Sistema de monitoreo de incidentes de seguridad en el tráfico de red basado en multi agentes para los servicios de Unidad de Informática de la EMI La Paz

Vladimir Brayan Fernandez Rondo
JUNIOR Carrera de Ingeniería de Sistemas Escuela Militar de Ingenieria
La Paz, Bolivia
vladfernd@gmail.com

Monitoring system for security incidents in network traffic base on multiple agents for the services of the Unit Computing of the EMI La Paz

Resumen – La Seguridad Informática en la actualidad ha tomado relevancia en distintas organizaciones, porque hoy en día todos los dispositivos se encuentran conectados mediante Internet y se ha considerado la información de los dispositivos como importancia para las diferentes organizaciones.
Se debe considerar que la seguridad de la información es parte de la seguridad informática, además de considerar los pilares fundamentales como son confidencialidad, integridad y disponibilidad.
Para establecer la Seguridad Informática es necesario establecer medidas de seguridad preventivas, reactivas o de recuperación en cada etapa se toman técnicas adecuadas a la organización.
Para la seguridad Informática el primer paso es prevenir ante incidentes de seguridad que puedan afectar los activos de la organización, se tomó en cuenta los activos que son parte de la infraestructura de red que prestan servicios dentro de la Institución, monitoreando la presencia de incidentes de seguridad.
Para establecer medidas de seguridad de los activos se realizó el análisis de riesgos considerando la triada fundamental de seguridad de la información, se consideró también para la tarea de monitorización la utilización del concepto de agentes inteligentes del tipo reactivo simple el cual mediante su codificación correspondiente se encarga de emitir alertas ante la presencia de incidentes de seguridad de la información.

Palabras Claves— Amenaza, integridad, confidencialidad, riesgo, vulnerabilidad, incidente, agente.

Abstract - Computer Security has now become relevant in different organizations, because today all devices are connected through the Internet and device information has been considered important for different organizations.
Information security should be considered as part of computer security, in addition to considering the fundamental pillars such as confidentiality, integrity and availability.
In order to establish Computer Security, it is necessary to establish preventive, reactive or recovery security measures. At each stage, appropriate techniques are taken to the organization. For Computer security, the first step is to prevent security incidents that may affect the organization's assets. The assets that are part of the network infrastructure that provide services within the Institution were taken into account, monitoring the presence of security incidents. security.
In order to establish security measures for the assets, the risk analysis was performed considering the fundamental triad of information security, the use of the concept of smart agents of the simple reactive type was also considered for the monitoring task, which through its corresponding codification is responsible for issuing alerts in the presence of information security incidents.

Keywords—Threat, integrity ,confidentiality, risk, vulnerability, incident, agent.

I. INTRODUCCIÓN

Debido al crecimiento de las nuevas tecnologías dependientes de Internet también crecen las posibilidades de sufrir incidentes informáticos

que puedan afectar a la disponibilidad, confidencialidad e integridad de la información que es relevante para para todos los usuarios de Internet, por tal motivo es necesario que dentro de las infraestructuras de red se implemente un servicio de monitoreo de la red que sea capaz de apoyar en la captura del tráfico generado por los diferentes servicios que se provee a los usuarios que se encuentran dentro de la red.
Los incidentes de seguridad que afectan los servicios de red se presentan de diferentes maneras ya sea por la navegación en sitios web no seguros, la descarga de archivos, sistemas operativos desactualizados, conexión a redes inalámbricas inseguras, instalar programas de sitios no confiables en Internet, entre otros a los que están expuestos los usuarios de Internet, estos incidentes llegan a afectar a un único usuario y también son capaces de afectar completamente a una infraestructura de red.
El monitoreo de incidentes de seguridad en el tráfico de red dentro de la Unidad de Informática Escuela Militar de Ingeniería pretende apoyar a la gestión de redes mediante el proceso de monitoreo constante de la infraestructura de red de la Unidad de Informática la cual también está a cargo de la red del campus de Alto Irpavi que está destinada a la comunidad universitaria , mediante el uso de multi agentes de manera que el conjunto de agentes sea capaz de recolectar el tráfico generado de acuerdo al protocolo utilizado por los servicios dentro de la red, este proceso contribuye a la prevención de incidentes y el seguimiento de fallos dentro de la red que afecten a la infraestructura de red de la Unidad de Informática de la Escuela Militar de Ingeniera

II. GENERALIDADES

A. Problemas

1) Problema Principal

La existencia de incidentes se seguridad en el tráfico de red de la Unidad de Informática de la Escuela Militar de Ingeniería Unidad Académica La Paz ocasiona riesgos en la continuidad de los servicios de red.

2) Problemas secundarios

- La información parcial con respecto a la configuración lógica de los equipos de la infraestructura de red ocasiona la presencia de vulnerabilidades imprevistas en los equipos de la red.
- La cantidad de servicios de red instalados por la Unidad de Informática ocasiona dificultad en el proceso de
- captura de trafico de red.
- El actual proceso de respuesta a incidentes de seguridad tiene como consecuencia la demora en la identificación de incidentes acaecidos en la red.
- El registro de los incidentes de seguridad en el tráfico de red se encuentra almacenado en cartapacios lo que dificulta la búsqueda de información para la respuesta inmediata a incidentes de seguridad.

B.Objetivos

1) Objetivo principal

Proponer un sistema de monitoreo de incidentes de seguridad en el tráfico de red de la Unidad de Informática de la Escuela Militar de Ingeniería Unidad Académica La Paz basado en multi agentes para reducir los riesgos en la continuidad de los servicios de red

2) Objetivos específicos

- Realizar un análisis de vulnerabilidades de los equipos de la infraestructura de la red para identificar el nivel de riesgo actual.
- Elaborar el diseño de la estructura de roles y tareas de los agentes para el proceso de captura de trafico de red.
- Diseñar el modelo de la arquitectura de organización de los multi agentes para la identificación de los incidentes de seguridad en el tráfico de red.
- Desarrollar el módulo con multi agentes que registre los incidentes de seguridad en la red para el apoyo a la respuesta inmediata de incidentes de seguridad en la red.

III. MARCO PRACTICO

A.Análisis de riesgo

El análisis de riesgos contempla un procedimiento el cual mediante indicadores logra identificar las posibles amenazas, como ser el impacto y el riesgo de cada activo presente en la Unidad de Informática.

1) Análisis de la situación actual

Para realizar el análisis de la situación actual, estudiaremos todo aquello que se involucra en el sistema o proceso actual de la Unidad de Informática para la respuesta a incidentes de seguridad de la información, para lo cual se utilizara métodos de recolección de información que ayuden a describir y comprender este proceso.

El área de interés para la propuesta del sistema de monitoreo de incidentes de seguridad de la información será el área de redes que pertenece a la Unidad de Informática U.A.L.P.
•Área de redes Tiene como objetivo administrar, desarrollar y mantener en adecuado funcionamiento la infraestructura de redes de la Unidad Académica.

TABLA I

EXTRACTO DE LA VALORACIÓN DE ANÁLISIS DE ACTIVOS

Amenazas	F	ID	F * I	II	F * I	IC	F * I	R
MIKROTIK			35		28		28	
Conexión remota	0.7	50	35	40	28	40	28	30.3
Acceso no autorizado	0.7	50	35	40	28	40	28	
Denegación de servicios	0.7	50	35	40	28	40	28	

Donde: F, representa la frecuencia u ocurrencia de que la amenaza se materialice, ID representa el impacto respecto a la disponibilidad, II representa en impacto respecto de integridad y IC representa el impacto respecto de confidencialidad dando como resultado R como el valor de riesgo del activo

2) Análisis de los activos actuales

Los activos de estudio analizados serán los que interactúen directamente con el sistema o con los procedimientos involucrados para contribuir en el desarrollo del sistema, así mismo se detallara las características técnicas de los activos identificados.

3) Identificación de los activos

Para la identificación de los activos se utilizó la herramienta nmap dando como resultado la siguiente información.

3) Análisis y valoración

Para el análisis y valoración de activos mediante los principios de seguridad de la información se debe realizar un análisis de vulnerabilidades de los activos y de esta manera valorar su probabilidad de incidencia, también se debe valorar el impacto que puede sufrir el activo si se materializa una amenaza de esta manera se valorara el impacto y la probabilidad de ocurrencia de la amenaza respecto a una vulnerabilidad.

- Disponibilidad ¿Qué importancia tendría que el activo no se encuentre disponible?

TABLA II
MATRIZ DE VALORACIÓN DE

Activo	Impacto * probabilidad	Nivel de riesgo
Mikrotik	30<impacto*frecuencia<=4	Alto

- Confidencialidad ¿Qué importancia tendría que la información asociada al activo fuera conocida por las personas no autorizadas?

- Escala de valoración muy alta, alta, media, baja, muy baja.

Una vez realizado la valoración de amenaza e impacto se procede a valorar el nivel de riesgo. Una vez se valoró el riesgo se procede a analizar su nivel de riesgo de cada activo, para localizarlo dentro de la matriz que corresponde al riesgo
La matriz donde se identificará el riesgo corresponde a la siguiente figura.
Figura I Matriz de valoración de riesgo

Impacto * Frecuencia	Muy alto 50	Alto 40	Medio 30	Bajo 20	Muy bajo 10
Muy alto (1.0)	50*1.0<=50	40*1.0<=40	30*1.0<=30	20*1.0<=20	10*1.0<=10
Alto(0.9)	50*0.9<=45	40*0.9<=36	30*0.9<=27	20*0.9<=18	10*0.9<=9
Medio(0.7)	50*0.7<=35	40*0.7<=28	30*0.7<=21	20*0.7<=14	10*0.7<=7
Bajo (0.5)	50*0.5<=25	40*0.5<=20	30*0.5<=15	20*0.5<=10	10*0.5<=4
Muy baja (0.3)	50*0.3<=15	40*0.3<=12	30*0.3<=10	20*0.3<=6	10*0.3<=3

El nivel de riesgo resultado del producto de impacto por vulnerabilidad debe situarse en la matriz de riesgo identificando de acuerdo a un color y rango de nivel de riesgo

Donde una vez realizado los cálculos se puede evidenciar los siguientes resultados.

Una vez se realiza el análisis de riesgo se procede a elaborar el diseño de agentes de acuerdo con los activos encontrados.
B. Diseño de multi agentes

la tarea será realizada mediante agentes reactivos, que presentan un comportamiento adaptativo que genera respuestas de acuerdo a la percepción de su entorno

1) Especificación de actores

Los actores se consideran elementos del entorno estos se deben de identificar mediante un nombre que se encuentre relación con sus objetivos

- Integridad ¿Qué importancia tendría que la información relacionada con el activo se modificaría sin su control?

Tabla V

rol	Especificación
Procesador trafico	• Percepción: captura de trafico de red. • Acción: registrar tráfico capturado en base de datos.

DETERMINACIÓN DE ROL DE AGENTE

TABLA III

ESPECIFICACIÓN DE ACTORES

Definición del agente	Actor
Agente reactivo encargado de recolectar tráfico de red	
Agente reactivo encargado de escanear los puertos habilitados de los dispositivos de red	
Agente encargado de gestionar el estado de los dispositivos de red	

Se debe especificar la determinación de roles de agentes

2)Diagrama de escenarios

Los escenarios deben de mostrar una instancia especifica en

la que el agente se involucre, se puede considerar al escenario como el entorno en el que los agentes reaccionaran y ejecutaran un objetivo.

3)Determinación de roles y objetivos de agentes

Se identificará los roles de los agentes considerados también como objetivos los cuales describen funcionalidades que se proponen.

4)Diagrama de relación de agentes

TABLA IV

MATRIZ DE VALORACIÓN DE RIESGO

Los agentes deben identificarse haciendo una relación del actor con su definicion

1)Determinación del producto backlog

TABLA V DETERMINACIÓN DEL PRODUCT BACKLOG

Product Backlog		
N° SPRINT	NOMBRE DE LA HISTORIA DE USUARIO	N° HISTORIA DE USUARIO
SPRINT 1	Diseño de la base de datos	1
	Registro de usuarios	2
	Gestionar Usuario	3
SPRINT 2	Registrar Activos	4
	Gestionar Activos	5
	Análisis de Riesgos	6
SPRINT 3	Registrar Agente	7
	Gestionar Agente	8
	Alertas	9
SPRINT 4	Gestionar incidentes	10
	Reporte de riesgos	11
	Reporte de incidentes	12

Tabla IV

DIAGRAMA DE ESCENARIO DE AGENTE

Escenario	Especificación	Detalle
Captura de paquetes de red	Cuando el usuario activa la captura de paquete red	• Consultar protocolo • Capturar paquetes de red

DIAGRAMA DE ESCENARIO DE AGENTE
Escenario Especificación Detalle Cuando el usuario activa la captura de paquete red
•Consultar protocolo
•Capturar paquetes de red

El diseño de la relación de multi agentes responderá al proceso de identificación de incidentes de seguridad.

2)Determinación de requerimientos

Para la interacción de agentes es necesario identificar y diseñar su relación, identificando el siguiente aspecto si un paso involucra un rol asignado a un agente y el siguiente involucra otro rol asignado a otro agente, tendrá que un intercambio de información a esto se denomina protocolo.

C.Desarrollo de sistema multi agentes

TABLA VII
TABLA DE REQUERIMIENTOS

NUMERO	DESCRIPCIÓN	TIPO
R1	Registro del cargo del personal que participe en el sistema (administrador, encargado de rede, encargado de soporte y mantenimiento)	evidente
R2	Registro de la importancia o impacto del activo, vulnerabilidades y frecuencia para el análisis de riesgo del activo	evidente
R3	Procesar datos de los activos para el análisis de riesgos	oculto
R4	Registro de usuarios del sistema	Evidente
R5	Registro de agentes para la identificación de incidentes de seguridad	oculto

R6	Generar alertas de acuerdo al incidente de seguridad identificado	Evidente
R7	Generar reporte del análisis de riesgo de los activos registrados y valorados	Evidente
R8	Generar reporte de incidentes de seguridad identificados	Evidente

3)Diagrama de casos de uso de alto nivel

Una vez identificado los requerimientos e identificados los involucrados del sistema se procederá a establecer los procesos del sistema mediante el uso de diagramas que puedan dar a entender el funcionamiento que tiene el sistema

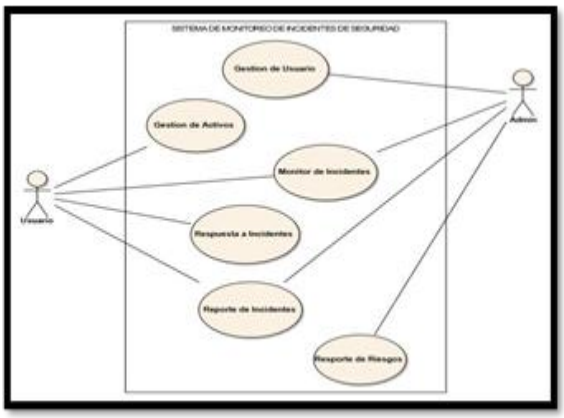


FIGURA II
DIAGRAMA DE CASOS DE USO DE ALTO NIVEL

El diagrama de casos de alto nivel muestra de forma general como se desplazará los actores dentro del sistema

4)Sprint 1

Una vez desarrollado el diagrama de casos de uso se realizará el diagrama del modelo de entidad relación.

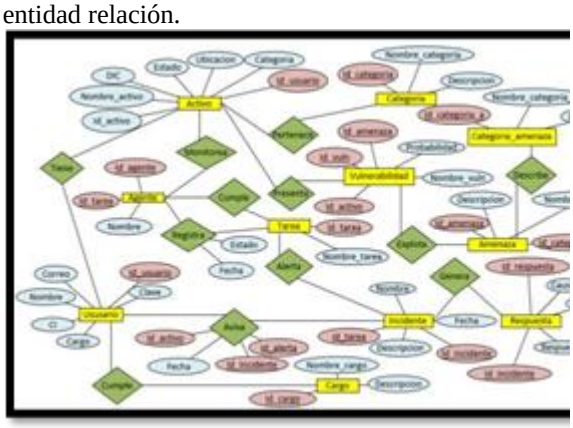


FIGURA III DIAGRAMA ENTIDAD RELACIÓN

El diagrama entidad relación mostrara de manera general como se relaciona cada entidad para proceder a elaboración del diseño relacional

Una vez se realiza el modelo de entidad relación y el diagrama de casos de uso de alto nivel.

Se procede a elaborar los módulos establecidos en los módulos del diagrama de casos de uso.

Modulo registro de usuarios que consta del diseño de diagrama de secuencia, prototipo de interfaz, interfaz final.

•Modulo de registro de usuario

Se procederá elaborar el diagrama de secuencia del módulo de registro de usuario.

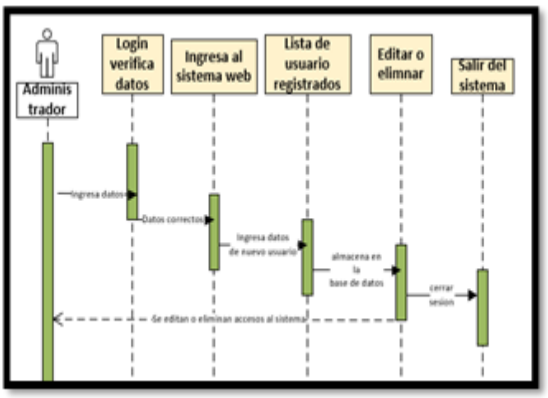


FIGURA IV
DIAGRAMA DE SECUENCIA

El diagrama de secuencia establece los pasos y la navegación del usuario en el modulo
Prototipo de registro de usuario

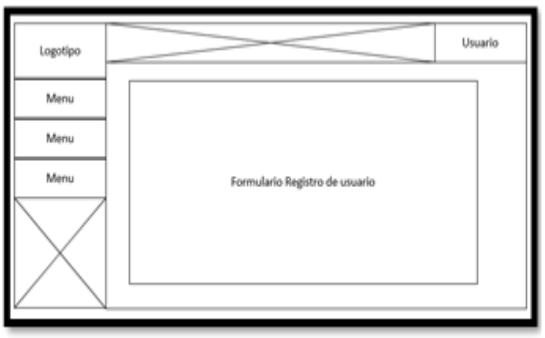


FIGURA V
PROTOTIPO REGISTRO DE USUARIO

El prototipo de interfaz de registro de usuario corresponde se debe maquetar mediante alguna herramienta de vista de navegación web
El prototipo de interfaz de registro de usuario corresponde se debe maquetar mediante alguna herramienta de vista de navegación web

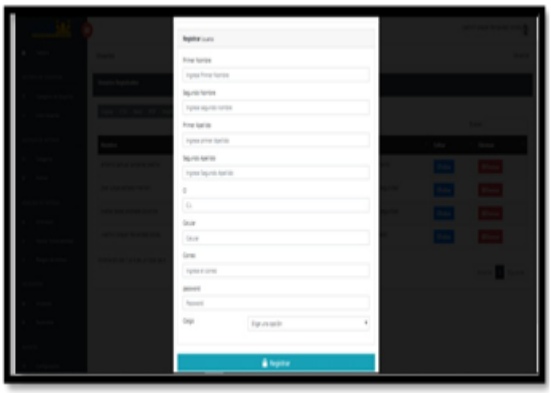


FIGURA VI
INTERFAZ DE REGISTRO DE USUARIO

Una vez realizado los diagramas de secuencia y el prototipo se proceden a codificar y desarrollar el módulo correspondiente

- Modulo de gestión de usuarios

.

Se procederá elaborar el diagrama de secuencia del módulo de registro de usuario

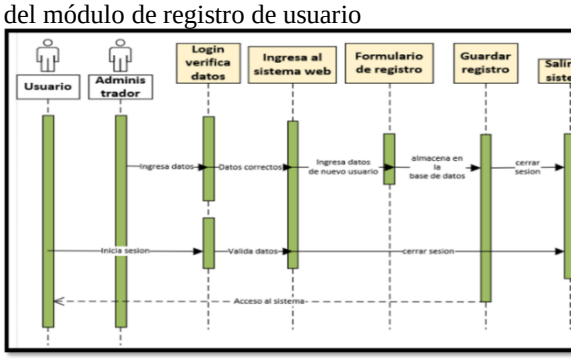


FIGURA VII
DIAGRAMA DE SECUENCIA

El diagrama de secuencia establece los pasos y la navegación del usuario en el modulo

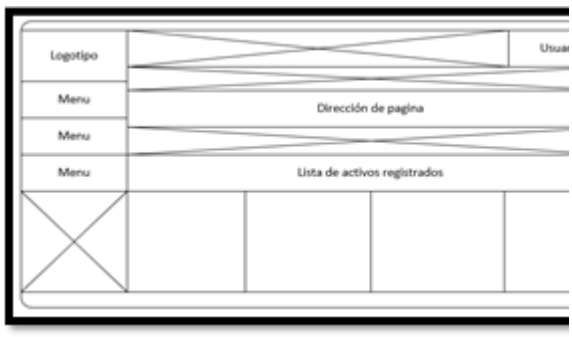


FIGURA VIII
PROTOTIPO DE INTERFAZ DE GESTIÓN DE USUARIO

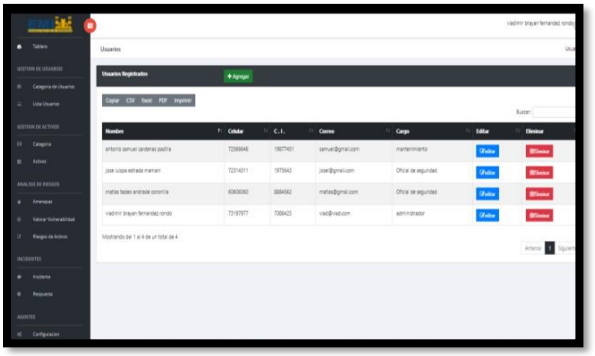


FIGURA IX
INTERFAZ GESTIÓN DE USUARIOS

Una vez realizado los diagramas de secuencia y el prototipo se proceden a codificar y desarrollar el módulo correspondiente

5)Sprint2

•Módulo de gestión de activos

Se procederá elaborar el diagrama de secuencia del módulo de registro de activo

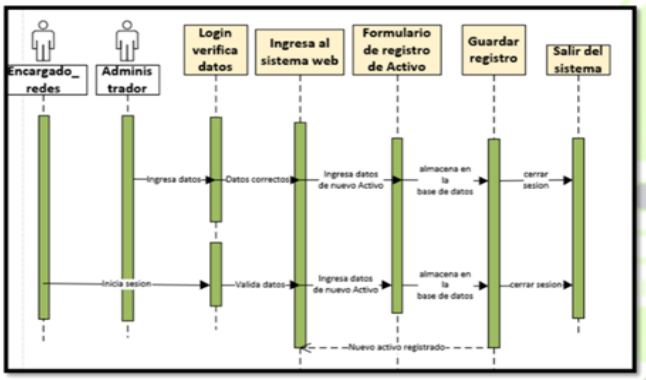


FIGURA X
DIAGRAMA DE SECUENCIA

El diagrama de secuencia establece los pasos y la navegación del usuario en el modulo

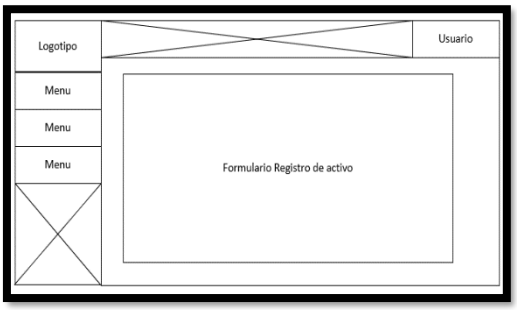


FIGURA XI
PROTOTIPO DE REGISTRO DE ACTIVO

El prototipo de interfaz de registro de usuario corresponde se debe maquetar mediante alguna herramienta de vista de navegación web

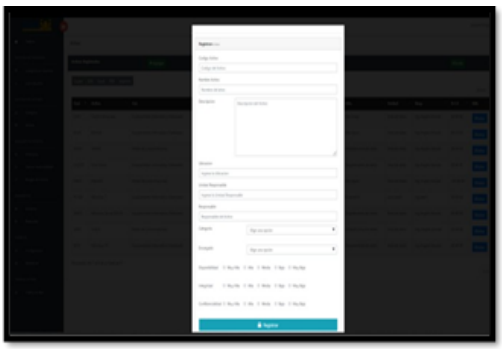


FIGURA XII
INTERFAZ REGISTRO DE ACTIVO

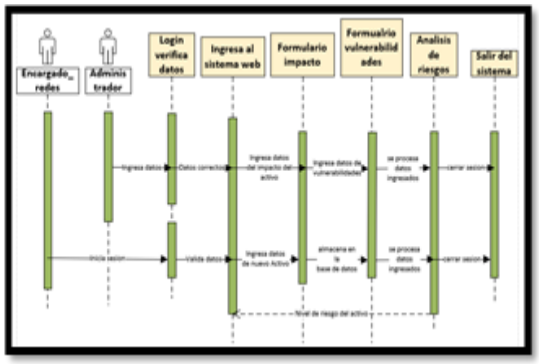


FIGURA XIII
DIAGRAMA DE SECUENCIA

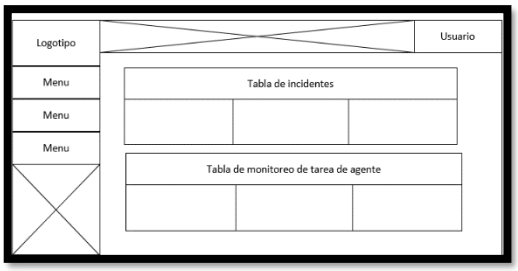


FIGURA XIV
PROTOTIPO DE INTERFAZ

El prototipo de interfaz de registro de usuario corresponde se debe maquetar mediante alguna herramienta de vista de navegación web

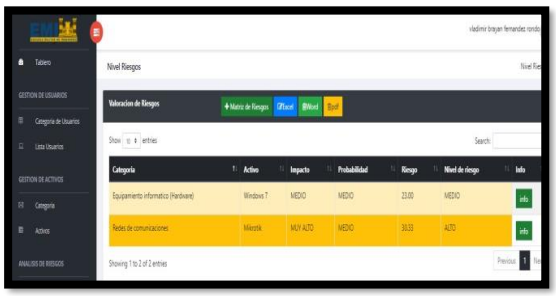


FIGURA XV
INTERFAZ DE ANÁLISIS DE RIESGO

Una vez realizado los diagramas de secuencia y el prototipo se proceden a codificar y desarrollar el módulo correspondiente
Una vez realizado los diagramas de secuencia y el prototipo se proceden a codificar y desarrollar el módulo correspondiente

•Modulo análisis de riesgos.

FIGURA XIII DIAGRAMA DE SECUENCIA

6) Sprint 3

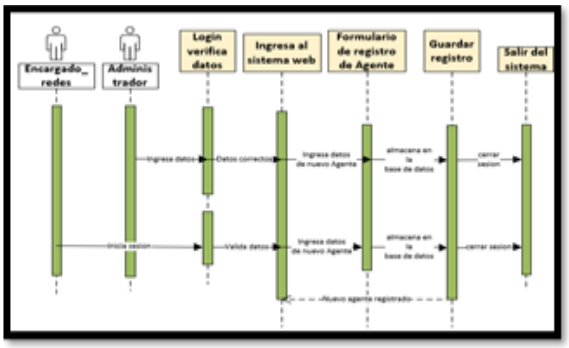


Figura XVI
DIAGRAMA DE SECUENCIA

El diagrama de secuencia establece los pasos y la navegación del usuario en el modulo

El diagrama de secuencia establece los pasos y la navegación del usuario en el modulo

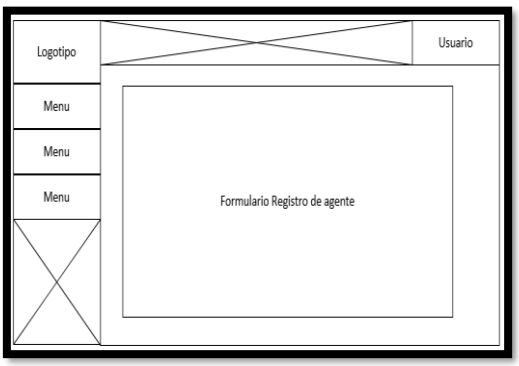


FIGURA XVII
PROTOTIPO DE INTERFAZ

El prototipo de interfaz de registro de usuario corresponde se debe maquetar mediante alguna herramienta de vista de navegación web

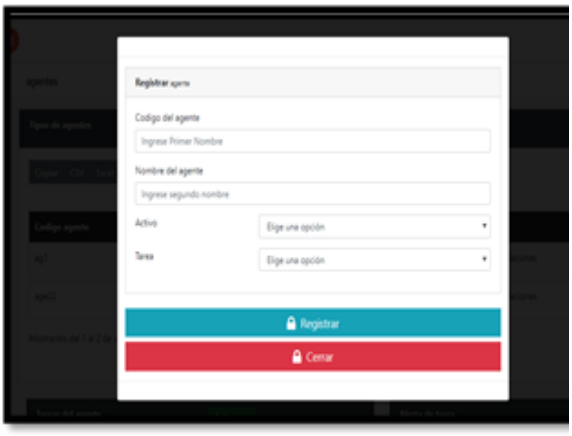
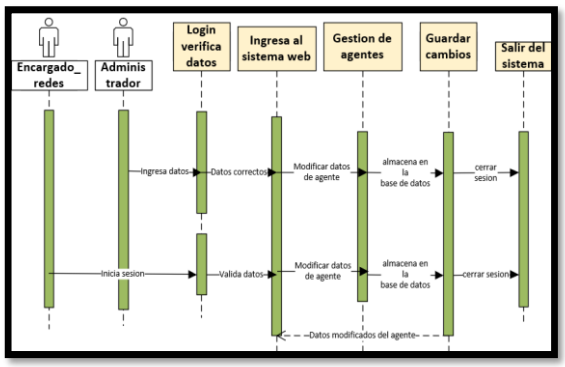


FIGURA XVIII
INTERFAZ DE REGISTRO DE AGENTE

Una vez realizado los diagramas de secuencia y el prototipo se proceden a codificar y desarrollar el módulo correspondiente

- Módulo de gestión de agentes



El diagrama de secuencia establece los pasos y la navegación del usuario en el modulo

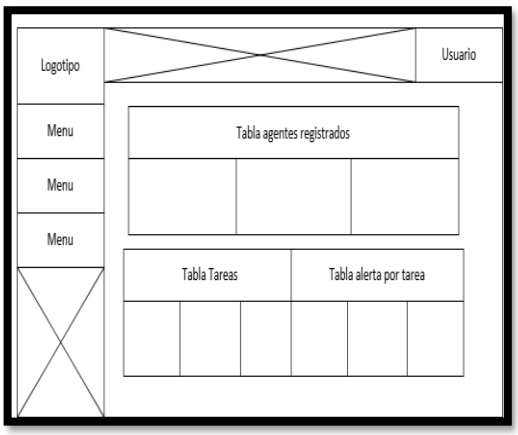


FIGURA XIX
PROTOTIPO DE INTERFAZ

El prototipo de interfaz de registro de usuario corresponde se debe maquetar mediante alguna herramienta de vista de navegación web

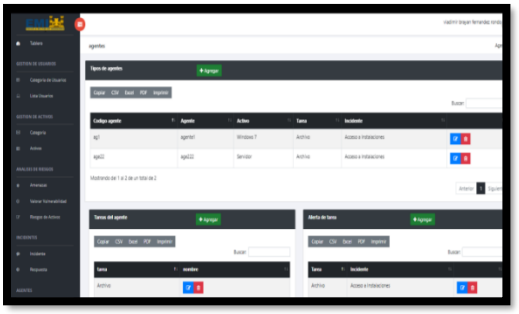


FIGURA XX
INTERFAZ DE GESTIÓN DE AGENTES

Una vez realizado los diagramas de secuencia y el prototipo se proceden a codificar y desarrollar el módulo correspondiente

- Desarrollo del agente reactivo simple.

Una vez establecido el módulo de navegación del módulo de Agentes se procederá a desarrollar los Agentes reactivos simple descrito en el capítulo III del marco teórico, el cual tiene como característica principal la reacción ante un estímulo del medio en el que se encuentra el Agente en nuestro caso el medio será la información del Sistema de Archivos del Sistema Operativo donde se instale el Agente.

Con la ayuda del diseño de roles y tareas previamente realizados se procederá a elaborar el modelo arquitectónico de los agentes con el cual se observará donde, y como están posicionados dentro del sistema.

Para la elaboración del agente es necesario la Figurar 26 donde se muestra que el agente está compuesto por la suma de la arquitectura más la programación que ambos darán como resultado el funcionamiento del agente.:

a) a)Agente Estado

1.- Casuística

Para la elaboración del diseño del modelo del agente estado se tomará en cuenta la siguiente situación que se establece en el plan de incidentes de seguridad de la información como divulgación o perdida de información donde el control realizado por el agente se realizará en archivos dentro del sistema permitiendo así gestionar el estado de estos archivos.

2.-Percepciones:

- Solicitar el estado del activo 3.-Acciones
- Informar acerca del estado del activo 4.-Metas
- Guardar en la base de datos el estado del activo 5.-Ambiente

- Estado de funcionamiento del activo

6.- Diseño del modelo de Agente Estado

FIGURA XXI
DISEÑO DEL MODELO DE AGENTE

Se realizo el diseño del modelo de agente para verificar el estado de archivos en un activo

b) Agente Escáner

1.-Casuistica

Para la elaboración del diseño del modelo del agente escáner se tomara como caso la situación que se establece en plan de incidentes de seguridad de la información como violación a las políticas de seguridad donde las políticas pueden estar

establecidas por las conexiones que el usuario un dispositivo realiza hacia otros dispositivos externos, el acceso hacia servicios preconfigurados, evitar los controles de seguridad perimetral, entre otros los cuales son relacionados con los controles de seguridad de las comunicaciones.

2.-Percepciones:

- Solicitar escaneo de red 3.-Acciones
- Consultar puertos TCP/UDP 4.-Metas
- Guardar en la base de datos el estado abierto o cerrado de los puertos.

5.-Ambiente

•Puertos TCP/UDP

6.- Diseño del modelo del Agente de Escaneo

A continuación, se realizará el diseño del modelo del agente de escaneo mediante un diagrama de casos de uso de segundo nivel

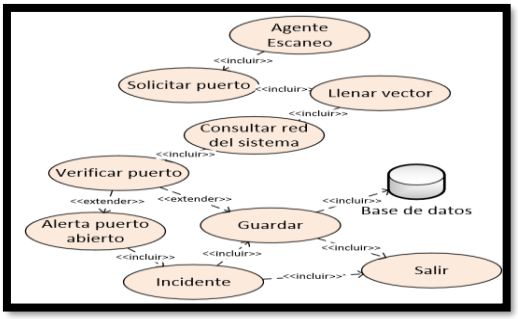


FIGURA XXII
DISEÑO DEL MODELO DE AGENTE

Se realizo el diseño del modelo de agente para verificar el estado de archivos en un activo

c) Agente Trafico

1.-Casuistica

Se tomará como caso para el diseño del modelo del agente la situación de ataques en el tráfico de red, que corresponden al análisis de puertos TCP/UDP ya que este análisis de puertos es realizado antes de que suceda un ataque por la red, que se estable en el plan de incidentes de seguridad de la información, enumerando así los puertos abiertos y cerrados de la víctima que se encuentre dentro de la red para posteriormente explotar una vulnerabilidad relacionada con los puertos analizados.

Para este modelo se utilizará la herramienta Snort que permitirá realizar el análisis de la red siendo esta un sistema de detección de intrusos que funciona en base a reglas que pueden ser configurada de acuerdo a los criterios de control que se requiera implementar como indica la documentación de la misma herramienta.

2.-Percepciones:

- Solicitar captura de trafico de red 3.-Acciones
- Recolectar el tráfico de red del protocolo TCP/IP 4.-Metas
- Guardar en la base de datos el tráfico de red capturado 5.-Ambiente
- Protocolo TCP/IP

6.- Diseño del modelo de Agente de trafico

A continuación, se realizará la elaboración del diseño del modelo del agente de tráfico representado en un diagrama de casos de uso de segundo nivel.

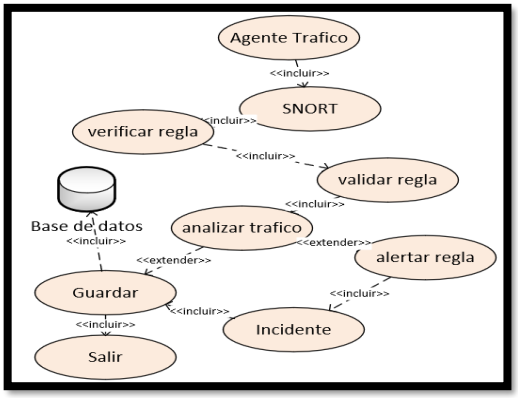


Figura XXIII
DISEÑO DEL MODELO DE AGENTE

Se realizo el diseño del modelo de agente para verificar el estado de archivos en un activo
Se procederá a elaborar el modelo de la arquitectura del agente especificado las percepciones, acciones, metas y ambiente para realizar la arquitectura de organización

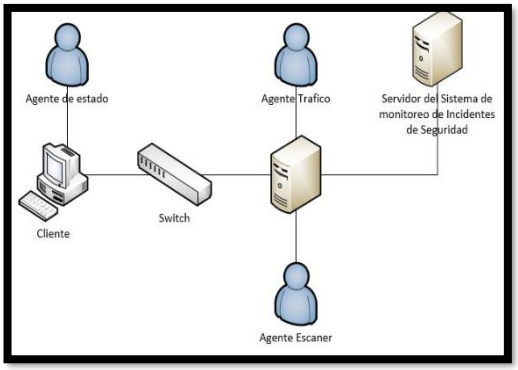


FIGURA XXIV
TOPOLOGÍA DE LA ARQUITECTURA DE AGENTES

Se realizo el diseño de topologia de la arquitectura de distribucion de los agentes

Se mostrará como los agentes se distribuyen dentro de la red y envían registros hacia el sistema central donde se podrá visualizar la información que es enviada por los agentes para la elaboración de la misma se ubicara un dispositivo de red, clientes y el servidor donde se aloja el sistema.

Los indicadores son los eventos que nos señalan que posiblemente un incidente de seguridad ha ocurrido generalmente algunos de estos elementos son:

- Alertas en sistemas de seguridad
- Caídas de servidores
- Reportes de usuarios
- Software antivirus dando informes
- Otros funcionamientos fuera de lo normal del sistema

Por lo tanto, se estableció controlar el tráfico de red y el estado de los dispositivos que pertenecen a la red, de manera que los agentes informen y guarden esta información en una base de datos, la cual será consultada posteriormente para generar reportes y generar alertas acerca de la presencia de incidentes de seguridad con lo que se identificara la presencia de incidentes de seguridad.

a) Diseño de interfaces
Para realizar el diseño de interfaces es necesario explicar mediante el diagrama de secuencias los pasos necesarios para la navegación por el módulo del agente

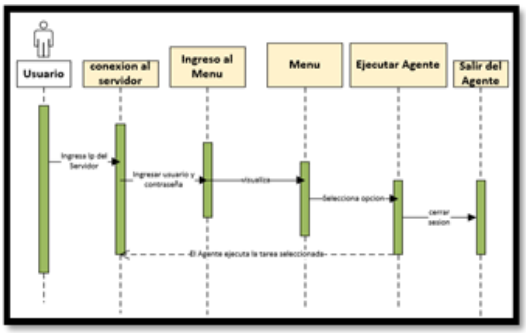


FIGURA XXV
DIAGRAMA DE SECUENCIA

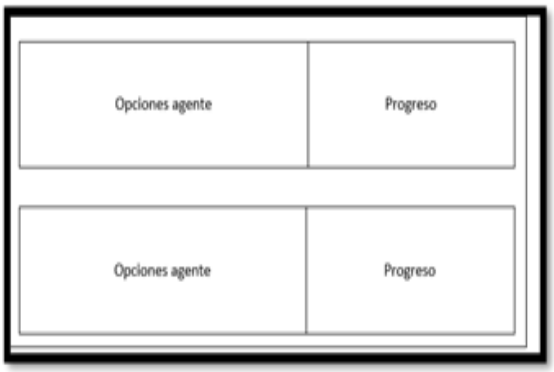


FIGURA XXVI
PROTOTIPO DE INTERFAZ

FIGURA XXVII
INTERFAZ DE AGENTE
A continuación, se desarrollará el módulo de Gestión de incidentes.

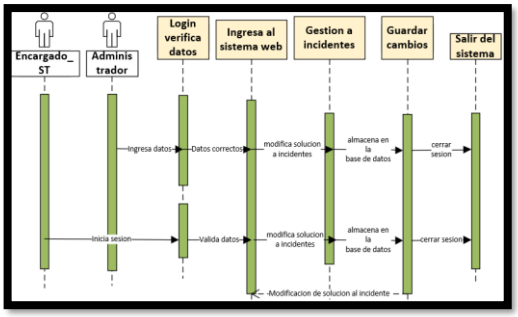


FIGURA XXVIII
DIAGRAMA DE SECUENCIA

El diagrama de secuencia establece los pasos y la navegación del usuario en el modulo

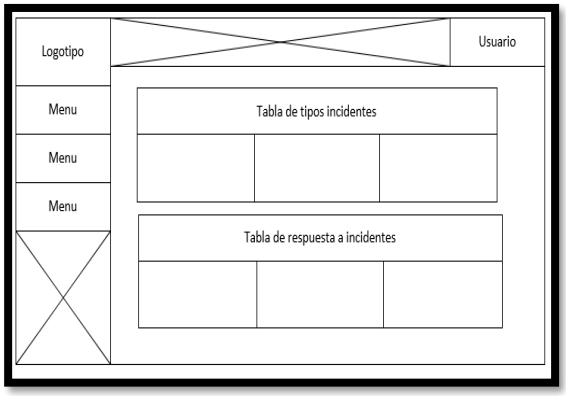


FIGURA XXIX
PROTOTIPO DE INTERFAZ

El prototipo de interfaz de registro de usuario corresponde se debe maquetar mediante alguna herramienta de vista de navegación web

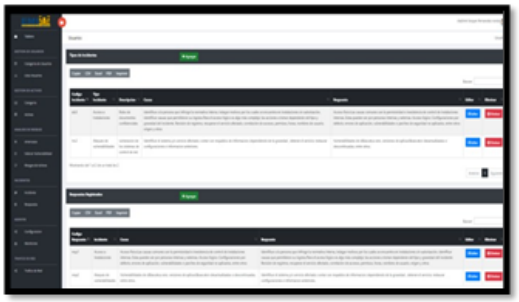


FIGURA XXX
INTERFAZ DE MONITOREO

7) Sprint 4

Para el desarrollo del presente sprint se ha tomado en cuenta las historias de usuario número diez, once, y doce que corresponde al Gestión de incidentes, Reportes de incidentes y reportes de análisis de riesgos.

Una vez realizado los diagramas de secuencia y el prototipo se proceden a codificar y desarrollar el módulo correspondiente

8) Sprint 5 Pruebas del Sistema

En el presente sprint se realizará las pruebas de los módulos previamente desarrollados en pruebas unitarias donde se realizarán tablas mostrando las pruebas realizadas

•Pruebas

Para las pruebas se utilizo herramientas con las cuales se levantaran alertas en el sistema, para esto se utilizara las siguientes herramientas

Nmap Metasploit

Las pruebas que se realizaran correspondes a la etapa de enumeración, escaneo de red y vulnerabilidades del análisis de vulnerabilidad.

IV. CONCLUSIONES Y RECOMENDACIONES

A)CONCLUSIONES

En la elaboración del presente trabajo de grado se establecieron las siguientes conclusiones:

Se ha realizado el análisis detallado de los procesos que cumple la Escuela Militar de Ingeniería en cuanto al organigrama de funciones de la Dirección de Tecnologías de Información y comunicación referente al área de redes para los cual mediante observación y encuestas al personal perteneciente a la institución se determinó la existencia de personal capacitado para el manejo del sistema y dar una óptima respuesta a incidentes de seguridad.

Se ha determinado el estado y funcionamiento de los dispositivos de red presentes dentro de la institución, así como los servicios que prestan dentro de la misma red, mediante un escaneo de direcciones IP y servicios de red además de realizar el análisis de vulnerabilidades de los servicios de red con el objetivo de encontrar el nivel de riesgo en el que se encuentran los dispositivos de red que a su vez son activos de información de acuerdo con el área de Seguridad Informática presente dentro de la Institución.

Se ha determinado el nivel de riesgo de los activos pertenecientes al área de redes, una vez conocidos los tipos de dispositivos presentes se elaboró el diseño del agente de manera que se pueda capturar tráfico de red detectando así ataques informáticos contra los equipos de la infraestructura de red.

Se ha determinado la categoría de activos de información que corresponde con el plan de

incidentes de seguridad de la información, de manera que se establezcan los activos de

información en una categoría adecuada para el análisis de riesgo.

Se ha realizado pruebas de ataques informáticos de manera que el sistema pueda monitorear y contribuir con el oficial de Seguridad Informática y los encargados pertenecientes a la red de redes de la institución, la información registrada acerca de los incidentes de seguridad quedase registrados en la base de datos del sistema.

Se ha realizado la integración de los agentes para lo cual se determinó el entorno de desarrollo del agente y la conexión hacia la base de datos que mande acerca de la información del activo para que se pueda registrar en la base de datos y así monitorear el estado del agente y la información que envía.

Se ha desarrollado el agente que capture el tráfico de red para la monitorización de la red y la existencia de ataques informáticos sin embargo al realizar las pruebas de funcionamiento se observó que se debe capacitar al personal de seguridad informática para la correcta configuración de las reglas de detección de incidentes de seguridad.

B) RECOMENDACIONES

En la elaboración del presente trabajo de grado se determinó las siguientes recomendaciones para la elaboración de proyectos similares o contribución al mismo.

Se recomienda limitar el uso del sistema en redes internas por la misma seguridad del sistema ante ataques dirigidos y por la información que almacena acerca de los activos de información.
Se recomienda limitar el acceso solo al personal autorizado y capacitado para evitar generar errores dentro del monitoreo de los incidentes de seguridad.

Se recomienda implementar sistema de restauración como ser backups sistemas de almacenamiento con redundancia de datos para evitar la pérdida del sistema de base de datos y del sistema web que tienen información acerca de los activos de información.

Se recomienda capacitar al personal que utilizara el sistema para evitar falsos positivos dentro de la detección de incidentes de seguridad dentro de la red, como también capacitar al personal para el correcto actuar ante los incidentes de seguridad que puedan suceder dentro de la infraestructura de red de la institución.

Se recomienda elaborar un plan de contingencia tecnológica de acuerdo a la normativa vigente en Bolivia, para prevenir ante la ocurrencia de incidentes de seguridad de la información.

RECONOCIMIENTO

Hago reconocimiento por la guía y contribución al desarrollo del presente trabajo de grado a los docentes que realizaron la revisión del proceso de la elaboración del presente documento.

V.REFERENCIAS

[1] R. S. Pressman, Ingenieria de Software, España: McGraw-Hill, 2010.
[2] I. Sommerville, Ingenieria de Software, Mexico: Cámara Nacional de la Industria Editorial Mexicana, 2011.
[3] J. Schmuller, Aprendiendo UML en 24 horas, Mexico : Editorial Division Computacional, 2000.
[4] CTIC-EPB, «Centro de Gestion Informaticos,» 2017.[En línea]. Available: https://www.cgii.gob.bo.

[5] L. Fabricio y R. Javier, «Terminos y definiciones,» octubre 2005. [En línea]. Available: http://www.iso27001.ex.

[6] J. R. Gerardo y R. P. Sonia, «los recursos de red y su monitoreo,» 2018.
[7] «deficionesyquees,» 2014. [En línea]. Available:https://definicionyque.es.
[8] CS-PIB-UPC, «ECDSI,» 2018.[Enlínea]. Available: https://www.cs.upc.edu/.

[9] I. N. d. C. d. E. INCIBE, «INCIBE-CERT,» enero 2019. [En línea]. Available: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

[10] U. P. C. CS-FIB-UPC, «COMPUTER SCIENCE DEPARTMENT,» 2018. [En línea]. Available: https://www.cs.upc.edu/~bejar/ecsdi/Teoria/ECSDI 03b-Prometheus.pdf.
[11] S. Russell y P. Norvig, Inteligencia Artificial un enfoque moderno, Ribera del Loira, 28: PEARSON

PRENTICE HAL, 2003.
[12] M. Soriano, Seguridad en redes y seguridad de la información, Technická 2, Praha 6, Czech Republic: České vysoké učení technické v Praze, 2014.
[13] S. M. Quiroz-Zambrano y D. G. Macías-Valencia, Seguridadeninformática, Manabi,Ecuados: Universidad Laica Eloy Alfaro de Manabí, 2017.
[14] I. T. S. d. e. Mante, Antologia de Ingenieria de Sistemas, Mexico: Instituto Tecnologico Superior de el Mante, 2017.
[15] B. O. Johansen, Introduccion al Teoria General de Sistemas, Mexico: Editorial Mexicana, 1993.
[16] P. M. Jordi y R. M. Jose, Introduccion a la ingenieria de software, Catalunya: FUOC. Fundación para la Universitat Oberta de Catalunya, 2013.
[17] M. S. Lujan, Progrmacion de aplicaciones web, San vicente: Editorial Club Universitario, 2002.

Fecha de Envió del Articulo: 12/05/2020
Fecha de Aceptación de artículo: 28/05/2020