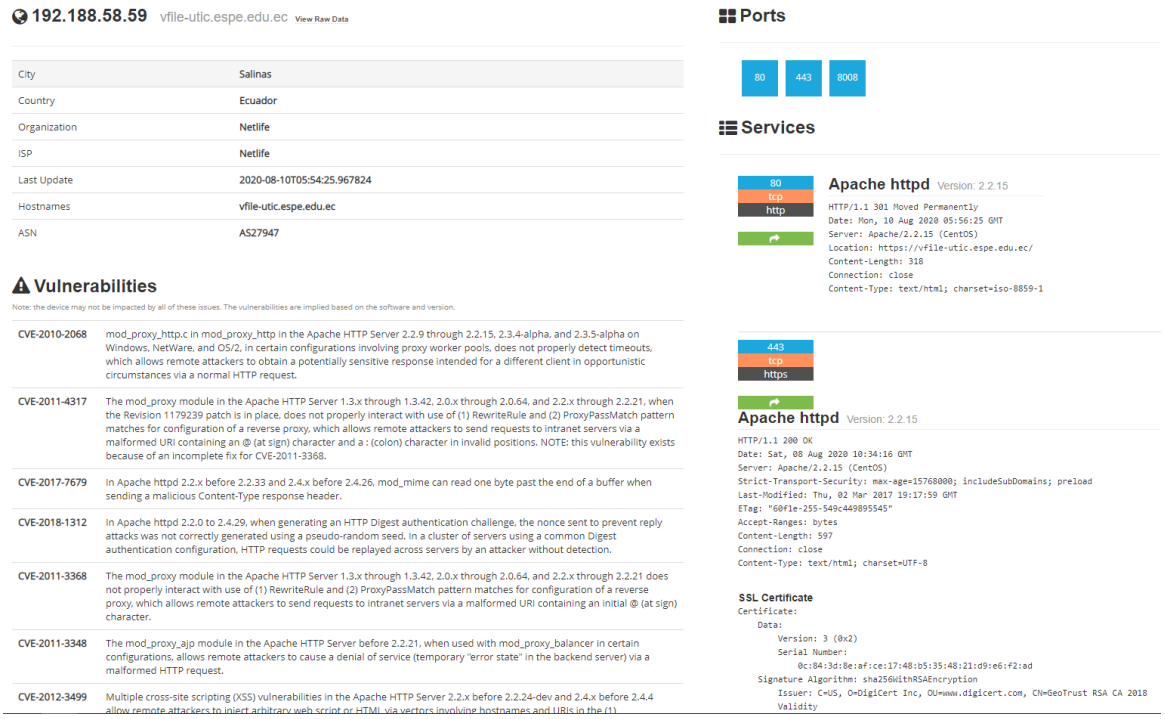


Nota. Tomado de *shodan.io* por Shodan, 2020.

El personal del CSIRT académico realiza búsquedas en base a lo solicitado y Shodan presenta 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 63.

Detalle de búsqueda en Shodan

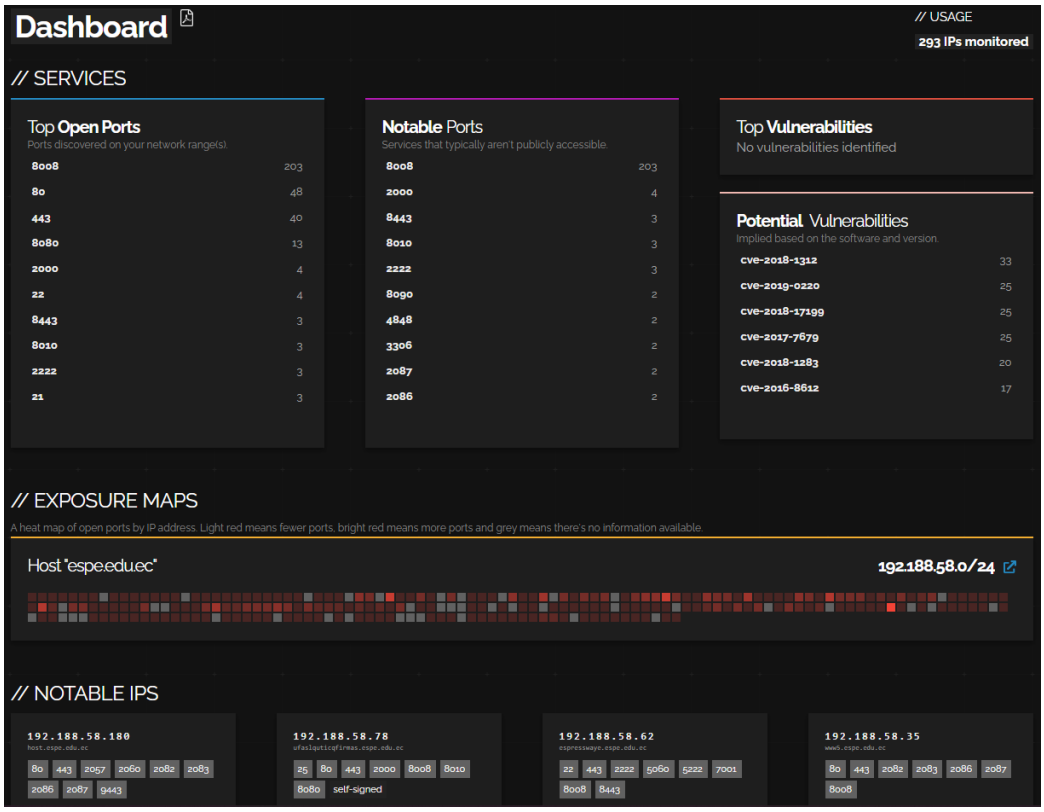


Nota. Tomado de *shodan.io* por Shodan, 2020.

Esta herramienta también permite monitorear 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, en el caso del CSIRT-ESPE se ha optado por analizar las IP correspondientes al hostname “espe.edu.ec”.

Figura 64.

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

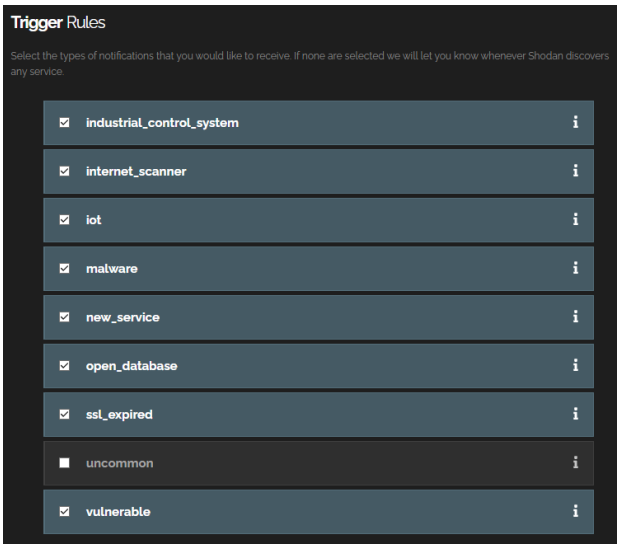


Nota. Dashboard de monitoreo en tiempo real del hostname “espe.edu.ec”. Tomado de *shodan.io* por Shodan, 2020.

La herramienta reporta varios tipos de eventos los cuales son configurados en las reglas de activación que sirven como filtros para determinar las alertas al usuario.

Figura 65.

Reglas de activación de alertas Shodan

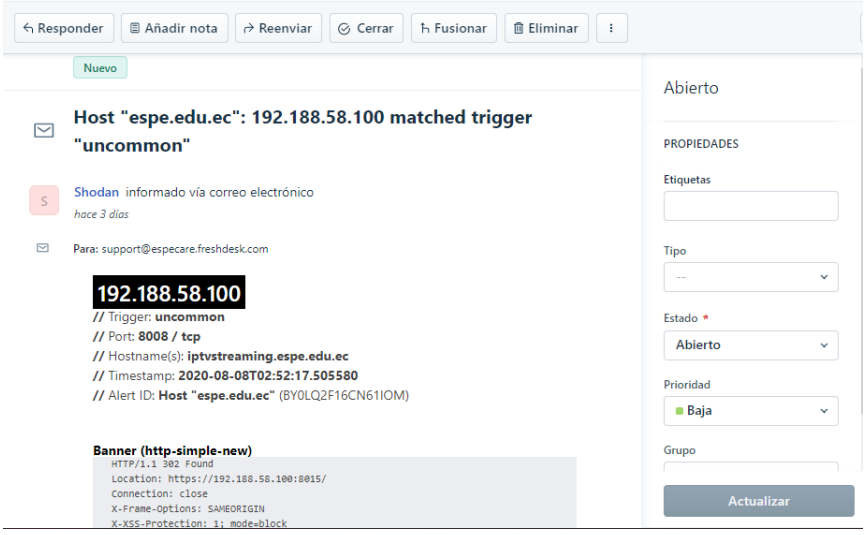


Nota. La figura representa los tipos de eventos seleccionado para dar alertas. Tomado de *shodan.io* por Shodan, 2020.

Las alertas son enviadas vía correo electrónico para que el operador pueda analizar y determinar si se trata de un incidente. La alerta está configurada para que llegue al correo electrónico de soporte y se genere un ticket automáticamente.

Figura 66.

Recepción de alertas Shodan en el correo electrónico



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

Eventos FortiAnalyzer

La visualización de eventos en tiempo real que provee el FortiAnalyzer integrado en la red de la ESPE es completo ya que divide el tráfico de la red por resumen de amenazas, destino, origen, países, vulnerabilidades, host comprometidos, eventos, aplicaciones y reglas aplicadas por el firewall.

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

Figura 67.

Amenazas bloqueadas en tiempo real

#	Threat	Category	CVE ID	Threat Level	Threat Score(Blocked/ Allowed)	Incidents(Blocked/ Allowed)
1	udp_flood	IPS		Critical	850	17
2	PHPUnit.Eval-stdin.PHP.Remote.Code.Ex...	IPS	CVE-2017-9841	Critical	150	3
3	Dasan.GPON.Remote.Code...	IPS	CVE-2018-10561 , CVE-2018-10562	Critical	50	1
4	exmaple[dot]com	Entertainment		High	359,310	11,977
5	Blocked Connection Attempts	Blocked by Firewall Policy		High	262,140	8,738
6	play[dot]google[dot]com	Freeware and Software Downloads		High	107,730	3,591
7	mqtt-mini[dot]facebook[dot]com	Social Networking		High	58,020	1,934
8	edge-mqtt[dot]facebook[dot]com	Social Networking		High	38,970	1,299
9	agafurretor[dot]com	Malicious Websites		High	37,020	617
10	android.prod.cloud.netflix.c...	Listas Negras		High	29,640	988

Total logs stored for analytics: 181 days 5 hours. Show 100 Total 386

Figura 68.

División de tráfico por países

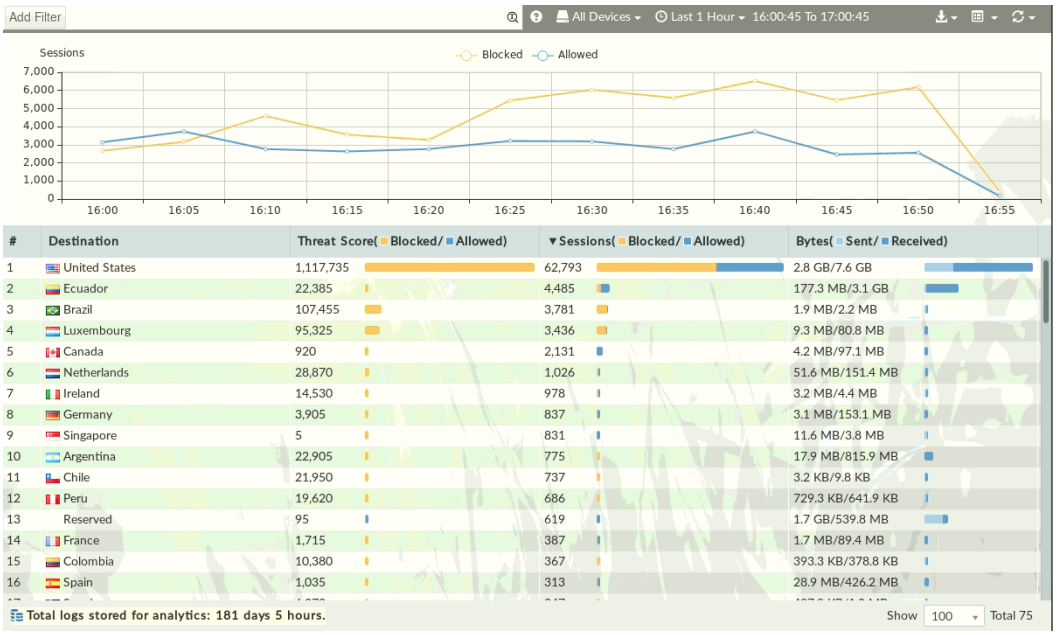


Figura 69.

Hosts infectados en tiempo real

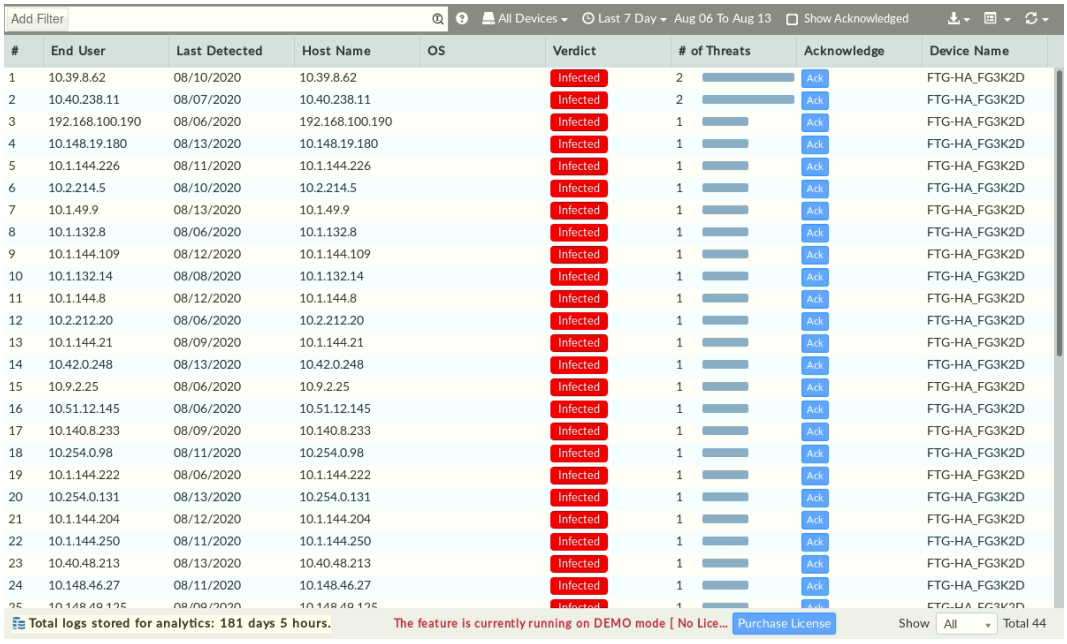
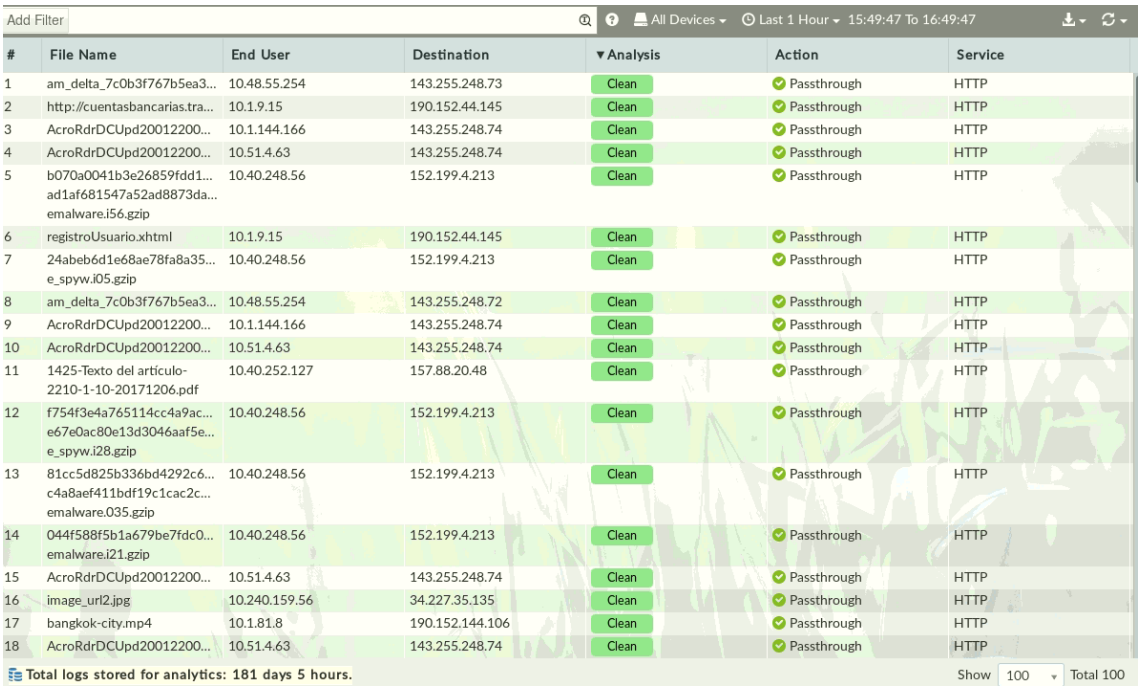


Figura 70.

Conexiones positivas



Add Filter | All Devices | Last 1 Hour | 15:49:47 To 16:49:47

#	File Name	End User	Destination	Analysis	Action	Service
1	am_delta_7c0b3f767b5ea3...	10.48.55.254	143.255.248.73	Clean	Passthrough	HTTP
2	http://cuentasbancarias.tra...	10.1.9.15	190.152.44.145	Clean	Passthrough	HTTP
3	AcroRdrDCUpd20012200...	10.1.144.166	143.255.248.74	Clean	Passthrough	HTTP
4	AcroRdrDCUpd20012200...	10.51.4.63	143.255.248.74	Clean	Passthrough	HTTP
5	b070a0041b3e26859fdd1... ad1af681547a52ad8873da... emalware.i56.gzip	10.40.248.56	152.199.4.213	Clean	Passthrough	HTTP
6	registroUsuario.xhtml	10.1.9.15	190.152.44.145	Clean	Passthrough	HTTP
7	24abeb6d1e68ae78fa8a35... e_spyw.i05.gzip	10.40.248.56	152.199.4.213	Clean	Passthrough	HTTP
8	am_delta_7c0b3f767b5ea3...	10.48.55.254	143.255.248.72	Clean	Passthrough	HTTP
9	AcroRdrDCUpd20012200...	10.1.144.166	143.255.248.74	Clean	Passthrough	HTTP
10	AcroRdrDCUpd20012200...	10.51.4.63	143.255.248.74	Clean	Passthrough	HTTP
11	1425-Texto del artículo-2210-1-10-20171206.pdf	10.40.252.127	157.88.20.48	Clean	Passthrough	HTTP
12	f754f3e4a765114cc4a9ac... e67e0ac80e13d3046aaf5e... e_spyw.i28.gzip	10.40.248.56	152.199.4.213	Clean	Passthrough	HTTP
13	81cc5d825b336bd4292c6... c4a8aef411bdf19c1cac2c... emalware.035.gzip	10.40.248.56	152.199.4.213	Clean	Passthrough	HTTP
14	044f588f5b1a679be7fdc0... emalware.i21.gzip	10.40.248.56	152.199.4.213	Clean	Passthrough	HTTP
15	AcroRdrDCUpd20012200...	10.51.4.63	143.255.248.74	Clean	Passthrough	HTTP
16	image_url2.jpg	10.240.159.56	34.227.35.135	Clean	Passthrough	HTTP
17	bangkok-city.mp4	10.1.81.8	190.152.144.106	Clean	Passthrough	HTTP
18	AcroRdrDCUpd20012200...	10.51.4.63	143.255.248.74	Clean	Passthrough	HTTP

Total logs stored for analytics: 181 days 5 hours. Show 100 Total 100

Nota. La figura representa las conexiones exitosas desde la red de la ESPE a internet, esto no significa que las conexiones son legítimas, el CSIRT-ESPE debe realizar monitorización y análisis para comprobar que los eventos son correctos y no vulneran algún sistema.

Figura 71.

Destinos comunes.

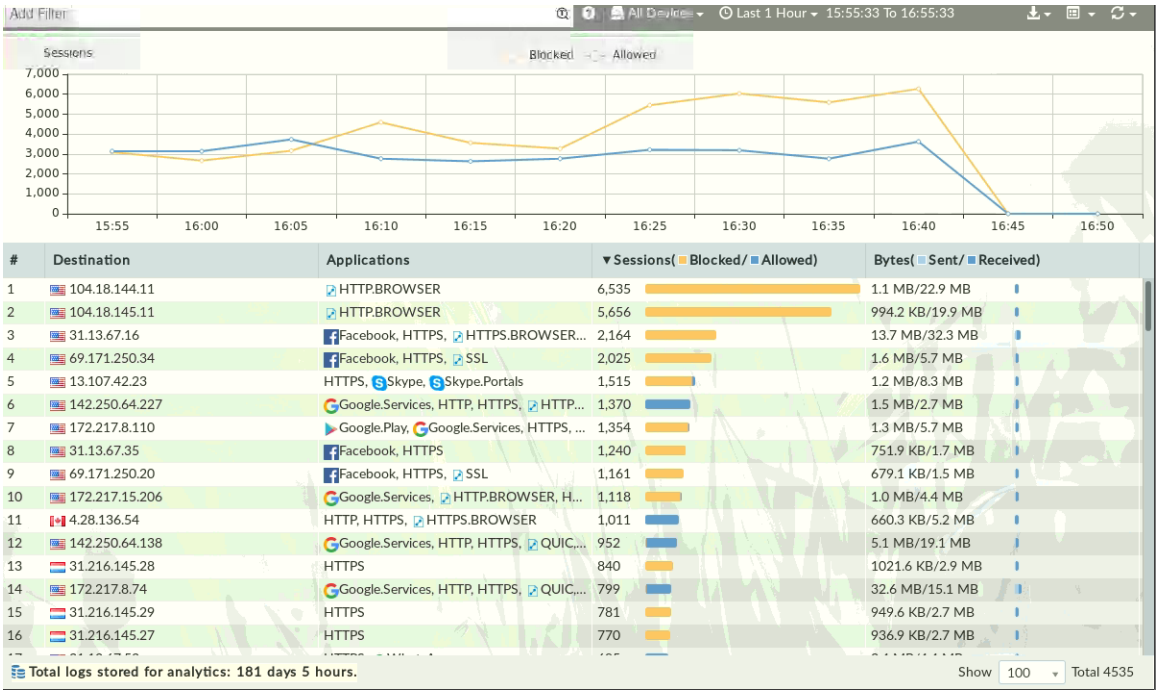


Figura 72.

Conexiones aceptadas por el firewall

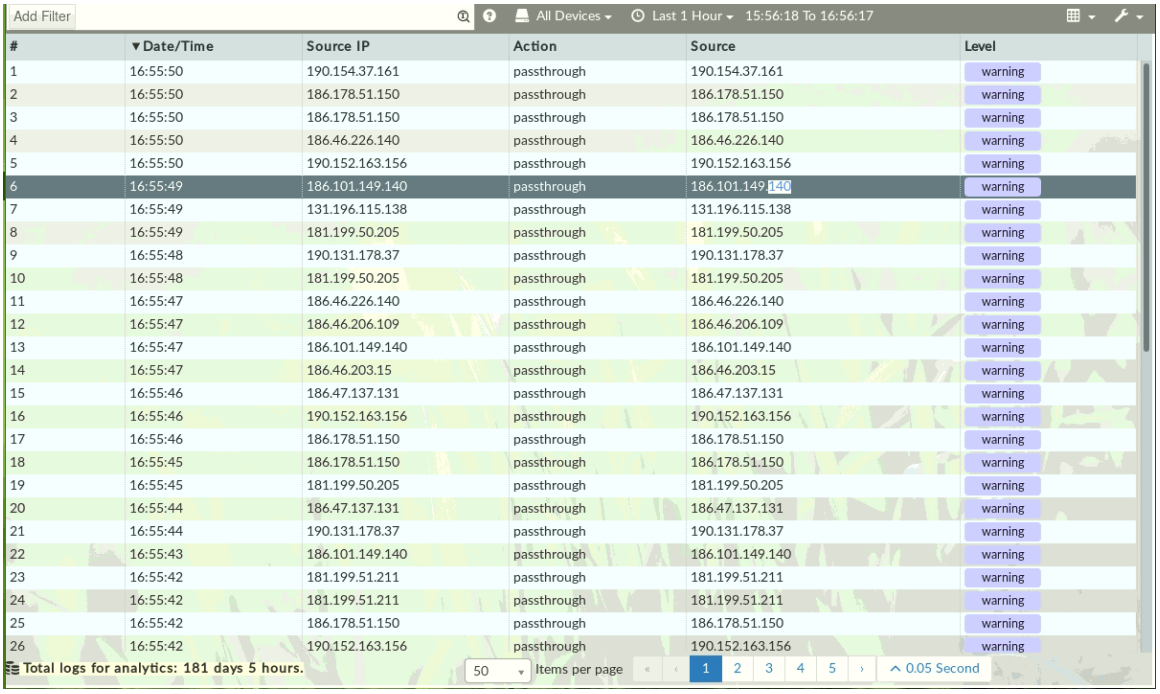
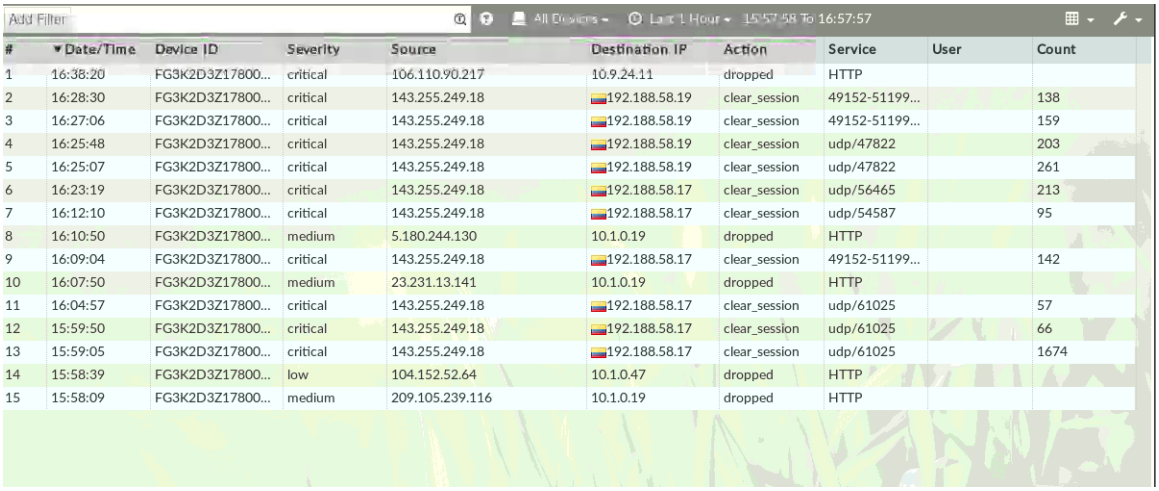


Figura 73.

Trafico bloqueado por el IPS incluido en los equipos Fortinet



Add Filter | All Devices | Last 1 Hour | 15:57:58 To 16:57:57

#	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		

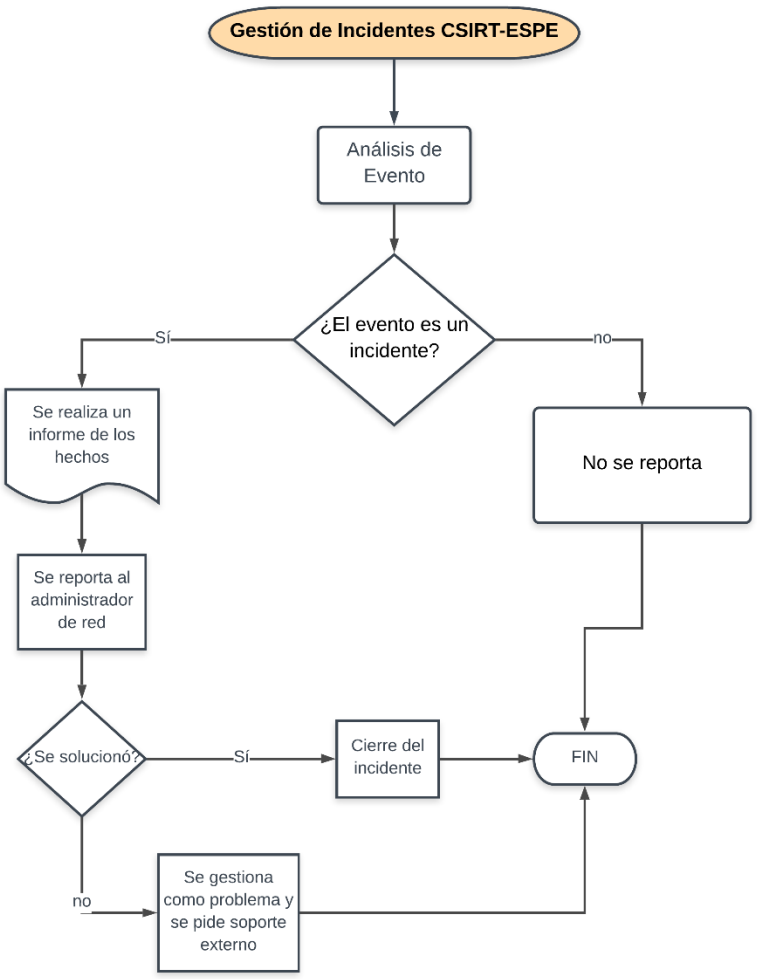
Gestión de Incidencias

El proceso de Gestión de Incidencias se basa en el análisis previo de un evento, es decir uno o varios eventos son considerados un incidente cuando perjudican o comprometen la seguridad de la información de la institución.

Para Gestionar un Incidente el personal del CSIRT-ESPE necesita hacer un análisis previo de los eventos que las herramientas de seguridad informática proveen. La siguiente figura es un diagrama de procesos que describe los pasos que lleva a cabo un operador del CSIRT para la Gestión de una Incidencia.

Figura 74.

Diagrama de procesos para gestionar un incidente

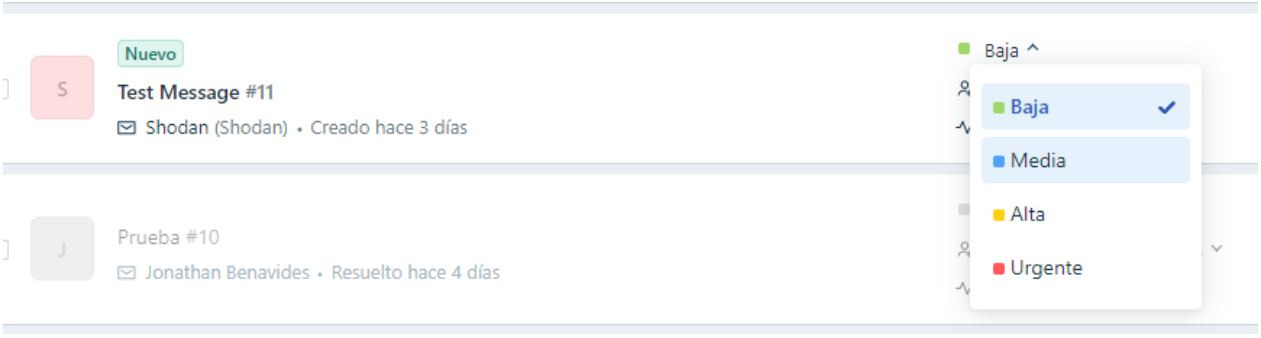


Nota. Elaboración propia.

Se puede llevar a cabo la gestión de un incidente cuando el cliente haga una solicitud en el portal https://especare.freshdesk.com/support/home o cuando el operador encuentre algún incidente dentro de las herramientas Shodan, Nessus, FortiAnalyzer. 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 75.

Categorización de un incidente

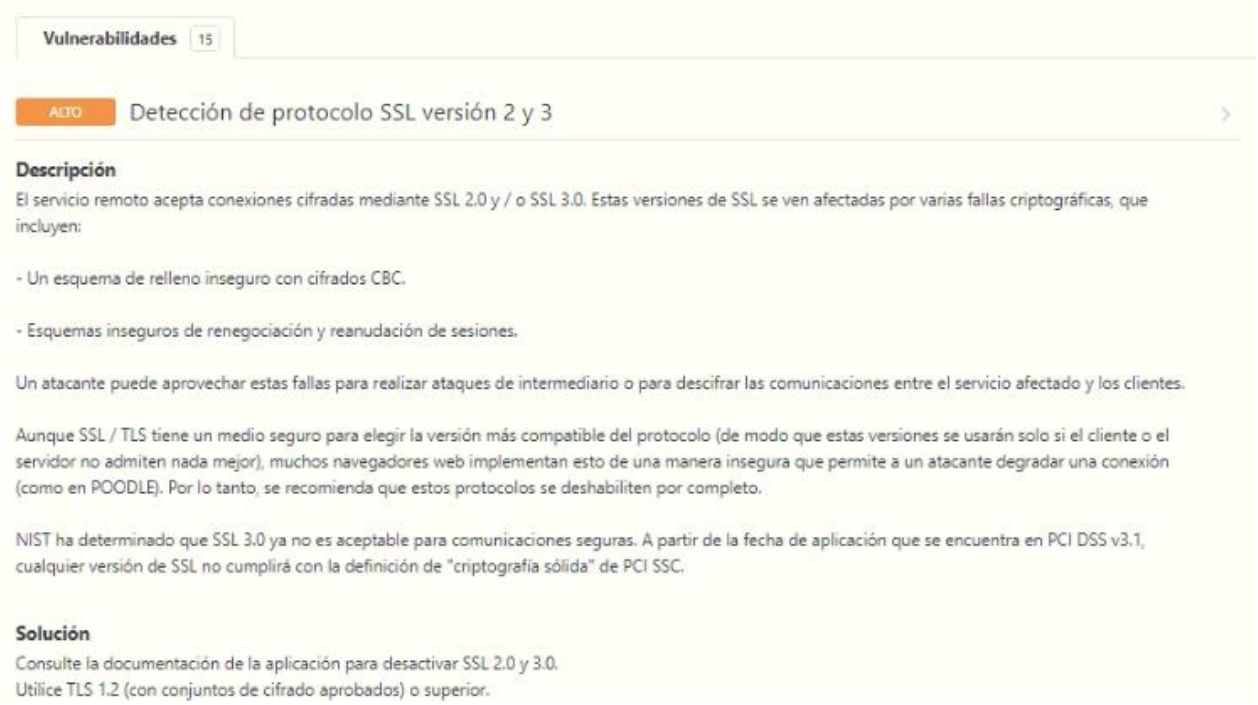


Nota. La figura indica la categorización del incidente en el portal CSIRT-ESPE de tickets seleccionando las opciones baja, media, alta y urgente

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 76.

Ejemplo de entrega de información de Nessus

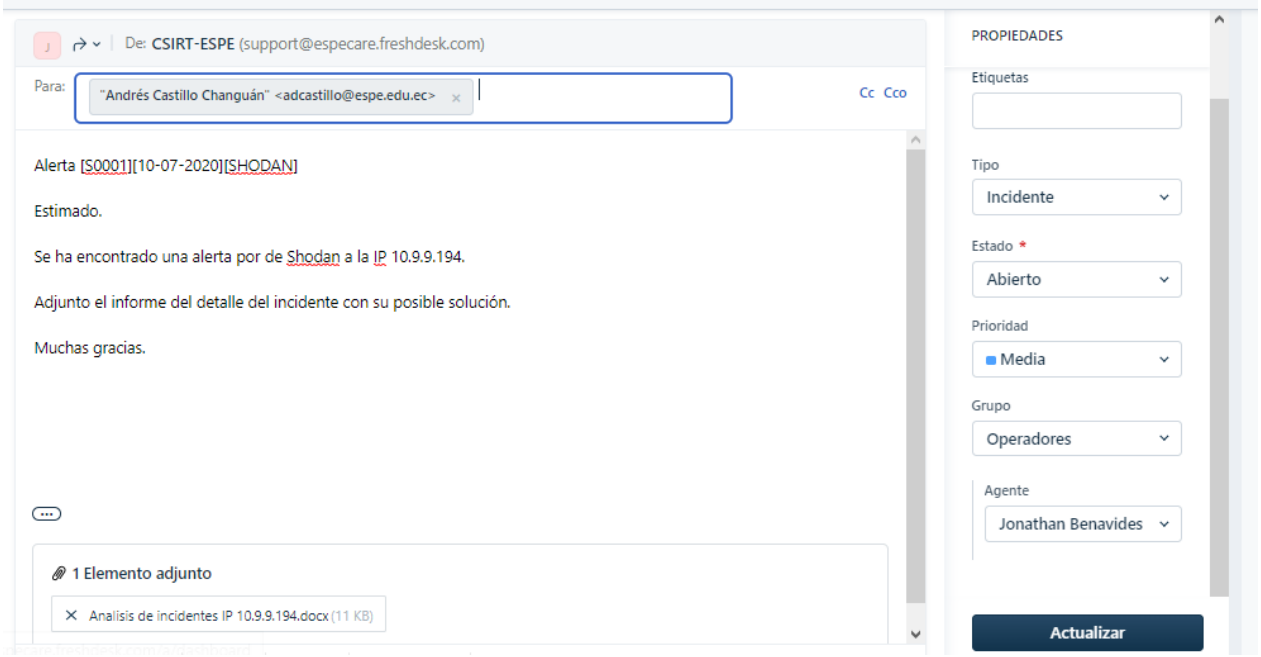


Nota. La figura representa un ejemplo del resultado que arroja la herramienta Nessus sobre una vulnerabilidad encontrada.

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. El informe es enviado vía correo electrónico al administrador de la infraestructura TI de la institución para dar solución al incidente. Este informe también sirve para ser documentado dentro de las bases de datos del CSIRT-ESPE para tener respaldo ante cualquier necesidad.

Figura 77.

Ejemplo de correo electrónico para alertas de un incidente

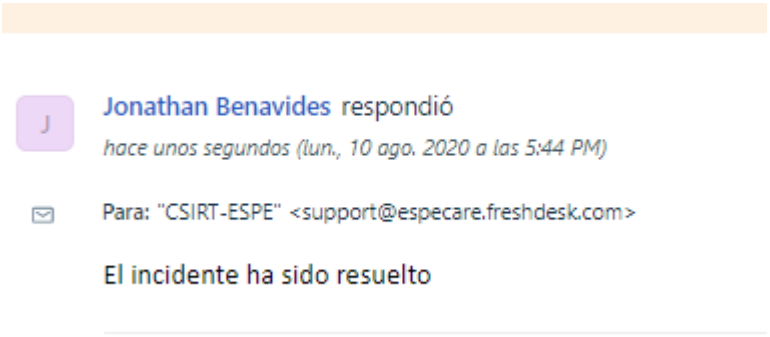


Nota. La figura es un ejemplo de correo electrónico enviado al administrador de la infraestructura TI para alertar un incidente.

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 78.

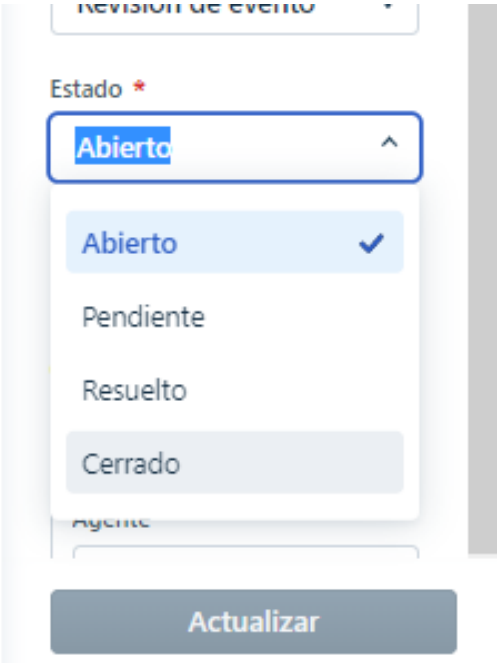
Ejemplo de respuesta del administrador de red



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 por el personal del CSIRT-ESPE.

Figura 79.

Resolución y cierre de un incidente



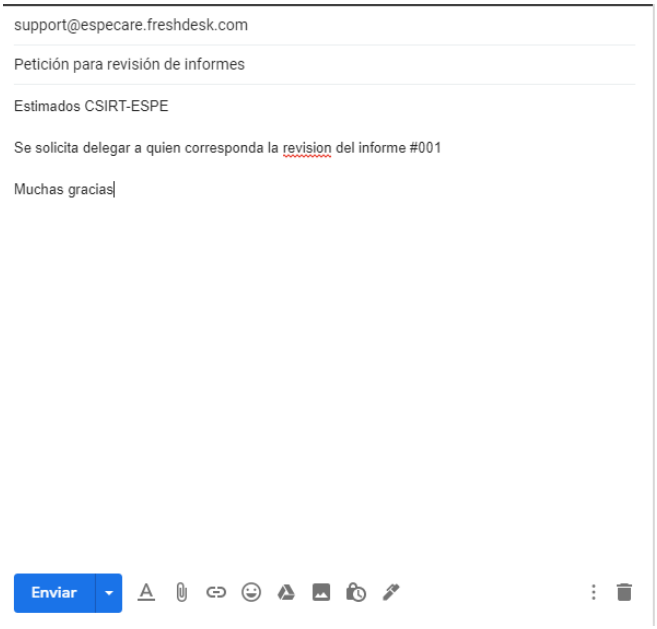
Nota. La figura representa el cierre del incidente después que el administrador de la

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 electrónico support@especare.freshdesk.com o mediante el portal https://especare.freshdesk.com/support/home.

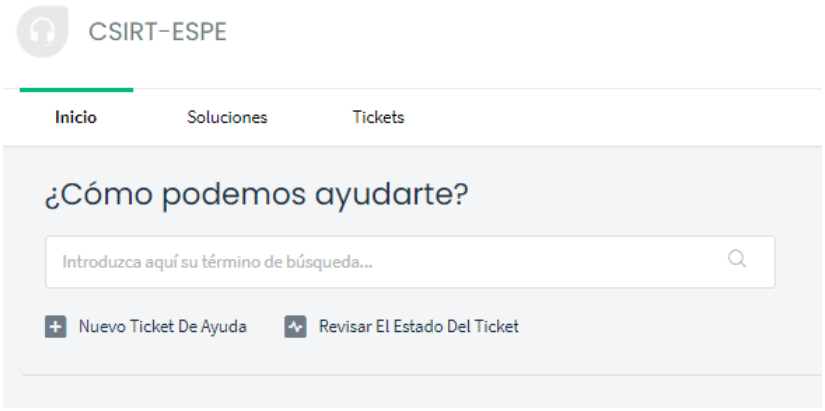
Figura 80. Ejemplo de petición al correo electrónico CSIRT-ESPE



Nota. La figura indica un ejemplo de petición de un cliente al personal del CSIRT.ESPE.

Figura 81.

Ejemplo de petición al portal CSIRT-ESPE

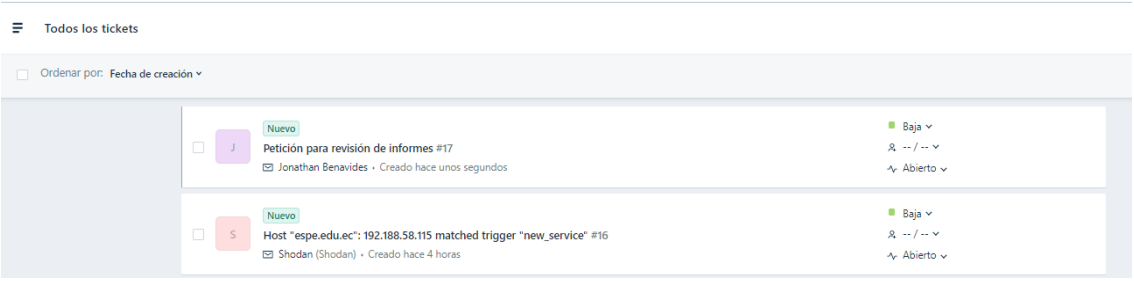


Nota. La figura indica que el portal del CSIRT-ESPE cuenta con un botón para generar un ticket o una petición.

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

Figura 82.

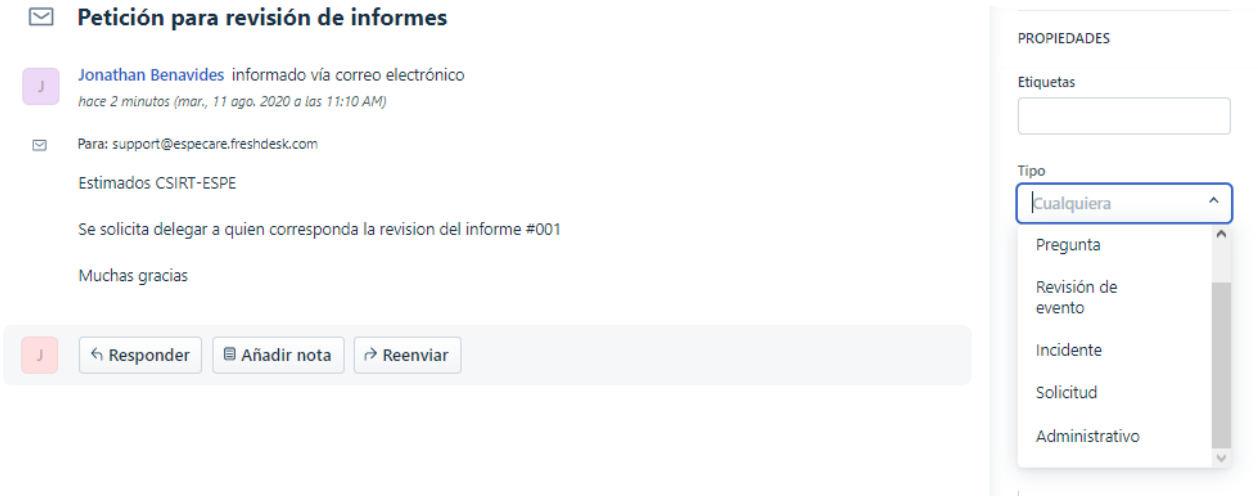
Recepción de petición del cliente



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

Figura 83.

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, en este caso el CSIRT-ESPE optará por buscar información y soporte en otros CSIRT socios (CEDIA, CSIRT-EPN, CSIRT- Universidad de la Plata, EcuCERT). Para este caso es importante no enviar información crítica de la universidad ya que sería una violación a la seguridad de la información.

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 CSIRT-ESPE, intentando proteger los sistemas implementados dando autorización para el mantenimiento y administración solo al personal de directivos e implementadores.

Tabla 14.

Gestión de Accesos al personal CSIRT-ESPE

Personal	Herramienta	Acceso
Mario Bernabé Ron Egas,	Shodan	Administrador
	FortiAnalyzer	Visualización
	Nessus	Administrador del sistema
	Freshdesk	Agente
Enrique Vinicio Enrique Carrera	Shodan	Visualización
	FortiAnalyzer	Visualización
	Nessus	Standard
	Freshdesk	Agente
Freddy Mauricio Tapia León	Shodan	Visualización
	FortiAnalyzer	Visualización
	Nessus	Standard
	Freshdesk	Agente
Recalde Herrera Luis Lenin	Shodan	Visualización
	FortiAnalyzer	Visualización
	Nessus	Standard
	Freshdesk	Agente
Alberto Daniel Núñez Agurto	Shodan	Visualización
	FortiAnalyzer	Visualización
	Nessus	Standard
	Freshdesk	Agente
Walter Marcelo Fuertes Díaz	Shodan	Visualización
	FortiAnalyzer	Visualización

Personal	Herramienta	Acceso
Dr. Henry Omar Cruz Carrillo	Nessus	Administrador del sistema
	Freshdesk	Agente
	Shodan	Visualización
	FortiAnalyzer	Visualización
Jonathan Francisco Benavides Cabascango	Nessus	Standard
	Freshdesk	Agente
	Shodan	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 CSIRT-ESPE 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 y el mundo está cuarentena por el virus del Covid-19 y la universidad se encuentra cerrada, siendo esta razón para adaptar la tecnología a un manejo remoto y ser administrada desde casa.

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 CSIRT-ESPE tomando en cuenta la propuesta realizada por (De la Torre Moscoso & Parra Rosero, 2018) en el diseño y estrategia del CSIRT Académico ESPE.

Tabla 15.

Gestión de operaciones TI

Nombre	Rol	Funciones
Ing. Mario Bernabé Ron Egas	Director General	- Organizar roles. - Aprobar actividades del CSIRT. - 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.
	Analista de servicios especiales	- Localizar vulnerabilidades. - Análisis técnico de software y hardware para el CSIRT. - 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.
Jonathan Francisco Benavides Cabascango	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.

Nombre	Rol	Funciones
		- Implementar infraestructura para nuevos servicios.
Freddy Mauricio Tapia León	Miembro del Comité de Tecnología	- Asesorar cambios en el CSIRT-ESPE- - Recomendar actividades. - Asesorar en políticas del CSIRT. - Asistencia a la dirección. - Trámites administrativos.
	Investigador	- Planificar y diseñar proyectos de investigación. - Publicar investigaciones sobre el CSIRT-ESPE. - Elaboración de artículos científicos.
Recalde Herrera Luis Lenin	Miembro del Comité de Tecnología	- Asesorar cambios en el CSIRT-ESPE- - Recomendar actividades. - Asesorar en políticas del CSIRT. - Asistencia a la dirección. - Trámites administrativos.
	Investigador	- Planificar y diseñar proyectos de investigación. - Publicar investigaciones sobre el CSIRT-ESPE. - Elaboración de artículos científicos.
Alberto Daniel Núñez Agurto	Investigador	- Planificar y diseñar proyectos de investigación. - Publicar investigaciones sobre el CSIRT-ESPE. - Elaboración de artículos científicos.
Dr. Henry Omar Cruz Carrillo	Investigador	- Planificar y diseñar proyectos de investigación. - Publicar investigaciones sobre el CSIRT-ESPE. - Elaboración de artículos científicos.
Walter Fuertes Díaz	Investigador	- Planificar y diseñar proyectos de investigación. - Publicar investigaciones sobre el CSIRT-ESPE. - Elaboración de artículos científicos.

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

Políticas del CSIRT académico ESPE

Las políticas del CSIRT Académico ESPE están fundamentadas en el informe titulado “Buenas Prácticas para establecer un CSIRT nacional” de (Organización de los Estados Americanos, 2016) ya que presenta en forma resumida los lineamientos que debe tener un CSIRT para su buen funcionamiento basados en FIRST.

Las políticas del CSIRT-ESPE pretenden entregar directrices para que se garantice el buen funcionamiento del ciclo de vida normal del servicio, entregando al cliente confidencialidad, disponibilidad e integridad de los sistemas y servicios de seguridad de la información que entregue el CSIRT-ESPE. Estas también sirven para detallar las funciones del CSIRT al personal y a los clientes para causar confianza en ellos y dejar claro la calidad del tipo de servicio que se ofrece

Las políticas mínimas indispensables para ser considerado como un CSIRT según FIRST son las siguientes:

- **De categorización de información:** El personal del CSIRT-ESPE debe categorizar la información basados en sus niveles de importancia.
    - En el caso de que el personal necesite enviar información confidencial por correo electrónico, este deberá ser cifrado.
- **De protección de datos:** El CSIRT-ESPE garantiza la protección de datos críticos.
    - Es responsabilidad del personal del CSIRT-ESPE el uso adecuado de los datos obtenidos por las herramientas.
    - Los datos obtenidos por el CSIRT-ESPE son confidenciales y deben ser usados exclusivamente en las actividades propias del CSIRT.
    - La información obtenida por las herramientas no es de uso

comunitario y no deben ser usadas por algún interés personal.

- Si el personal hace uso de dispositivos ajenos a la institución, no podrá guardar información privada del CSIRT-ESPE en dicho dispositivo.
- Se realizará la creación de cuentas para el uso de herramientas al personal que haya firmado un acuerdo de confidencialidad.
- Si cualquier miembro del personal hace uso indebido de los activos tecnológicos y de su información, se notificará a las autoridades competentes para los fines legales respectivos.
- Se limita el uso e ingreso a los activos tecnológicos a personas externas del CSIRT-ESPE.

- **De retenimiento de información:** El CSIRT-ESPE define el tiempo que debe mantener una información o registro guardado.
  - Si algún miembro del personal es separado de sus funciones, las cuentas y claves de usuario serán desactivadas dentro de 3 días laborales.
- **De destrucción de información:** Política de destrucción de información, registros, activos, etc., para garantizar la protección de datos cuando algún servicio o dispositivo llegue a su fin.
  - El personal que cuente con información confidencial sin autorización deberá informar a la dirección para destruirla mediante los procesos establecidos para la destrucción de información.
- **De revelación de información:** Como y cuando el CSIRT-ESPE puede distribuir información al personal externo, interno, proveedores y clientes.
  - El personal del CSIRT-ESPE debe hacer uso exclusivo del correo

propio del CSIRT para revelar o entregar información.

- El uso del correo electrónico del CSIRT-ESPE es exclusivo de su personal con el fin de realizar actividades propias del CSIRT.

- **De acceso a información:** Analiza los permisos de acceso del personal a la infraestructura TI y a la información crítica del CSIRT-ESPE, tomando en cuenta la comunidad a quien da sus servicios.
  - Es considerado un activo tecnológico cuando: el hardware, software, equipos informáticos, servidores, infraestructura de red consten en el inventario institucional de la ESPE.
  - Es propiedad de la Universidad de las Fuerzas Armadas toda información obtenida de dichos activos tecnológicos excluyendo la información personal de los trabajadores.
  - Los usuarios y claves de acceso son intransferibles.
- **Del uso apropiado de las herramientas:** Define la forma y el uso que se da a la infraestructura TI configurada para el CSIRT-ESPE.
  - Es responsabilidad del personal del CSIRT-ESPE el uso adecuando de las herramientas y activos tecnológicos.
  - El uso de las herramientas y activos tecnológicos se utilizarán exclusivamente para interés de la institución.
  - El personal del CSIRT-ESPE deberá gestionar la protección de los activos tecnológicos con el fin de proteger las herramientas en contra de robo, daño o a accidentes.
  - Los dispositivos que presenten malware deberán ser desconectados de la red hasta darlos mantenimiento.
  - Si el personal usa equipos ajenos a la institución, el CSIRT-ESPE no

se responsabiliza por daños o infección de malware de los mismos.

    - Se eliminará cuentas de usuario si se detecta el mal uso de las herramientas.

- **De gestión de incidentes:** Define como se lleva a cabo los incidentes, tiempos de respuesta y procesos a llevar a cabo.
    - La dirección del CSIRT-ESPE deberá notificar a las autoridades las acciones ilegales o sospechosas que atente en contra la institución o incumplan normas internas.
- **De colaboración:** Define las políticas para la cooperación con otros CSIRT.
    - Es responsabilidad del personal mantener una buena relación con socios y proveedores a fin de garantizar la colaboración.
    - Se debe gestionar acuerdos con socios para mejorar la calidad del servicio del CSIRT-ESPE.

Según un análisis realizado por (Andrade & Fuertes, 2013) las políticas del CSIRT-ESPE también deben contar con los controles de la norma ISO/IEC 27002 con sus políticas de:

- Seguridad de la información
- De control de usuarios
- De Transmisión de información
- De notificación de incidentes
- De tratamiento de incidentes

Ver (Anexo A: Políticas y buenas prácticas para controles de seguridad de la información).

Evaluación de la operación de servicio

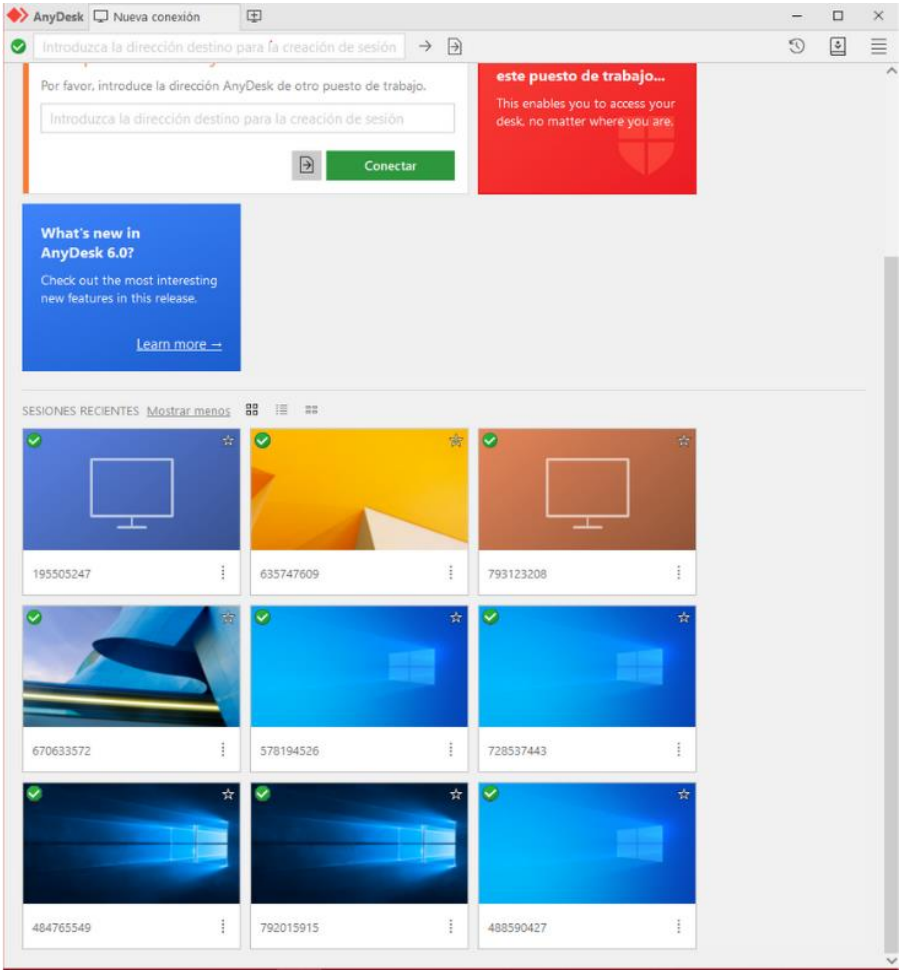
Evaluación de Anydesk

Debido a la pandemia actual del Covid-19, el personal deberá trabajar remotamente desde casa, por lo cual se adecuó la infraestructura del aula H-402 para recibir conexiones remotas por Anydesk:

Resultado:

Figura 84.

Funcionamiento de Anydesk



Nota. La figura representa el estado en línea de los equipos configurados en el laboratorio H-402 para recibir conexiones remotas.

Tabla 16.

Evaluación de operación de la herramienta Anydesk

Herramienta	Funciones	Cumplimiento	Observaciones
Anydesk	Permite conexiones remotas	Si	Conexiones remotas a personal del CSIRT-ESPE
	Solicita clave de acceso	Si	Permite el ingreso solo al personal autorizado.
	Conexión estable	Si	Permite la operación continua.
	Control centralizado de equipos	No	No disponible en versión gratuita.
	Actualizaciones automáticas	Si	La actualización no modifica las conexiones ya creadas.
	Transferencias de archivos	Si	Permite enviar y recibir archivos.
	Numero de sesiones ilimitadas	Si	El personal del CSIRT-ESPE podrá ingresar al equipo ilimitadamente.

Nota. La tabla representa la evaluación de la herramienta Anydesk para cumplir las funciones que requiere un operador del CSIRT-ESPE.

$$x = \left(1 - \frac{Número\ de\ funciones\ faltantes}{Número\ de\ funciones\ requeridas}\right) \times 10$$

$$x = \left(1 - \frac{1}{7}\right) \times 10 = 8{,}57$$

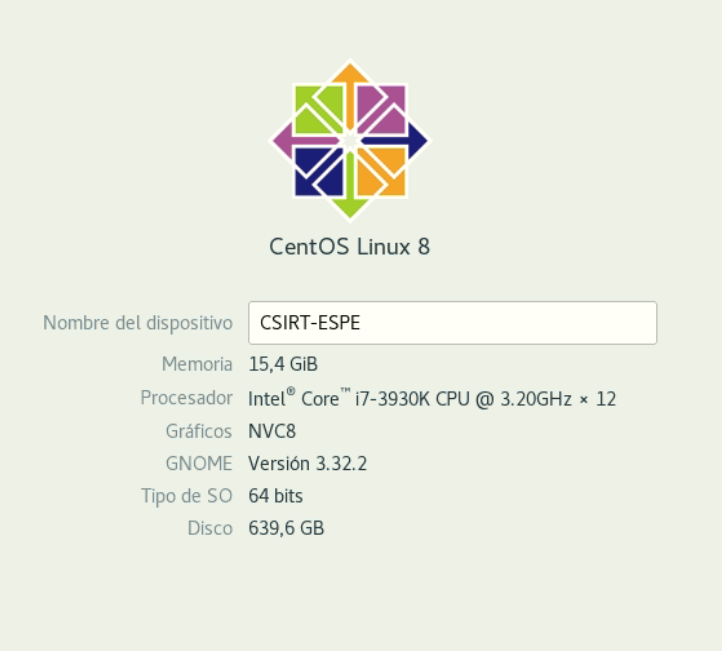
Evaluación de Nessus

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.

Resultado:

Figura 85.

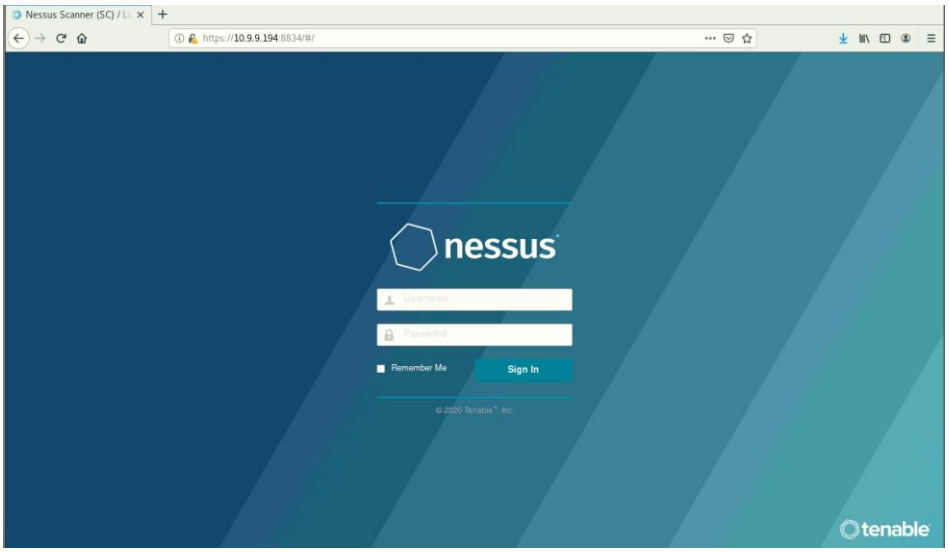
Operación del servidor Centos 8



Nota. La figura indica la distribución de Linux instalada en el servidor.

Figura 86.

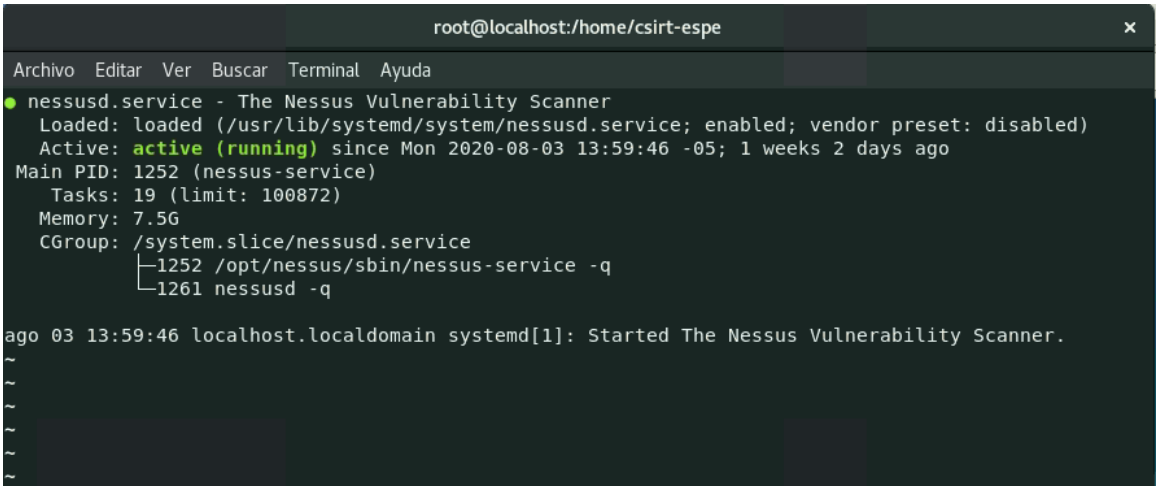
Funcionamiento de Nessus



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

Figura 87.

Estado del servicio de Nessus en el servidor



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

Tabla 17.

Evaluación de operación de la herramienta Nessus

Herramienta	Funciones	Cumplimiento	Observaciones
Nessus	Descubre vulnerabilidades	Si	Nessus cuenta con escaneo de vulnerabilidades, detalles de riesgo, detalle 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	Puede administrar dos tipos de usuarios: administrador y standard.
	Alerta de malware.	Si	Existe escaneos propios para detectar malware.
	Información sobre soluciones de problemas.	Si	Nessus recomienda al usuario soluciones de las fallas de seguridad.
	Feeds	Si	A través de su página web provee información sobre nuevas amenazas encontradas junto con tendencias de ciberseguridad y soluciones a casos detectados.
	Monitoreo de eventos en tiempo real	No	Nessus no dispone de visualización de logs o eventos en tiempo real.

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

$$x = \left(1 - \frac{Número\ de\ funciones\ faltantes}{Número\ de\ funciones\ requeridas}\right) \times 10$$

$$x = \left(1 - \frac{2}{8}\right) \times 10 = 7{,}5$$

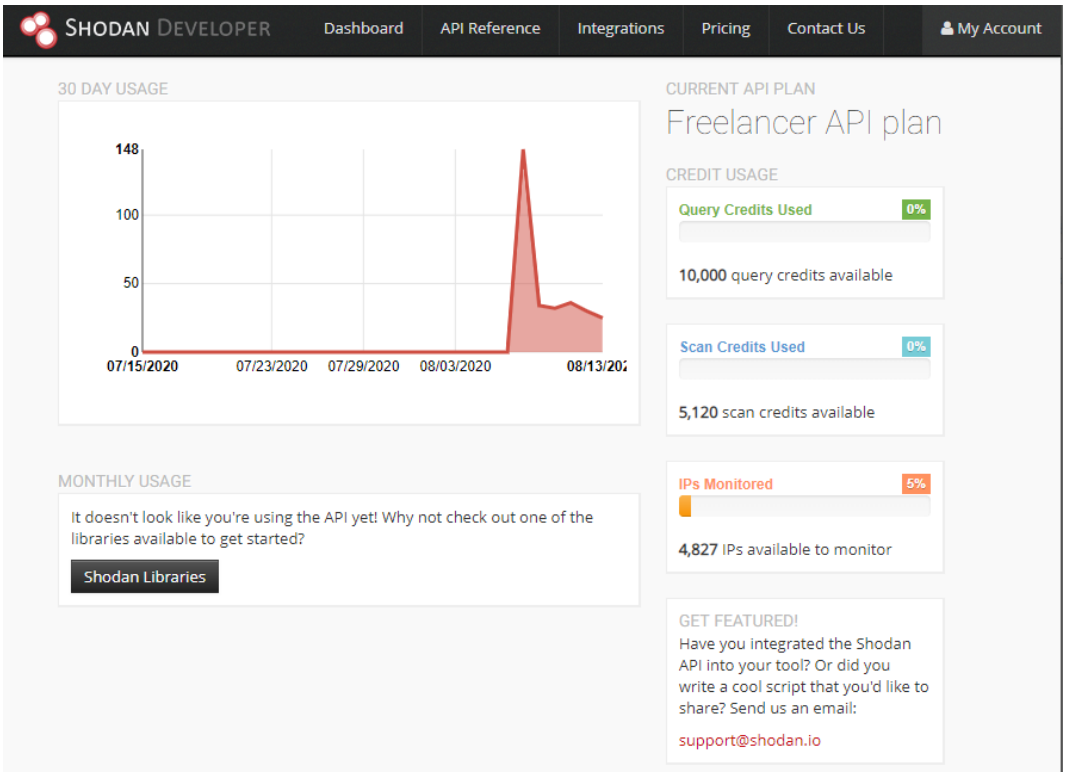
Evaluación de Shodan

El CSIRT-ESPE ha optado por utilizar el motor de búsqueda Shodan, lo cual para el presente proyecto se configuró para recibir alertas en tiempo real sobre los servicios puestos en línea con el hostname" espe.edu.ec", cabe recalcar que, si el personal necesita realizar escaneo a más servicios web ajenos a dicho hostname, lo puede hacer ya que el plan Freelancer configurada para este proyecto permite monitorear hasta 5120 IPs.

Resultado:

Figura 88.

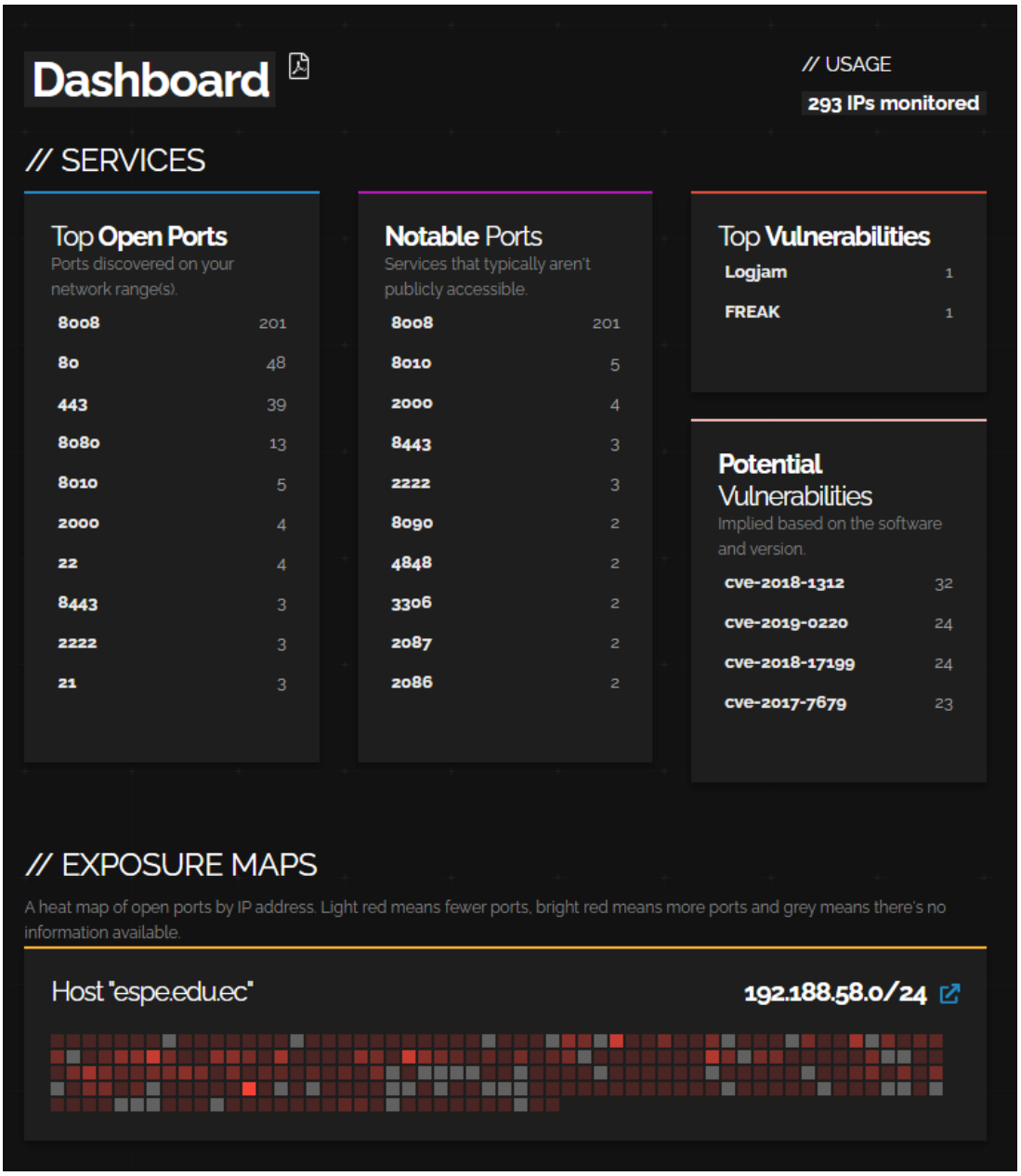
Operación de Shodan como monitor



Nota. La figura indica el uso de las IP monitoreadas por el hostname “espe.edu.ec”

Figura 89.

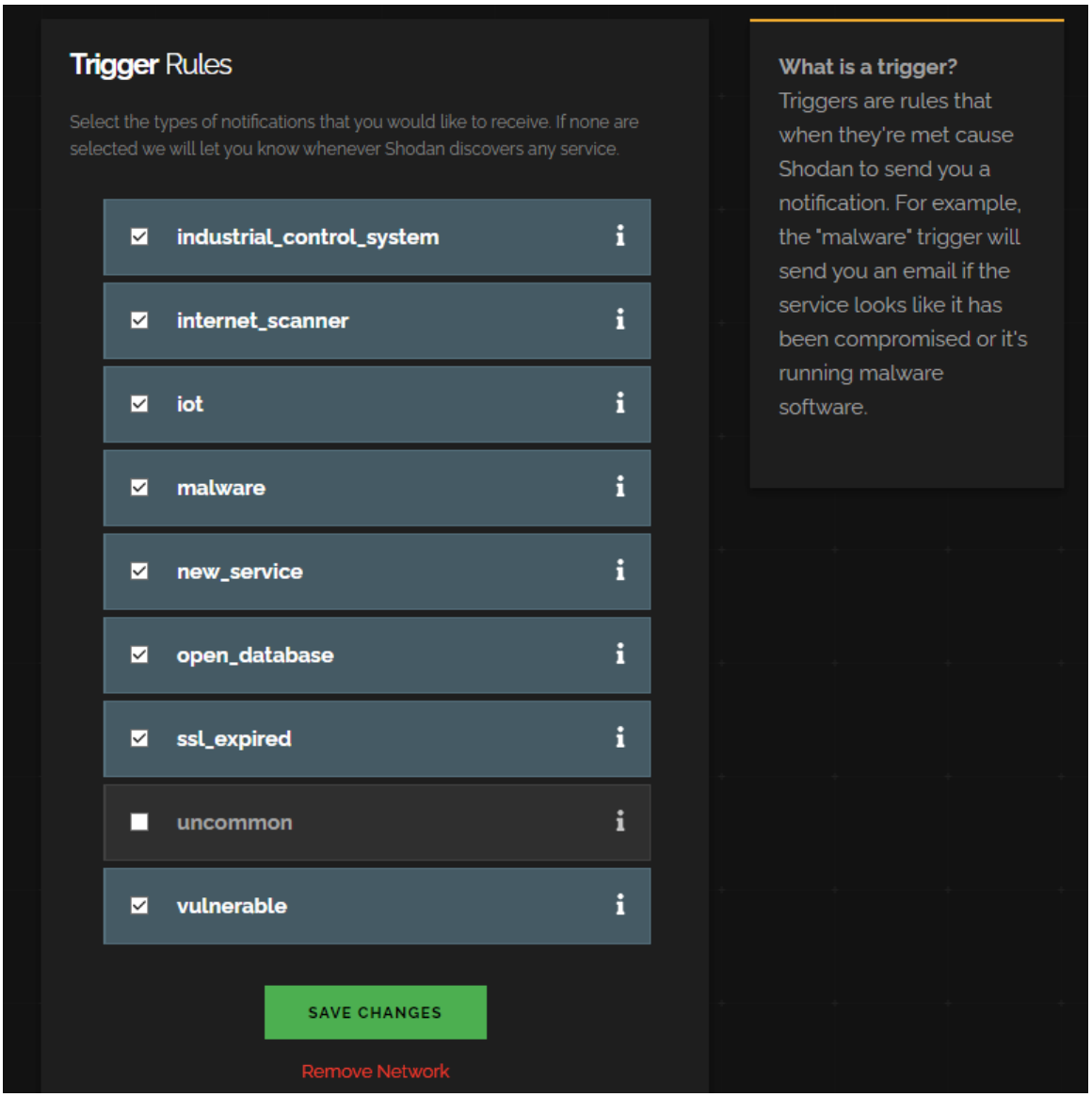
Operación de Shodan Monitor.



Nota. La figura indica el funcionamiento de shodan monitor para las IP con el hostname "espe.edu.ec"

Figura 90.

Tipo de alertas configuradas para el CSIRT-ESPE



Nota. La figura indica los disparadores configurados para emitir una alerta en el caso de que se cumpla, por ejemplo, si encuentra malware en uno de los servicios, shodan lo alertará vía correo electrónico.

Tabla 18.

Evaluación de operación de Shodan

Herramienta	Funciones	Cumplimiento	Observaciones
Shodan	Descubre vulnerabilidades	Si	Shodan indica las vulnerabilidades, puertos abiertos, servicios, etc., de las IPs monitoreadas.
	Informes y alertas	Si	Permite generar informes de búsquedas y vulnerabilidades.
	Manejo de incidentes	No	No permite el manejo de tickets.
	Control de accesos	No	En la cuenta freelancer no permite crear usuarios ni cuentas.
	Alerta de malware.	Si	Existe escaneos propios para detectar malware.
	Feeds	Si	A través de su página se puede encontrar libros, cursos, podcast que sirven de información al usuario.
	Monitoreo de eventos en tiempo real	Si	Monitorea en tiempo real y alerta mediante correo electrónico.
	Uso externo mediate APIs	Si	Permite el uso de sus características mediante llaves de acceso.

Nota. La tabla representa la evaluación de la herramienta Shodan para cumplir las funciones que requiere un operador del CSIRT-ESPE.

$$x = \left(1 - \frac{Número\ de\ funciones\ faltantes}{Número\ de\ funciones\ requeridas}\right) \times 10$$

$$x = \left(1 - \frac{2}{8}\right) \times 10 = 7{,}5$$

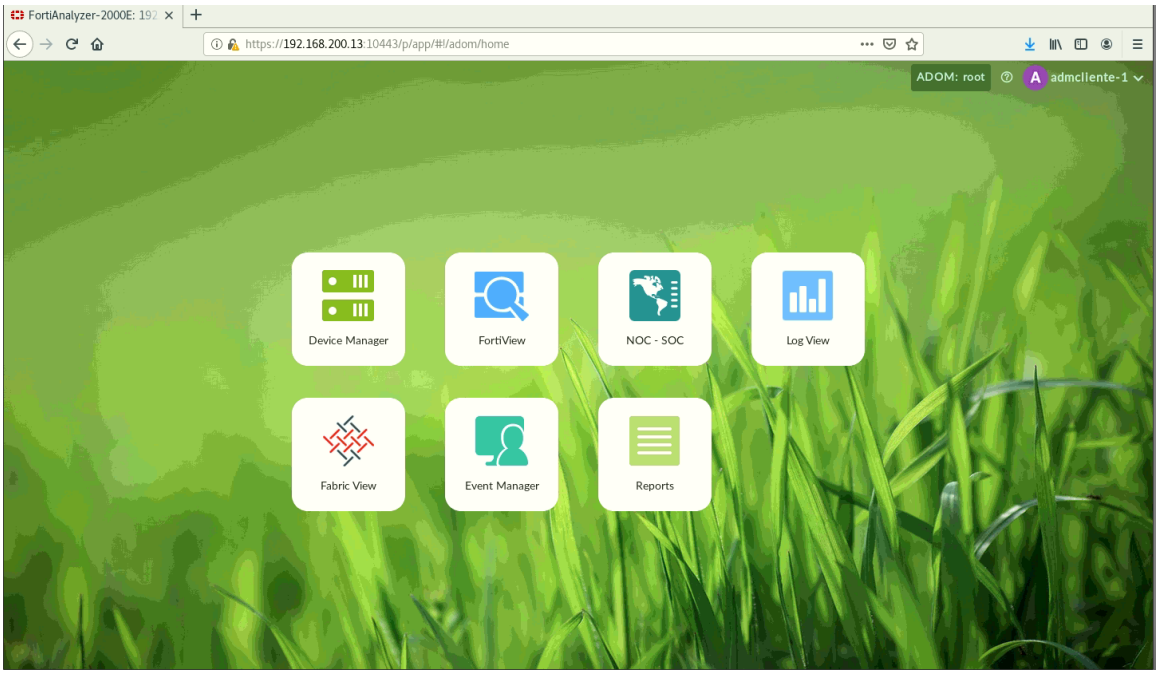
Evaluación de FortiAnalyzer

El FortiAnalyzer es usado por el CSIRT-ESPE para generar logs y eventos del tráfico de la ESPE, también se puede monitorear en tiempo real las amenazas y los hosts comprometidos dentro de la red local de la universidad.

Resultado:

Figura 91.

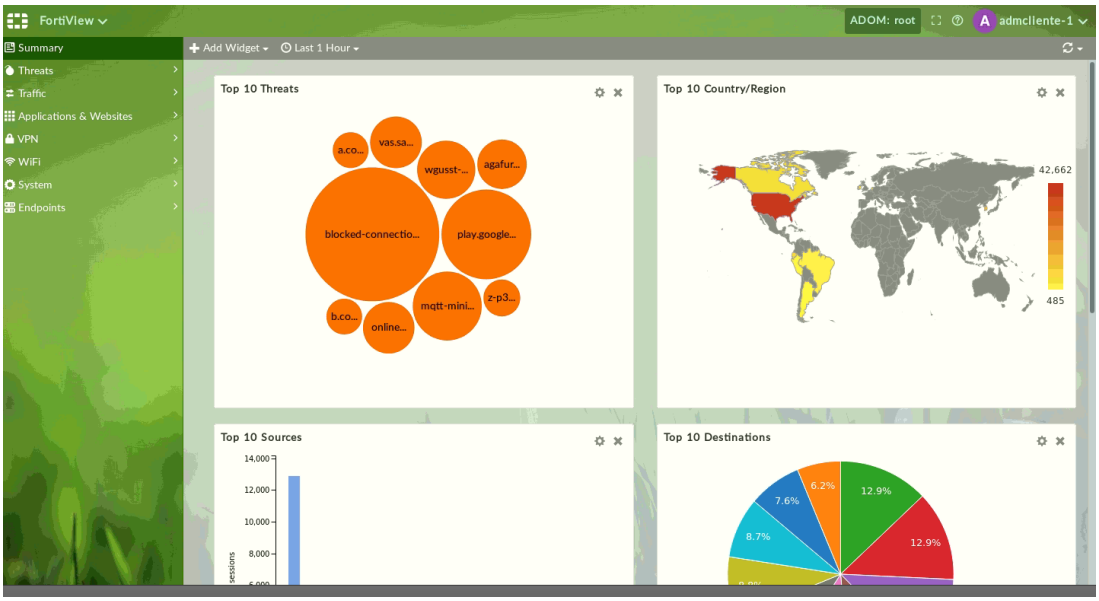
Operación de FortiAnalyzer.



Nota. La figura indica el menú principal del dispositivo FortiAnalyzer

Figura 92.

Resumen de amenazas y conexiones maliciosas.



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

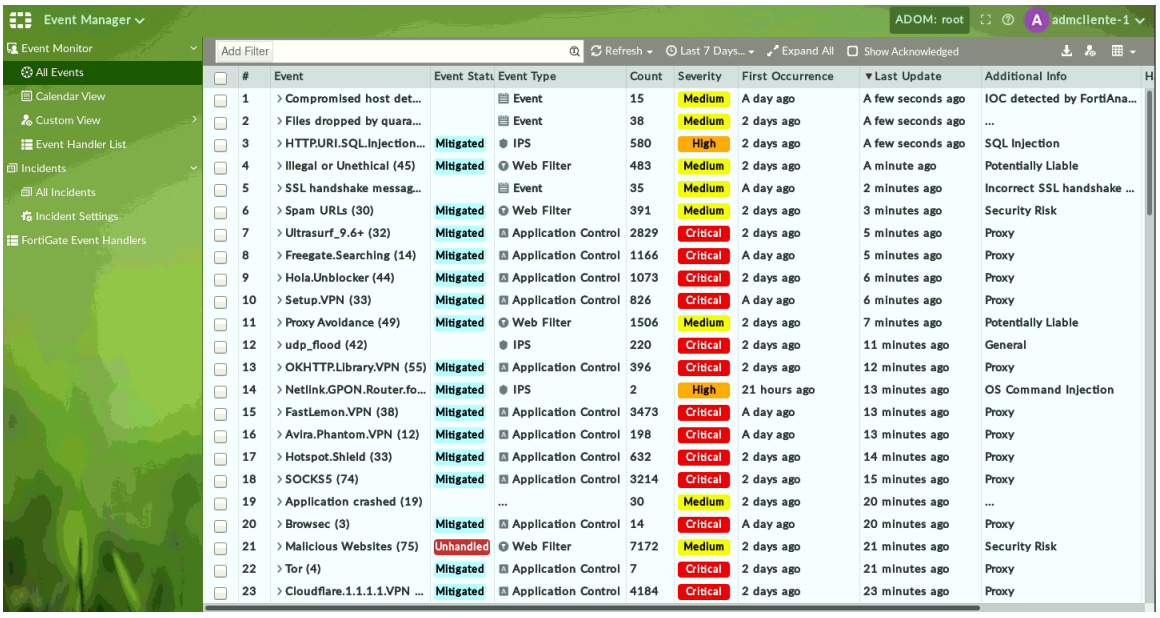
Figura 93.

Listado de host comprometidos

Nota. La figura describe los hosts infectados dentro de la institución.

Figura 94.

Listado de eventos dentro de la institución.



Nota. La figura indica el listado de eventos dentro de la red de la ESPE.

Tabla 19.

Evaluación de operación de FortiAnalyzer

Herramienta	Funciones	Cumplimiento	Observaciones
FortiAnalyzer	Descubre vulnerabilidades	Si	FoortiAnalyzer indica las vulnerabilidades, puertos abiertos, servicios, etc., de la red de la Universidad.
	Informes y alertas	Si	Permite generar informes.
	Manejo de incidentes	No	No permite el manejo de tickets.
	Control de accesos	Si	Permite 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

Herramienta	Funciones	Cumplimiento	Observaciones
			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 bloqueo automático basado en reglas.

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

$$x = \left(1 - \frac{Número\ de\ funciones\ faltantes}{Número\ de\ funciones\ requeridas}\right) \times 10$$

$$x = \left(1 - \frac{1}{8}\right) \times 10 = 8{,}75$$

Evaluación de Freshdesk

El servicio web de Freshdesk fue instalado para la gestión de incidentes, helpdesk, soporte y peticiones de los clientes hacia el CSIRT-ESPE. 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.

Resultado:

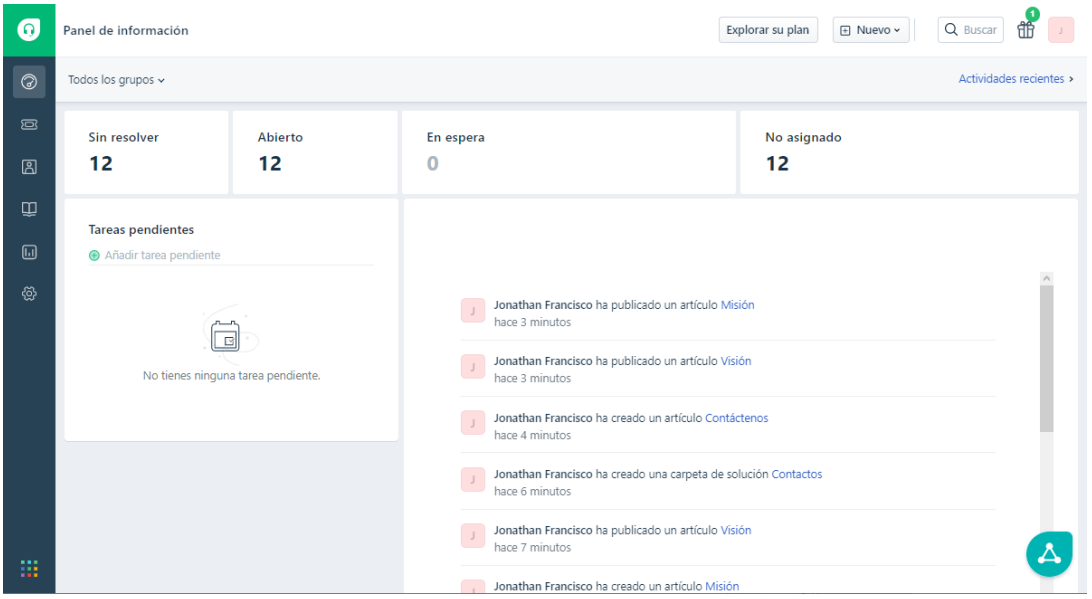
***Figura* 95.**

Operación del Portal CSIRT-ESPE de servicio al cliente

Nota. La figura indica el portal CSIRT-ESPE para servicio al cliente o recepción de solicitudes.

Figura 96.

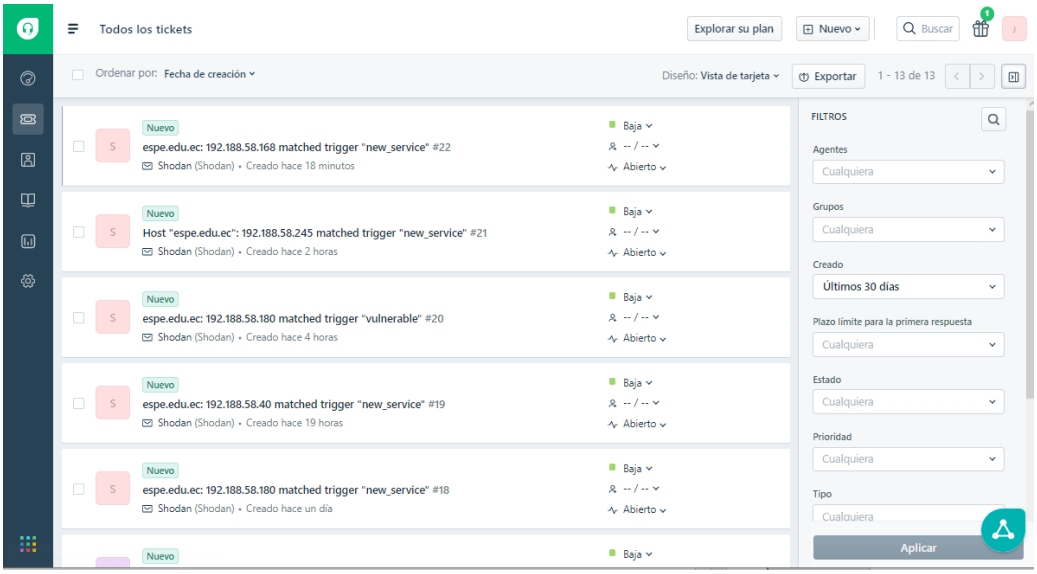
Dashboard de gestión de peticiones e incidentes.



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

Figura 97.

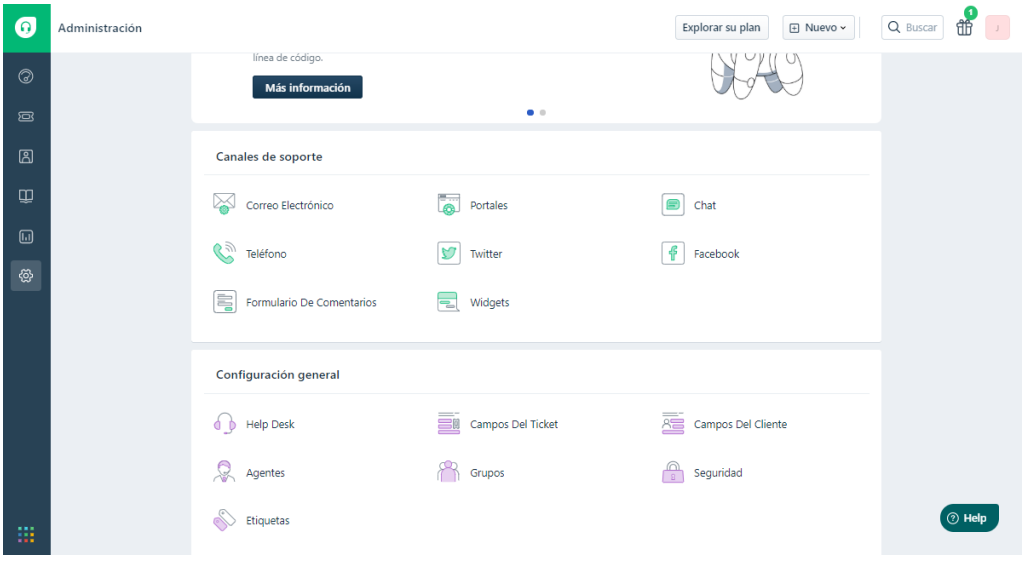
Listado de tickets o solicitudes.



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

Figura 98.

Administración de Freshdesk.



Nota. La figura describe el panel de administración del portal CSIRT-ESPE.

Tabla 20.

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 con 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 FortuAnalyzer para cumplir las funciones que requiere un operador del CSIRT-ESPE.

$$x = \left(1 - \frac{Número\ de\ funciones\ faltantes}{Número\ de\ funciones\ requeridas}\right) \times 10$$

$$x = \left(1 - \frac{0}{10}\right) \times 10 = 10$$

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 21.

Evaluación general de herramientas del CSIRT-ESPE

Herramienta	Estado actual	Métrica	Valor	Puntuación
Anydesk	En operación	Cumplimiento de funciones	8,57	Satisfactorio
Nessus	En operación	Cumplimiento de funciones	7,5	Aceptable
Shodan	En operación	Cumplimiento de funciones	7,5	Aceptable
FortiAnalyzer	En operación	Cumplimiento de funciones	8,75	Satisfactorio
Freshdesk	En operación	Cumplimiento de funciones	10	Satisfactorio

Cabe recalcar que las herramientas fueron escogidas para cumplir los servicios iniciales del CSIRT-ESPE 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 CSIRT.

Para la evaluación de la puesta en marcha inicial del CSIRT-ESPE vamos a tomar en cuenta los servicios implementados juntamente con sus funciones, los cuales

comprenden de:

Tabla 22.

Funciones de los servicios básicos de un CSIRT

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. - Estrategias de mitigación.
Coordinación de la respuesta a incidentes.	- 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 CSIRT, contrarrestando con las herramientas implementadas para verificar su cumplimiento.

Tabla 23.

Evaluación general del servicio y herramientas

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

Servicio	Función	Herramienta que sustenta	Cumplimiento de función%
	- Análisis de soluciones.	Nessus, Usuario	80
Apoyo en la respuesta de incidentes	- Ayuda por teléfono.	Teléfono del laboratorio.	100
	- Ayuda por correo electrónico.	Freshdesk	100
	- Ayuda por informes.	Freshdesk , Nessus, FortiAnalyzer, Shodan.	100
	- Estrategias de mitigación.	Personal CSIRT.	80
Coordinación de la respuesta a incidentes.	- Ayuda en la recuperación.	Anydesk, Usuario.	90
	- Análisis de posibles ataques	FortiAnalyzer Shodan Nessus	100
	- Colaboración con otras áreas de la institución.	Freshdesk, personal CSIRT.	100
	- Coordinar con el personal los diferentes casos.	Freshdesk.	100
		PROMEDIO TOTAL	93.8%

En conclusión, la operación del servicio es satisfactoria y cumple con el 93.8% las funciones básicas de un CSIRT.

Capítulo V

Conclusiones

- Un CSIRT Académico completo requiere de una gran inversión en software e infraestructura para dar un servicio óptimo e independiente a otras áreas. En el presente proyecto se logró poner en marcha inicial al CSIRT-ESPE con poca inversión y reutilizando infraestructura propia de la Universidad tomando en cuenta que se entregará los servicios básicos de un CSIRT.

- La revisión sistemática de literatura de la documentación y proyectos en marcha que existen para la implementación de un CSIRT Académico permite utilizar buenas prácticas que acortan el tiempo en la ejecución de un proyecto.

- Se seleccionó las herramientas en base a la utilidad y disponibilidad de recursos que permiten su instalación conforme a los requerimientos iniciales del proyecto.

- La relación con otras entidades como CEDIA y otros equipos de respuesta nacionales y extranjeros fue fundamental para el desarrollo del proyecto ya que permitió tener una visión más real de las funciones de un CSIRT y se logró aprovechar el licenciamiento de herramientas otorgado por dichas instituciones socias.

Recomendaciones

- Priorizar la formación en temas de seguridad de la información al personal docente, estudiantes y administrativos integrando campañas de concientización o materias de seguridad informática en pregrado o postgrado.

- Realizar la gestión para que la ESPE destine un presupuesto anual para la

adquisición de software, infraestructura TI y capacitación al personal del CSIRT, considerando que el presente proyecto se basó en herramientas gratuitas o en licencias básicas para la puesta en marcha inicial del CSIRT y la capacitación se realizó ad-hoc con ayuda de los CSIRTs relacionados.

- Mantener reuniones continuas con los colaboradores externos para compartir información, realizar mejoras dentro del CSIRT-ESPE e integrar nuevos servicios en el CSIRT-ESPE basados en los intereses de la comunidad a la que se presta servicio.

Bibliografía

Andrade, R., Fuertes, W., & Escuela Politécnica del Ejercito. (2012). *Diseño y dimensionamiento de un equipo de un equipo de respuesta ante incidentes de seguridad informática (CSIRT). Caso de estudio : ESPE*. *2012*(Diseño y dimensionamiento de un equipo de un equipo de respuesta ante incidentes de seguridad informática (CSIRT)), 9.

Bravo Campoverde, M. E. (2015). *(ITIL) Gestión de versiones*. https://es.scribd.com/document/271087126/Bilioteca-de-infraestructura-de-tecnologia-de-informacion-ITIL-Gestion-de-versiones-VERSIONES-pdf

Cisco Networking Academy. (2020). *Introducción a la Ciberseguridad*. https://www.netacad.com/es/courses/cybersecurity/introduction-cybersecurity

De la Torre Moscoso, H. M., & Parra Rosero, M. A. (2018). Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE. In *Repositorio ESPE*. Universidad de las Fuerzas Armadas ESPE.

Dentzel, Z. (2013). *El impacto de internet en la vida diaria*. https://www.bbvaopenmind.com/articulos/el-impacto-de-internet-en-la-vida-diaria/

Enisa. (2006). *Cómo crear un CSIRT paso a paso* (p. 90).

Excutive Master Project Management. (2019). *Módulo 2. Estrategia de Servicio ITIL*. https://uv-mdap.com/programa-desarrollado/bloque-vi-itil-v3/estrategia-de-servicio-basado-en-itil/

Fernández-Baladrón, C. (2007). ITIL: Information Technology Infrastructure Library. *Bit*, *160*, 46–49.

FIRST. (2018). *FIRST - Improving Security Together*. https://www.first.org/

Fuertes, W., Carrera, V., Ron, M., Tapia, F., Sánchez, M., Recalde, L., Nuñez, A., & Cruz, H. (2020). *Diseño e Implementación del sistema de gestión de servicios e infraestructura de TI para el CSIRT/CERT Académico de la ESPE*.

Guedez, A. (2018). *ISO, COBIT e ITIL, ¿cuál de estas normas y estándares internacionales te conviene más para potenciar tu empresa?* https://www.gb-advisors.com/es/normas-y-estandares-internacionales/

Hackmageddon, & Passeri, P. (2020). *Q1 2020 Cyber Attacks Statistics*. https://www.hackmageddon.com/2020/04/14/q1-2020-cyber-attacks-statistics/

Internet World Stats. (2018). *Internet World Stats - Usage and Population Statistics*. https://www.internetworldstats.com/

ITIL Foundation. (2015). *Gestión de la Configuración y Activos del Servicio*. https://segenuino.com/itil/transicion_servicios_TI/gestion_configuracion_activos_servicio.html

Kemp, S. (2020). *Digital 2020 Global DIgital Overview*. https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media

Koltchof, A., Pieper, M., & Tjassing, R. (2015). *Gestión de Servicio de TI basada en ITIL V3 Guia de Bolsillo*. Van Haren Publishing.

Merino Vásquez, José Christian; Torres Asencios, E. J. (2016). *Implementación de un modelo de la seguridad informática basados en ITIL V3 para un Pyme de TI*.

NIST. (2020). *National Institute of Standards and Technology | NIST*.

https://www.nist.gov/
Office of Government Commerce. (2010a). *Operaciân del servicio* (The Stationery Office (ed.)). https://books.google.com.ec/books/about/Operaciân_del_servicio.html?id=htb2mp3A2WAC&redir_esc=y
Office of Government Commerce. (2010b). *Transiciân del servicio*.
Organización de los Estados Americanos. (2016). *Buenas prácticas para establecer un CSIRT nacional* (p. 105). https://www.sites.oas.org/cyber/Documents/2016 - Buenas Practicas CSIRT.pdf
Organización Internacional de Normalización. (2018). *ISO 27001 - Seguridad de la información: norma ISO IEC 27001/27002*. https://www.normas-iso.com/iso-27001/
Reyes, F., Fuertes, W., Tapia, F., Toulkeridis, T., Aules, H., & Pérez, E. (2018). A BI Solution to Identify Vulnerabilities and Detect Real-Time Cyber-Attacks for an Academic CSIRT. *Advances in Intelligent Systems and Computing*, *857*.
Ríos, S. (2014). ITIL v3 Manual íntegro. In *B-able* (p. 101). http://www.biable.es/wp-content/uploads/2014/ManualITIL.pdf
Romanos, J. G. (2008). *La gestión de la configuración y la gestión de activos como una gestión del conocimiento*. http://www.redalyc.org/articulo.oa?id=92217123004
Ron Egas, M., Vásquez Cañas, Rodrigo Larafranco, E., Nicolás, M., & Javier, D. (2017). *Prectical Guide To Implement An Academic Computing Security Incident Response Team (Adademic CSIRT)* (p. 15).
Securelist. (2019). *Desarrollo de las amenazas informáticas en el primer trimestre de 2019*. https://securelist.lat/it-threat-evolution-q1-2019-statistics/88983/
Thompson, E. C. (2018). Incident Response Frameworks. In *Cybersecurity Incident Response*.
Universidad Técnica Virtual Tecnologico de Monterrey. (2019). *Transición del Servicio (ST)*.
Uyana García, M. A. (2014). *Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos, CSIRT*.
WeLiveSecurity. (2015). *¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?* https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/
Wikiversity. (2015). *Estándar ITIL*. https://es.wikiversity.org/wiki/Estrategia_del_servicio_en_ITIL