DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN PREVIO LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA: IMPLEMENTACIÓN DE UNA APLICACIÓN DE BUSINESS INTELLIGENCE QUE PERMITA EL ANÁLISIS DE VULNERABILIDADES PARA MITIGAR EL IMPACTO DE LOS INCIDENTES EN LA RED DE INVESTIGACIÓN CEDIA. CASO DE ESTUDIO ESPE

AUTOR: REYES MENA, FRANCISCO XAVIER

DIRECTOR: ING. FUERTES DÍAZ, WALTER MARCELO PhD

SANGOLQUÍ 2017

CERTIFICADO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

Certifico que el trabajo de titulación, "Implementación de una Aplicación de Business Intelligence que Permita el Análisis de Vulnerabilidades para Mitigar el Impacto de los Incidentes en la Red de Investigación CEDIA. Caso de estudio ESPE" realizado por el señor Francisco Xavier Reyes Mena, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar al señor Francisco Xavier Reyes Mena para que lo sustente públicamente.

Sangolquí, 1 de septiembre de 2017

Ing. Walter Fuertes, PhD.

DIRECTOR

AUTORÍA DE RESPONSABILIDAD

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

Yo, Francisco Xavier Reyes Mena, con cédula de identidad N° 1715833529, declaro que este trabajo de titulación "Implementación de una Aplicación de Business Intelligence que Permita el Análisis de Vulnerabilidades para Mitigar el Impacto de los Incidentes en la Red de Investigación CEDIA. Caso de estudio ESPE" ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 1 de septiembre de 2017

Francisco Xavier Reyes Mena

C.C 1715833529

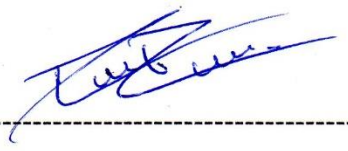
AUTORIZACIÓN

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

Yo, Francisco Xavier Reyes Mena, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación "Implementación de una Aplicación de Business Intelligence que Permita el Análisis de Vulnerabilidades para Mitigar el Impacto de los Incidentes en la Red de Investigación CEDIA. Caso de estudio ESPE" cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 1 de septiembre de 2017



Francisco Xavier Reyes Mena

C.C: 1715833529

DEDICATORIA

La presente tesis está dedicada a Dios, por darme la fuerza para seguir adelante y nunca decaer ante las circunstancias que se presentaron, además de brindarme un apoyo que lo puedo sentir en cada paso que doy.

Agradecer a mis padres por ser el ejemplo de lucha, sacrificio y constancia ante las circunstancias que nos presente la vida y también por ser el sustento por el cual estoy llegando a culminar mis estudios universitarios. A mi madre Patricia Mena por siempre brindarme su apoyo y cariño, los cuales han sido fundamentales para llegar a ser la persona que ahora soy. A mi padre Justo Reyes, cuyo arduo trabajo me ha servido de ejemplo para exigirme más y poder alcanzar una meta cumpliendo todos los objetivos propuestos.

A mi hermano cuyo ejemplo ha fomentado en mi la responsabilidad con la que se debe ejecutar un proyecto, además del cariño y el corazón que debe prevalecer en cada acción que haga en un trabajo.

AGRADECIMIENTO

Quiero agradecer en primer lugar a Dios, por regalarme un día más de vida permitiéndome llegar hasta donde he llegado, brindarme una familia maravillosa, darme la fuerza suficiente para terminar este proyecto. Gracias por acompañarme en cada paso que doy.

A mis padres, por ser sustento y ejemplo, que ha generado en mi la responsabilidad para llegar a terminar este proyecto. A mi madre Patricia Mena por sus conejos, su amor y comprensión que me ha llevado a realizar mis actos en pro del bien. A mi padre Justo Reyes por su sacrificio y su ejemplo de trabajo responsable y ético, el cual ha sido mi referente para culminar este objetivo.

A mi hermano por su ayuda y apoyo incondicional, es un ejemplo para mí.

A mi director de tesis, Ing. Walter Fuertes, PhD, por la confianza brindada para llevar a cabo este proyecto, por su guía, consejos y ejemplo, que han impulsado mi ánimo para realizar un proyecto de calidad.

A mis profesores, cuyo conocimiento han servido de base fundamental para llegar a culminar mi proyecto de grado, además de generar un aprendizaje en valores que han forjado a la persona que ahora soy.

A mis amigos por bríndame su apoyo y tener una palabra de aliento en momentos en los que mi ánimo decaía.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En la actualidad las universidades están siendo amenazadas por ataques informáticos, lo que puede deteriorar su imagen, reducir estudiantes y hasta terminar en robo de información o alteración. Esta investigación tiene como objetivo diseñar una solución mediante Inteligencia de Negocios que actúe como un factor estratégico en el análisis de vulnerabilidades de un equipo de emergencias ante incidentes informáticos CSIRT, de una corporación del desarrollo de Internet avanzado que agrupa a varias universidades miembros del Ecuador. Para llevarlo a cabo se aplicó la metodología de Investigación-acción con un enfoque cualitativo, dividido en tres fases: Primera, se realizó una evaluación cualitativa de dos herramientas de análisis de intrusos como son, "Passive Vulnerability Scanner" y "Snort" que estaban siendo utilizadas, para verificar si eran excluyentes o complementarias. Paralelamente, se iban registrando los logs en tiempo real de los incidentes registrados por dichas herramientas en una base de datos relacional MySQL. Segunda, se aplicó la metodología de Ralph Kimball, para el desarrollo de varias rutinas que permitan aplicar el proceso "Extraer, Transformar y Cargar" de los logs no normalizados que luego serán procesados por una interfaz gráfica. Tercera, se construyó una aplicación de software mediante SCRUM, que permita vincular los logs obtenidos a la herramienta Pentaho BI, con el propósito de generar alertas tempranas como un factor estratégico. Los resultados muestran la funcionalidad de esta solución que ha generado alertas tempranas y que en consecuencia ha incrementado el nivel de seguridad de los miembros de este CSIRT.

PALABRAS CLAVES:

- **INTELIGENCIA DE NEGOCIOS**
- **CIBERSEGURIDAD**
- **DATAMART**
- **CSIRT**
- **VULNERABILIDADES**

ABSTRACT

Nowadays, Universities are being threatened by computer attacks, which can deteriorate their image, lost customers and even end up stealing information or alterations. This research aims to design a solution through Business Intelligence that acts as a strategic factor in the vulnerability analysis of an emergency equipment in front of computer incidents CSIRT, an advanced Internet development corporation that clusters many universities of Ecuador. In order to carry it out, the methodology of Action Research was applied with a qualitative approach, divided into three phases: First, a qualitative evaluation of two intrusion analysis tools such as "Passive Vulnerability Scanner" and "Snort" were being used, to verify if they were exclusive or complementary. At the same time, the real-time logs of the incidents registered by those tools were recorded in a MySQL relational database. Second, Ralph Kimball's methodology was applied for the development of several routines that allow to apply the process "Extract, Transform and Load" of non-normalized logs that will then be processed by a graphical interface. Third, a software application was built using SCRUM to link the logs obtained to the Pentaho BI tool, in order to generate early alerts as a strategic factor. The results show the functionality of this solution that has generated early alerts and have consequently increased the security level of the CSIRT members.

KEYWORDS:

- **BUSINESS INTELLIGENCE**
- **CYBERSECURITY**
- **DATAMART**
- **CSIRT**
- **VULNERABILITIES**

CAPÍTULO I
INTRODUCCIÓN

1.1 Antecedentes

En la investigación realizada por Dolystrini Marquéz y Ana Victoria Marcano, se establece que las "Universidades son catalogadas como una comunidad con diversos intereses que reúne a profesores y estudiantes en la tarea de buscar la verdad y afianzar los valores trascendentales del hombre, y como una organización donde la gestión del conocimiento debe estar enmarcada dentro de la realidad de un mundo cada vez más globalizado y competitivo. Hoy en día existe una tendencia en las universidades hacia el uso de la tecnología, ya que facilita que la información tenga vehículos de entrega y difusión accesibles y de amplio alcance, así como la creación de software de administración académica y el uso de bibliotecas electrónicas" (Márquez & Marcano, 2012). Es por esto que se puede considerar a las universidades como blanco de ataques que buscan conseguir información del conocimiento que generan y de quienes forman parte de estas instituciones. Así mismo el incremento de uso de las tecnologías a implicado beneficios en todas las industrias (medicina, turismo, educación, entretenimiento, etc.), y ha abierto un campo de vulnerabilidades que pueden llegar a ser explotadas (Importancia.org, 2016).

Cada tecnología implementa potencialidades delictivas y ofrece oportunidades para cometer infracciones, como se puede visualizar en la página www.zone-h.org en donde se encuentran registrados 58.884 ataques exitosos realizados desde 1998 hasta el 19 de julio del 2016 a entidades educativas a nivel mundial, lo cual refleja la importancia de un Equipo de Respuesta a Incidentes Informáticos (CSIRT de las siglas en ingles Computer Security Incident Response Team) Académico, estos son importantes para reducir ataques a entidades educativas.

Los CSIRT se originan a fines de los '80 con la aparición de "Morris", considerado el primer gusano informático que se propagó rápidamente y logró infectar aproximadamente 6000 equipos a lo largo de todo el mundo (Lanfranco, Macia, Venosa, Molinari, & Díaz, 2010). Debido a esto, los administradores de sistemas y gestores de la tecnología de la información, vieron la necesidad de cooperar entre sí para poder enfrentarse este tipo de casos. Éste fue un paso decisivo para establecer un

enfoque común y más organizado en el tratamiento de los incidentes relacionados a la seguridad de la información. En 1988 se crea el primer CSIRT llamado CERT Coordination Center (CERT/CC) en la Universidad Carnegie Mellon (Pittsburgh, Pensilvania). En 1992 el proveedor académico holandés SURFnet puso en marcha el primer CSIRT de Europa, llamado SURFnetCERT. Desde entonces, el número de equipos de similares características ha ido creciendo paulatinamente, y su distribución ahora incluye a muchos países del mundo (Lanfranco, Macia, Venosa, Molinari, & Díaz, 2010).

La empresa Digiware en su informe anual 2015, develó que Ecuador es el cuarto país que más recibe ataques cibernéticos en Latino América con un 11,22% de los ataques recibidos. En el mismo informe Digiware revela que el continente recibe el 19% de los ataques a nivel global (Freire, 2015). Estos valores incrementan la necesidad de organismos de control y de manejo de incidentes de seguridad informática.

En el Ecuador existen tres instituciones para el control y manejo de incidentes de seguridad informática: CSIRT CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado, el cual se enfoca en la protección de Universidades miembro), EcuCERT (Equipo Ecuatoriano de Respuesta ante Emergencias Informáticas) y CSIRT UTPL (Equipo de Respuesta a Incidentes Informáticos de la Universidad Técnica Particular de Loja) , cada uno de ellos proporciona seguridad a un nivel establecido, estos son: Académico, Nacional y Académico, respectivamente (Registro de Direcciones de Internet para América Latina y Caribe, 2009).

Los CSIRT académicos dan seguimiento a eventos que se han suscitado con éxito, como el caso registrado en enero del presente año, en el cual una red de ciber-delincuentes accedió a los sistemas informáticos de universidades privadas del Ecuador para registrar como alumnos a personas que nunca cursaron estudios superiores. Este delito incluyó a una lista de 366 personas que habrían inscrito ilegalmente sus títulos falsos en la base de datos de la Senescyt, este hecho ha permitido constatar las vulnerabilidades que presenta la red y la importancia que

implica para las universidades el protegerse de manera adecuada ante la inminente amenaza de ataques avanzados (Canal News Ecuador, 2016).

Las instituciones educativas guardan información de contactos, direcciones, datos socioeconómicos, cuentas bancarias, etc. Todos estos registros son sensibles y por tanto su pérdida puede implicar gastos y daños, no solamente económicos (Canal News Ecuador, 2016).

El CSIRT-CEDIA es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad (REDCEDIA, 2014); sin embargo, requiere de un sistema informático el cual recopile incidentes e información de sus miembros, para proveer alertas tempranas.

Es así que, según el informe de Ciberseguridad elaborado por el Banco Internacional de Desarrollo (BID) y la Organización de los Estados Americanos, se ha establecido que en Ecuador la capacidad de respuesta a incidentes de seguridad informática se encuentra en un nivel formativo (Existe un equipo de respuesta con roles y responsabilidades identificadas, la actividad se concentra en la detección y respuesta a incidentes cibernéticos específicos de la organización), pero se debe seguir escalando a los niveles superiores, los cuales son: establecido, estratégico y dinámico. Para avanzar al nivel nombrado como establecido, debe existir un desarrollo e implementación de un plan de gestión de vulnerabilidades, además que los incidentes se clasifiquen en consonancia con los planes de respuesta (Porrúa & Contreras, 2016). Por esto, la presente investigación planteó una opción para mejorar la gestión de incidentes en el CSIRT CEDIA.

Este desarrollo formó parte de la 3era fase del Proyecto de Investigación titulado: “Plataformas Computacionales de Entrenamiento, Experimentación, Gestión y Mitigación de Ataques a la Ciberseguridad” código PIC-ESPE-015-019 planteado por el grupo de investigación RACKLY de las Universidad de las Fuerzas Armadas ESPE; que tuvo cofinanciamiento de CEDIA.

1.2 Problemática

Como resultado de una evaluación realizada por CEDIA a Proveedores de Servicio de Internet (ISP de las siglas en ingles Internet Service Provider) dentro del territorio ecuatoriano, se muestra que en el año 2014 se registraron más de 3000 ataques de desfiguración de páginas Web (ECU-CERT, 2014). Desde entonces el ECU-CERT trabaja con ISP públicos y privados en la reducción de amenazas en Internet, como, por ejemplo: En cooperación con la Corporación Nacional de Telecomunicaciones (CNT) y proveedores privados se bloqueó dominios de red para evitar su funcionamiento, dejando 5000 usuarios ilegales fuera de línea (ECU-CERT, 2014).

El número de incidentes y amenazas en la red está en constante crecimiento junto con necesidad de información privilegiada, es por eso que las comunidades científicas y académicas deben incrementar sus medidas de seguridad, es en ese escenario que el propósito del CSIRT-CEDIA es:

i. Apoyar a los miembros de la comunidad del CEDIA a implementar medidas proactivas con el objetivo de reducir los riesgos de incidentes de seguridad informáticos;
ii. Apoyar a la comunidad del CEDIA a responder a estos incidentes cuando ocurran.

Esto mejorando la capacidad de respuesta a incidentes informáticos, la oferta de soluciones para la detección de vulnerabilidades y fortaleciendo los sistemas de detección de intrusiones (CSIRT-CEDIA, 2014).

Según John Lyon, experto en cibercrimen y ciberseguridad, "en 2020 ya no se podrá proteger nuestras redes frente a los ataques", quien alerta a los Gobiernos y a los ciudadanos de la importancia de empezar ya a defender nuestros sistemas o después "será demasiado tarde" (Lyon, 2015).

1.3 Justificación

El escenario de las telecomunicaciones a nivel global y los indicadores que muestran el estado de la ciberseguridad, definen la necesidad de una mejora continua de los procesos en el manejo de incidentes, la misión de CEDIA es promover, coordinar y desarrollar redes avanzadas de informática y telecomunicaciones para impulsar, en forma innovadora, la investigación científica, tecnológica y la educación en el Ecuador (REDCEDIA, 2014). Esto obliga al CSIRT-CEDIA a mantener la vanguardia en el desarrollo e implementación de soluciones que aseguren el funcionamiento óptimo de la red de Internet avanzado.

En el informe de Ciberseguridad 2016 se muestra que Ecuador se encuentra en un nivel formativo tomando en cuenta el Factor Tecnología de dicho informe, de este factor se menciona que la etapa formativa de "Centro de mando y control" se refiere a la falta de una estructura nacional de Coordinación y la etapa formativa de "Capacidad de respuesta a incidentes" se refiere a la existencia de equipos de respuesta, pero la actividad se concentra en la detección y respuesta a incidentes específicos de la organización. Es necesario que exista mayor coordinación y cooperación entre instituciones involucradas. CEDIA como red de Instituciones educativas y de investigación tiene una mayor capacidad de desarrollar proyectos que involucren miembros de distintos intereses, ya que es una organización sin fines de lucro proyectada a fomentar proyectos de investigación en el área de las TIC (Porrúa & Contreras, 2016).

El CSIRT es un equipo de respuesta a incidentes de seguridad, este equipo es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad. El CSIRT brinda sus servicios a entidades relacionadas o que dependan de una corporación, organización de gobierno o educativa. El CSIRT-CEDIA es el Equipo de Respuesta a Incidentes de Seguridad Informática del CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado) (REDCEDIA, 2014).

Para enfrentar el reto de obtener acciones efectivas antes de un ataque, el uso de Business Intelligence para la administración de los resultados del análisis de

vulnerabilidades, supone un menor tiempo entre la detección de la vulnerabilidad y la solución lo que reduce la probabilidad de sufrir efectos negativos por un ataque.

1.4 Objetivos

1.4.1 Objetivo General

Mejorar el análisis de vulnerabilidades de las Universidades miembros de CEDIA aplicando Business Intelligence, con el fin de mitigar el impacto de los incidentes.

1.4.2 Objetivos Específicos

i. Realizar una evaluación cualitativa de "Passive Vulnerability Scanner" VS "Snort" analizando la funcionalidad de cada uno en un mismo escenario de prueba.
ii. Implementar una aplicación de Business Intelligence que permita la gestión de las vulnerabilidades en el CSIRT-CEDIA.
iii. Realizar pruebas, evaluación y documentación de la propuesta.

1.5 Alcance

El escaneo de vulnerabilidades tiene como objetivo la identificación de los puertos que están abiertos en un sistema, esto mediante el paso sucesivo de solicitudes a diferentes puertos; el escaneo de vulnerabilidades se puede llegar a generar por los siguientes métodos: escaneo activo y escaneo pasivo, en la investigación nos enfocamos en el escaneo pasivo (CCM Benchmark, 2008). El escaneo pasivo analiza los problemas que se suscitan en una red, pero sin interferir en ella, de modo que también se lo denomina análisis no agresivo.

Se realizó una evaluación entre "Passive Vulnerability Scanner" y "Snort", utilizando la herramienta "Pytbull" la cual brinda un diagnostico realizando: módulos de ataques del lado del cliente, test de reglas, pruebas con tráfico malo, pruebas con paquetes fragmentados, módulos de inicio de sesión erróneos, técnicas de evasión, negación de servicios, módulo de replay Pcap y módulo de Shellcodes, también se utilizó los DARPA intrusion detection evaluation datasets, con los cuales se puede

evaluar falsas alarmas y la tasa de detección, esto con el fin de encontrar la herramienta que provea de mayores resultados. Posteriormente, los datos obtenidos se exportaron a una base de datos y se analizó con PENTAHO para generar un módulo de trabajo con Business Intelligence. También se diseñó e implementó un sistema de análisis de vulnerabilidades, utilizando Business Intelligence, el cual interactúe con los datos exportados. El proyecto se desarrolló en la Universidad de las Fuerzas Armadas ESPE, en el laboratorio H403, con los datos del CSIRT en un periodo de 9 meses.

CAPÍTULO II
MARCO TEÓRICO

En este capítulo se especifica los fundamentos teóricos / técnicos que se aplicaron en el desarrollo del sistema de Business Intelligence, en el cual se describe las técnicas, herramientas y métodos, que apalancaron el presente estudio.

2.1 Ciberseguridad

La Unión Internacional de Telecomunicaciones (ITU), en su resolución 181, establece que la ciberseguridad es el: "conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno." (Recomendación UIT–T X.1205, 2010). La ciberseguridad en el mundo se encuentra controlada por nomas, en este subcapítulo se menciona las más importantes:

2.1.1 ISO/IEC 27032

Esta norma internacional establece dos áreas. La primera proporciona una guía técnica para abordar riesgos de Ciberseguridad comunes, tales como: los ataques Ingeniería Social, el acceso secreto y no autorizado a sistemas informáticos, la proliferación de software malicioso, el software espía y otros tipos de software potencialmente no deseables. En consecuencia, se proponen controles que consisten en: prepararse, detectar, monitorear y responder a los ataques. La segunda área se centra en la colaboración, para que se pueda generar un paso de información efectivo y eficiente, además de la coordinación y el manejo de incidentes entre las partes interesadas en el Ciberespacio (NTE INEN-ISO/IEC 27032, 2014).

2.1.2 COBIT 5

ISACA ha elaborado una guía basándose en COBIT 5 “Transforming Cybersecurity Using COBIT 5”, en la cual expone 3 factores de cambio:

- Conectividad permanente: Se lo plantea como factor de cambio debido a que: (i) Los datos críticos y la información están agrupados en la nube; (ii) Están creciendo los hotspots Wi-Fi; (iii) Es fácil tener acceso a los sistemas del trabajo en casa o en movimiento. En consecuencia, estos tres puntos generan como impacto el aumento de la ventana de oportunidades de los ataques.
- Negocio y Sociedad centrados en IT: Se establece como factor de cambio debido a que: (i) Los sistemas en línea son las nuevas infraestructuras críticas; (ii) La dependencia de la sociedad de lo permanente crea ventanas más amplias del tiempo de ataque; (iii) No hay un plan alternativo en caso de emergencias. De este modo, los puntos antes mencionados generan como impacto el aumento del número de procesos de negocio en los que se pueden enfocar los atacantes.
- Nuevo Sistema de Clases por Habilidades Tecnológicas: Se lo plantea como factor de cambio debido a que: (i) Las características de los dispositivos móviles siguen siendo un misterio para muchos; (ii) Menos nativos digitales tienen habilidades TI profundas; (iii) Nuevas aplicaciones y sistemas operativos favorecen la conveniencia sobre el control de los usuarios. Por consiguiente, los puntos antes mencionados generan como impacto un aumento del papel del error humano para permitir el cibercrimien (Analítica, 2013).

En el documento La ley de la ciberseguridad de la Information Security Community el abogado en TIC Jorge Navarro establece el nivel de contribución realizada por estándares a la ciberseguridad, la cual se expone en la tabla 1.

Tabla 1

Nivel de Contribución por Estándar

ESTÁNDAR	NIVEL DE CONTRIBUCIÓN
ISO/IEC 27001 (2005, 2013), Information Technology - Security techniques - Information security management systems - Requirements.	ALTO
ISO/IEC 27002 (2009 2013), Information Technology - Security techniques - Code of practice for security management.	ALTO
ISO/IEC 270052008, Information Technology - Security techniques - Information security risk management.	BAJO
ISO/IEC 270062011, Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.	MEDIO
ISO/IEC TR 27008:2011, Information technology -- Security techniques -- Guidelines for auditors on information security controls.	BAJO
ISO/IEC 29100:2011, Information Technology - Security techniques -- Privacy framework.	ALTO
ISO/IEC 20000-1:2011 Information technology - Service management -Pan 1: Service management system requirements.	ALTO
ISO 22301:2012 Societal security - Business continuity management systems - Requirements.	MEDIO
ISO 31000:2009. Risk management - Principles and guidelines.	BAJO
ISO GUIDE 72, Guidelines for the justification and development of management systems standards.	ALTO
ISO GUIDE 73. Risk management - Vocabulary.	MEDIO
ISO 9000:2005, Quality management systems -- Fundamentals and vocabulary.	ALTO
85 10012:2009 Data protection - Specification for a personal information management system.	ALTO

Continua

NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems.	MEDIO
OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security.	MEDIO
Generally Accepted Privacy Principles (GAPP) from American Institute of CPAs.	ALTO
Control Objectives for Information and Related Technology (COBIT 4.1).	ALTO
Control Objectives for Information and Related Technology (COBIT 5).	ALTO
PCI DSS, Payment Card Industry Data Security Standard.	MEDIO
HIPAA, Health insurance Portability and Accountability Act.	ALTO
SOx, Sarbanes-Oxley Act of 2002.	BAJO
ITIL. Information Technology Infrastructure Library.	MEDIO
The Open Web Application Security Project (OWASP).	BAJO
Cloud Security Arana Cloud Controls Matrix (CCM).	MEDIO

Fuente: (Navarro, 2014)

2.1.3 Framework para la Ciberseguridad del NIST

Para abordar mejor los riesgos de ciberseguridad, el 12 de febrero del 2013 el presidente de Estados Unidos Barack Obama emite al Orden Ejecutiva 13636 la cual establece una mejora de la ciberseguridad de las infraestructuras críticas, con el objetivo de mejorar la seguridad, la resistencia de la infraestructura crítica y mantener un entorno cibernético. La Orden establece el desarrollo de un sistema de marco de seguridad cibernética que aborde un conjunto de estándares y mejores prácticas para ayudar a las organizaciones a gestionar los riesgos de seguridad cibernética. El marco está enfocado en gestionar el riesgo de ciberseguridad. A continuación, en la tabla 2 se visualiza los componentes del Framework. Además, en la tabla 3 se presenta los componentes del núcleo del Framework (National Institute of Standards and Technology - Framework, 2017).

Tabla 2

Componentes del Framework NIST

Componente	Descripción
Núcleo	conjunto de actividades de seguridad cibernética, resultados deseado y referencias aplicables que son comunes en los sectores de infraestructura crítica. El núcleo toma en cuenta normas, directrices y prácticas que brinden comunicación de las actividades y los resultados de la seguridad cibernética en toda la organización. El núcleo está compuesto por cinco funciones.
Niveles de Implementación	establece el contexto de como una organización considera el riesgo de la seguridad cibernética y los procesos de gestión que emplea en el manejo del mismo. Los niveles caracterizan las prácticas de una organización en un rango que va, desde Parcial (nivel uno), hasta Adaptado (Nivel cuatro).
Perfiles	representan los resultados basado en las necesidades empresariales que una organización ha seleccionado de las categorías y subcategorías del núcleo, además pueden ser usados para identificar oportunidades de mejora.

Fuente: (National Institute of Standards and Technology - Framework, 2017)

Tabla 3

Componentes del núcleo del Framework NIST

Función	Categoría
Identificar	• Gestión de activos • Ambiente de negocios • Gobernanza • Evaluación de riesgos • Estrategia de gestión de riesgos
Proteger	• Control de acceso • Concienciación y Capacitación • Seguridad de datos • Procesos y procedimientos de protección de la información • Mantenimiento • Tecnología de protección
Detectar	• Anomalías y eventos • Monitoreo continuo de seguridad • Procesos de Detección
Responder	• Planificación de respuesta • Comunicaciones • Análisis • Mitigación • Mejoras
Recuperar	• Planificación de la recuperación • Mejoras • Comunicaciones

Fuente: (National Institute of Standards and Technology - Framework, 2017)

2.1.4 Controles para la Ciberseguridad

El Instituto de Seguridad, Redes y Auditoría de administración de sistemas (SysAdmin Audit, Networking and Security Institute, SANS) emitió en el 2008 los Controles Críticos de Seguridad (Critical Security Controls, CSC), los cuales en el

2013 fueron transferidos al Centro para la Seguridad de Internet (Center for Internet Security, CIS) (ETHACK, 2014). Los CSC constan de 20 puntos que buscan proteger activos, infraestructura y la organización, además de reducir el compromiso, esfuerzo de recuperación y costos, A continuación, se detallan los 20 controles críticos:

- Inventario de dispositivos autorizados y no autorizados.
- Inventario de software autorizado y no autorizado.
- Configuraciones seguras del hardware y software en dispositivos móviles, computadores, servidores.
- Análisis continuo y eliminación de vulnerabilidades.
- Protección anti-malware.
- Seguridad del software de aplicación.
- Control de dispositivos Wireless.
- Capacidades de recuperación de datos.
- Análisis de habilidades de seguridad y programas de formación.
- Configuraciones seguras para dispositivos de red.
- Limitación y control de los puertos de red, protocolos y servicios.
- Uso controlado de los privilegios administrativos.
- Defensa del perímetro.
- Mantenimiento, monitorización y análisis de los logs de auditoría.
- Control de acceso basado en la necesidad de conocimiento.
- Control y monitorización de las cuentas.
- Prevención de pérdida de datos.
- Gestión y respuesta a incidencias.
- Ingeniería de red segura.
- Realización de tests de penetración.

Cada control cuenta con una explicación, en la cual se establecen las desventajas que conlleva el no implementar, adema se detallan las acciones que las organizaciones están llevando a cabo para implementar, automatizar y medir la efectivad de un determinado ítem (Ortega, 2014).

2.2 Equipos de Respuesta ante Incidentes de Seguridad Informática

Un Equipo de Respuesta a Incidentes de Seguridad Informática (Computer Security Incident Response Team, CSIRT) es un equipo que forma parte de una organización mayor, como un gobierno, una empresa o una institución educativa y se encargan de gestionar los incidentes que ocurran dentro del ámbito informático. Principalmente cumple las siguientes funciones: (i) Gestión de incidentes, (ii) Tratamiento de vulnerabilidades, (iii) Análisis de sistemas, (iv) Formación, (v) Control de tecnología.

Estos servicios varían de un CSIRT a otro y se orientan a las necesidades de una comunidad objetivo, estos pueden tener costo dependiendo de la finalidad del CSIRT, hay equipos que se conforman en torno a una necesidad puntual y con un fin establecido, hay organismos que dependen del gobierno de un país y buscan la difusión de vulnerabilidades para mejorar la seguridad y el conocimiento de la población en su interacción con la tecnología (TechTarget, 2012).

Existen varias asociaciones y organismos que buscan la interacción entre CSIRTs para compartir información de vulnerabilidades detectadas e incidentes ocurridos y reportados, así como, desarrollar proyectos conjuntos en favor de la ciberseguridad. Dentro de ello se puede mencionar a:

- CERT es el Equipo de Respuesta ante Emergencias informáticas. Lo conforma una división del Instituto de Ingeniería de Software de la Universidad de Carnegie Mellon, trabaja con grandes empresas de software en busca de resolver vulnerabilidades y desarrollan herramientas, productos y métodos que ayuden al análisis forense en las organizaciones, análisis de vulnerabilidades y monitoreo de grandes redes de comunicación (CERT, 2016).
- FIRST es el Foro de equipos de respuesta a incidentes, la idea de este foro nació en 1989 un año después de la creación de CERT Cordination Center que surgió ante la aparición del primer virus tipo gusano que se propagó en Internet. Ante este evento quedó de manifiesto la necesidad

> del intercambio de información y cooperación entre equipos de similares características y con objetivos comunes para enfrentar nuevas vulnerabilidades y ataques de alto rango (FIRST, 2017).

En ecuador el EcuCERT dependiente de la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador forma parte de FIRST. Su compromiso radica en contribuir a la seguridad de las redes de telecomunicaciones de todo el país y así como del uso de la red de Internet; para esto ofrecerá productos relevantes, servicios de calidad a nuestros mandantes y cooperará con otros equipos CSIRT dentro y fuera del Ecuador (EcuCERT, 2016).

2.3 Análisis de vulnerabilidades

Las vulnerabilidades se presentan a partir de errores individuales en un determinado componente, sin embargo, nuevas y complejas vulnerabilidades surgen de la interacción entre varios componentes como el kernel del sistema, sistemas de archivos, servidores de procesos, entre otros. Estas vulnerabilidades representan un peligro a la seguridad de la red (Acosta, Buitrago, Newball, Ramírez, & Sánchez, 2004).

En un sistema se busca proteger activos, esto significa los recursos que forman parte del sistema: Hardware, Software, Datos y otros (personas e infraestructura) (Mifsud, 2012).

De estos activos, el más crítico tienden a ser los datos, debido a que estos interactúan con el hardware y el software, y como principal factor, porque representan valor para una empresa como se lo puede ver en la figura 1.

Figura 1. Proceso Generativo de Dato a Valor

Fuente: (Mifsud, 2012)

De acuerdo con Torruela (Torruela González, 2017) , las vulnerabilidades se pueden clasificar según su origen, el cual se lo divide en tres grupos:

- Diseño: a este grupo pertenecen las que pueden ser causadas por una debilidad en el diseño de las redes informáticas, así como también, las políticas de seguridad deficientes e inexistentes.
- Implementación: este grupo lo conforman los errores de programación, los sistemas informáticos que se encuentran desactualizados o mal implementados, los errores que vengan propios del fabricante, y también se incluye las vulnerabilidades llamadas de día cero, las cuales se caracterizan por ser conocidas únicamente por ciberdelincuentes para beneficiarse de su explotación.
- Uso: En esta categoría se encuentran la mala configuración de los sistemas informáticos, así como también el desconocimiento y la falta de conciencia de los usuarios y de los responsables, a esto se suma el uso de aplicaciones no seguras o un incorrecto manejo de aplicaciones seguras.

De acuerdo con Mifsud (2012), las vulnerabilidades de manera global se encuentran clasificadas de la siguiente manera:

- “Desbordamiento de buffer: se genera cuando un programa no controla la cantidad de datos que se copian en buffer, de forma que si esa cantidad es superior a la capacidad del buffer los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original. Se puede aprovechar para ejecutar código que permita obtener privilegios de administrador" (EducaLab, 2014).
- Condición de carrera (race condition): se da cuando varios procesos acceden al mismo tiempo a un recurso compartido, por ejemplo, una variable, cambiando su estado y obteniendo de esta forma un valor no esperado de la misma.

- Error de formato de cadena (format string bugs): la principal causa se da cuando se acepta sin validar la entrada de datos proporcionada por el usuario, ante esto se lo considera un error de programación y el lenguaje más afectado es C/C++.
- Cross Site Scripting (XSS): lo conforman cualquier ataque que permita ejecutar scripts como VBScript o JavaScript, en el contexto de otro sitio Web, un uso de esta vulnerabilidad es el phishing.
- Inyección SQL: se produce cuando se inserta o "inyecta" código SQL invasor dentro del código SQL programado, a fin de alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de código "invasor" incrustado, en la base de datos.
- Denegación del servicio: provoca que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.
- Ventanas engañosas (Window Spoofing): son aquellas ventanas (pop-up) en las cuales se establece un premio (dinero o bienes materiales), y las que solicitan información personal para establecer a la víctima como ganador.

Un análisis de vulnerabilidades contempla fundamentalmente: Análisis de la situación actual, priorización de la información, evaluación de vulnerabilidades, corrección de vulnerabilidades priorizándolas por el riesgo que representan y por último se realiza un seguimiento a las amenazas solventadas (etic-solutions, 2013).

2.4 Incidentes de seguridad

Según el Centro de respuesta a incidentes informáticos del Ecuador (EcuCERT), “un incidente está definido como un evento inesperado o no deseado que tiene una probabilidad significativa de comprometer las operaciones de un sistema y de amenazar la seguridad de la información, poniendo en riesgo la confidencialidad, integridad o disponibilidad” (EcuCERT, 2015). Para la resolución de incidentes se

plantea seguir el siguiente diagrama de flujo (ver figura 2). Como lo señala el EcuCERT (2015) , los incidentes se los puede llegar a clasificar de la siguiente manera:

- Fraude IP-PBX: los incidentes provocados por VoIP son distintos de los ocasionados por datos. En consecuencia, requieren soluciones únicas y robustas para evitar que los ciberdelincuentes realicen ataques maliciosos que pueden ocasionar denegaciones de servicio (DoS), llamadas de larga distancia no autorizadas (fraudes de larga distancia) y robo de información confidencial. Para evitar esto las empresas deben usar de manera segura PBX IP y VLANs. Además, se recomienda implementar soluciones de seguridad específicas para estos sistemas, las cuales brinden una protección integral, aplicación estandarizada de políticas, estricto control de acceso y una privacidad de la información sensible.
- Phishing: es una técnica de Ingeniería Social que emplea el envío masivo de correos electrónicos spam en nombre de alguna entidad, con el objetivo de obtener datos personales y financieros (principalmente aquellos asociados a claves de acceso), o de redirigir a los usuarios a una página Web falsa de la entidad donde estos tengan que depositar sus datos. Este tipo de incidente se caracteriza por solicitar al usuario, con carácter de urgente, la confirmación o el envío de determinados datos bajo la excusa de problemas técnicos, cambios en la política de seguridad, detección de posibles fraudes, promociones o concursos. También tiene la finalidad de utilizar la información recabada para realizar compras por Internet, transferencias bancarias o retiros de efectivo a nombre de la víctima del fraude.
- Open Proxy: es un mecanismo que funciona como pasarela Web y permite hacer de puente entre nuestro navegador y el servidor al que se quiere conectar. Estos tipos de herramienta son utilizados en compañías para restringir el contenido que se puede visitar, acelerarlo mediante mecanismos de "cacheo" e incluso rastrear navegaciones que un

determinado usuario ha podido hacer. En ocasiones estos proxis son expuestos por error en Internet sin ningún tipo de control, y es común utilizarlos para navegar de forma anónima o saltarse controles de determinados sitios basados en el direccionamiento IP.

- BotNet: es un grupo de computadoras comprometidas a través de bots. Éstos son programas de software que permiten tomar el control remoto de la PC de una víctima desprevenida. Se le conoce a la PC comprometida de esta manera como PC zombi, de esta manera es controlada por alguien más, al cual se lo denomina con el nombre de bot herder (pastor de robots).
- Defacement: es un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página Web por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración.
- Fraudes en redes sociales: es la amenaza más peligrosa que enfrentan los internautas, y se produce a través de un virus, el cual una vez que ingresa a la computadora, altera el funcionamiento bloqueando el acceso a redes, dañando archivos, etc. Así, a través de mensajes, imágenes, o solicitud de actualización de datos o información, se logra robar claves, tarjetas de crédito, etc. Actualmente el amplio crecimiento que han tenido las redes sociales, las convirtió en un sitio ideal para llevar adelante éste delito. Además, han aparecido denuncias sobre ciberdelincuentes que estarían robando identidades con el fin de pedirle dinero a sus contactos.

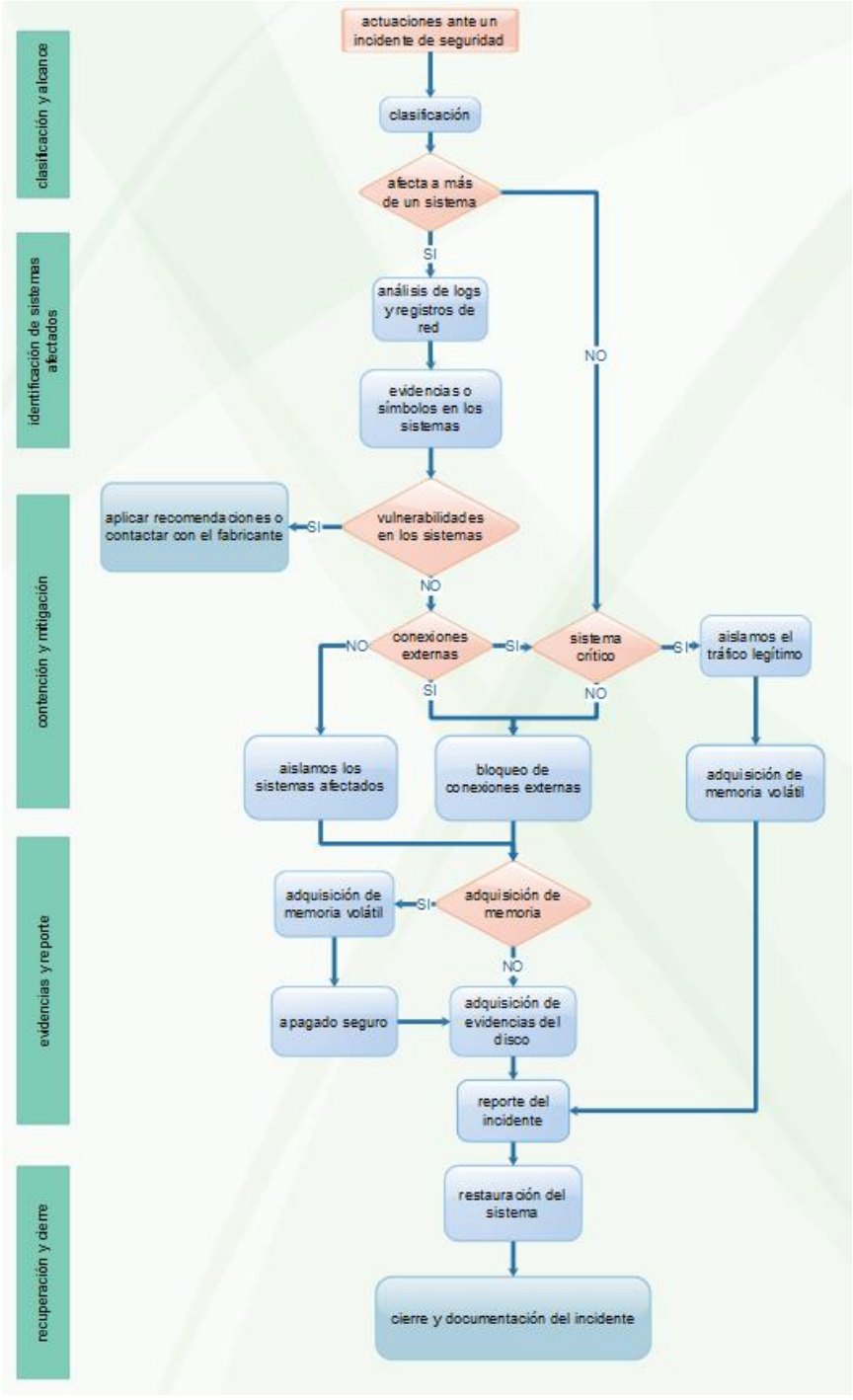


Figura 2. Flujograma de Actuación ante un Incidente de Seguridad

Fuente: (Díaz Vico, Fírvida Pereira, & Lozano Merino, 2013)

2.5 Business Intelligence

En 1958 Hans Peter Luhn investigador de la empresa IBM, fue el primero que utilizó el término “Business Intelligence System” para referirse a un sistema automático que acepta información en su formato original, disemina los datos adecuada y rápidamente a los lugares correctos (Armendáriz, y otros, 2016).

En este contexto, el Business Intelligence es fundamental para incrementar el valor de una organización, ya que brinda un panorama más amplio para la toma de decisiones basado en información precisa y oportuna; garantizando la generación del conocimiento necesario que permita escoger la alternativa que sea más conveniente para el éxito (Gomez & Bautista, 2010).

El padre del Business Intelligence es Howard Dresner, el cual es socio de la firma Gartner Group, que es una compañía a nivel mundial de investigación y asesoramiento de tecnología de la información. El la define como los conceptos y métodos para mejorar la toma de decisiones empresariales mediante el uso de sistemas basado en hechos de apoyo (Armendáriz, y otros, 2016).

En el Ecuador la investigación en el tema de Business Intelligence se ve avanzada en el periodo comprendido entre el 2010 y el 2017, con unos 63 documentos que despliega la base de datos de Scopus. Por el contrario, en el periodo comprendido entre el 2005 y el 2010, en el cual solo se llega a 4 publicaciones; el query utilizado para la búsqueda fue el siguiente:

(TITLE-ABS-KEY("Business Intelligence" OR "Data Warehouse" OR "DW" OR "On-Line Analytical Processing" OR "OLAP" OR "Multidimensional Database" OR "Data Mart" OR "Decision support database" OR "Decision support System" OR "Multidimensional Modeling" OR "Multidimensional Design" OR "Multidimensional Data Modeling" OR "multidimensional data Model" OR "multidimensional Model" OR "Data cube" OR "Data mining" OR "scorecard" OR "dashboard" OR "KPI" OR "Key Performance Indicator" OR "ETL" OR "Extraction Transformation and Load")) AND (AFFILCOUNTRY("Argentina" OR "Bolivia" OR "Brazil" OR "Chile" OR "Colombia" OR "Costa Rica" OR "Cuba" OR "Ecuador" OR "El Salvador" OR

"Guatemala" OR "Haiti" OR "Honduras" OR "Mexico" OR "Nicaragua" OR "Panama" OR "Paraguay" OR "Peru" OR "Dominican Republic" OR "Uruguay" OR "Venezuela" OR "Puerto Rico")) and ((PUBYEAR > 1999) and (PUBYEAR < 2013)) (Bustamante, 2016).

Caracteristicas Principales

El Businness Intelligence cuenta con características, las cuales ayudan a tener un panorama de su enfoque, entre las características principales se tiene: (i) El reconocimiento de la experiencia; (ii) El análisis de datos contextualizados; (iii) La capacidad de extraer e integrar datos de múltiples fuentes; (iv) El procesamiento de los registros obtenidos en información útil para el conocimiento del negocio; (v) La búsqueda de relaciones de causa y efecto, trabajando con hipótesis y desarrollando estrategias y acciones competitivas (Gálvez, 2016).

Arquitectura de Businness Intelligence

Las soluciones de Businness Intellience se enfocan en herramientas tecnológicas que brindan la extracción, integración, representación y análisis de datos, estas herramientas son las siguientes:

- Integración de datos. Procesos ETL. Software que realiza la integración de datos y su consolidación en una base de datos DataWareHouse (DWH). Para ello datos procedentes de distintas fuentes se extraen, transforman y cargan.
- Modelado de datos. Software que permite construir el modelo lógico de datos que actuará como soporte para el sistema BI.
- Reporting. Software para generación de informes utilizando los indicadores y dimensiones.
- Cuadros de Mando. Visualización rápida de los indicadores más importantes.

- OLAP: Procesamiento analítico en línea. Software para el análisis multidimensional de los datos que permite tener una visión más rápida e interactiva de los mismos.
- Minería de Datos o Data Mining. Análisis de la información de interés para la predicción de tendencias, comportamiento e identificación de patrones ocultos. (Marchena & Reinoso, 2016).

2.6 Metodología Ralph Kimball

Esta metodología de Kimball está enfocada a la construcción de un almacén de datos (Data Warehouse), el cual es una colección de datos que se caracteriza por la integridad, la no volatilidad y por ser variable en el tiempo para así obtener una ayuda en la toma de decisiones (Leon, 2014).

Kimball defiende una metodología de trabajo "Bottom-up", la cual establece que el procedimiento a seguir para construir un almacén de datos es empezar en un principio por pequeños componentes para ir evolucionando a estructuras y modelos superiores. Esto Kimball lo instaura de esta manera, ya que para él un almacén de datos no es más que la unión de las diferentes bases de datos departamentales (Data Mart) de una organización (Dertiano, 2015).

Se encuentra basada en el "Ciclo de Vida Dimensional del Negocio", este está conformado por cuatro principios, los cuales son: (i) Centrarse en el negocio; (ii) Construir una infraestructura de información adecuada; (iii) Realizar entregas en incrementales significativos; (iv) Ofrecer la solución completa (Azuaje, 2014).

Para el presente proyecto la metodología de Kimball servirá de referencia para la elaboración de una base de datos departamental, estableciendo las diferencias entre los sistemas Passive Vulnerability Scanner (PVS) y Snort, además de los componentes de los mismos (alertas en tiempo real y vulnerabilidades).

2.7 Metodología Scrum

Scrum es un proceso en el que se aplican de manera regular un conjunto de buenas prácticas para trabajar colaborativamente y generar un proyecto correctamente

estructurado. Las buenas prácticas se originan en un estudio de la manera de trabajar de equipos altamente productivos.

Esta metodología plantea entregas parciales y regulares del producto final, con la finalidad de satisfacer de una manera temprana las necesidades del cliente del proyecto. Es por esto que Scrum está en proyectos donde: (i) El entorno es complejo; (ii) Se necesita obtener resultados pronto; (iii) Los requisitos son cambiantes o poco definidos; (iv) La innovación, la competitividad, la flexibilidad y la productividad son fundamentales; (v) Se quiere trabajar utilizando un proceso especializado en el desarrollo de producto (Proyectos agiles - Introducción, 2017).

Scrum está conformado por las siguiente actividades: (i) Planificación de la iteración; (ii) Ejecución de la iteración; (iii) Reunión diaria de sincronización del equipo; (iv) Demostración de los requisitos completados; (v) Retrospectiva; (vi) Refinamiento de la lista de requisitos y cambios en el proyecto; cada actividad establece el personal involucrado, el tiempo y la forma de ejecución (Proyectos agiles - Funcionamiento, 2017). En la figura 2 se puede apreciar este proceso.

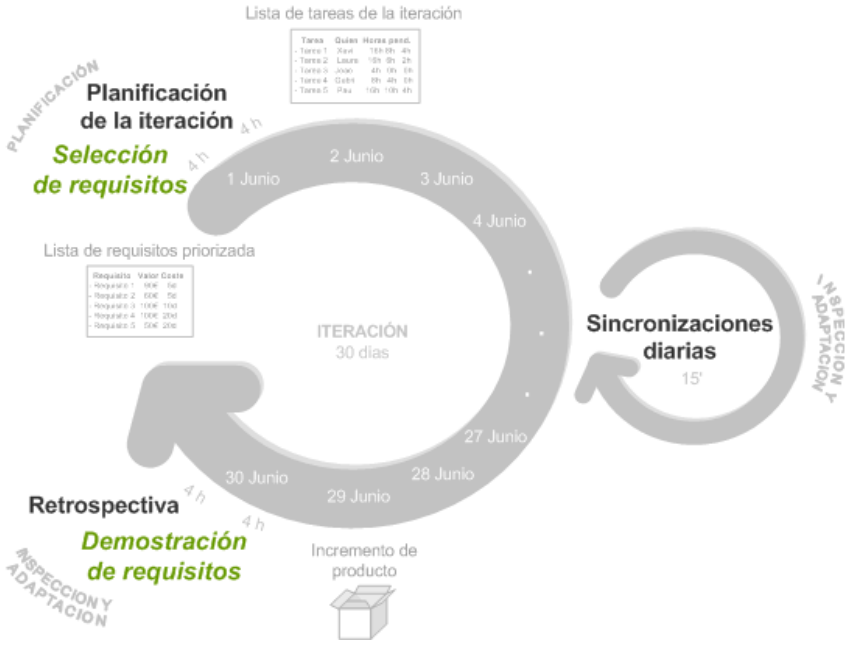


Figura 3. Metodología Scrum

Fuente: (Proyectos agiles - Funcionamiento, 2017)

CAPÍTULO III
INVESTIGACIÓN DE CAMPO

En este capítulo se describe la evaluación comparativa de los sistemas Passive Vulnerability Scanner (PVS) y Snort. Para este propósito se han considerado los siguientes criterios de comparación: (i) Memoria virtual usada (VIRT), (ii) Memoria RAM usada (RES), (iii) Porcentaje de CPU, (iv) Porcentaje de memoria física, (v) Análisis de eventos, (vi) Detección de eventos, (vii) Niveles de Riesgo, (vii) Análisis de tráfico por FTP, (ix) Análisis de tráfico por HTTP. Esta comparación contribuye en el proceso para establecer las diferencias entre cada una de ellas y si son excluyentes o complementarias.

3.1 Comparación cualitativa entre Passive Vulnerability Scanner y Snort

En este proceso se buscó puntos de análisis que sean claves para establecer una similitud. Para esto se determinó el uso de conjunto de datos (DataSets), con los cuales se llegó a generar una influencia de tráfico malicioso. Estos conjuntos de datos representan una recopilación tabulada de información de un determinado ente. En esta investigación se ha realizado la descarga de los conjuntos de datos de la Defense Advanced Research Projects Agency (DARPA), los cuales se generaron a partir de ataques que se provocaron en la década de los 90. A pesar del tiempo esta información sigue siendo relevante a nivel de seguridad, sobre todo cuando se sebe programar un IDS para dejarlo completamente funcional. Además, se ha ejecutado el conjunto de datos proveniente de Malware Capture Facility Project, el cual se caracteriza por la recolección de malware a través de una botnet. A continuación, se explica las dos herramientas evaluadas.

3.1.1 Passive Vulnerability Scanner (PVS)

Es un producto de la compañía Tenable Network Security, la cual se destaca por analizar todo el tráfico que está pasando en una red (i.e. por puertos, servicios, hosts, aplicaciones, sistemas operativos y vulnerabilidades). PVS genera dos archivos, el uno destinado a un monitoreo de vulnerabilidades en tiempo real. El segundo se centra en un monitoreo de la Web y de la actividad FTP. Un factor importante es la investigación realizada por Ron Gula para la corporación Tenable, en la cual afirma

que PVS no se considera un Sistema de Detección de Intrusos (IDS), debido a que PVS se enfoca en las vulnerabilidades. Expone que detectar un sistema comprometido es muy diferente que detectar un sistema que está bajo ataque (Gula, 2013).

3.1.2 IDS Snort

Snort es un sistema capaz de analizar todo el tráfico de red, verificando a través de reglas configuradas si hay actividad maliciosa generándose en la red protegida. Puede ser configurada de tres maneras: (i) Sniffer de paquetes; (ii) Packet logger; (iii) Detección de intrusiones de red (NIDS). Snort a través de programas realizados por terceros, llega a generar un complemento robusto para actualizar reglas y visualizar el contenido de una manera gráfica e intuitiva.

3.1.3 Comparativa

Conviene destacar que en la investigación se llegó a determinar que el PVS no actúa como IDS, esto quiere decir que simplemente verifica el tráfico que pasa por la red. Es decir, no tiene ninguna acción sobre los paquetes que por ésta circulan. Para una comparación justa, se utilizaron conjuntos de datos (DataSets) provenientes del grupo de Intrusión, detección y evaluación de DARPA del laboratorio Lincoln en el Instituto de Tecnología de Massachusetts (Massachusetts Institute of Technology, MIT). Estos se analizaron en el archivo alert y los logs generados por Snort, así como el archivo realtime y reportes generados por el PVS. PVS es muy versátil y puede complementar la administración de varios IDS, permitiendo que la escalabilidad de la red no se limite a equipos o productos de una sola marca. Del análisis se desprende que (véase tabla 4).

En la tabla 4 se especifica el consumo de memoria virtual, memoria RAM, CPU y memoria física que las herramientas registraron sobre una distribución Centos7 con arquitectura de 64 bits. Los datos muestran que Snort tiene un consumo menor en recursos comparado con PVS. Esto se debe principalmente a que Snort no cuenta con una interfaz Web gráfica de usuario que venga por defecto en el sistema. Además, el análisis en Snort está estructurado en “reglas", en las cuales se establecen parámetros sujetos al paquete que se va a capturar. Por otro lado, en PVS se analiza los “plugin’s”,

que brindan una especificación para ser desplegados cuando se suscite un evento. Sin embargo, no capturan los paquetes para analizarlo. En la valoración se puede establecer que PVS cuenta con más categorías para clasificar el riesgo de los eventos suscitados en la red que Snort.

Tabla 4

Consumo de recursos computacionales

Parámetros	***Herramientas***	
	Snort	***PVS***
Memoria virtual usada (VIRT)	1.2 G	1.6 G
Memoria RAM usada (RES)	0.2 G	0.8 G
Porcentaje de CPU	0.3	6.0
Porcentaje de memoria física	12.2	43.4
Análisis de eventos	Reglas	Plugin
Detección de eventos	Ataques	Evento – Vulnerabilidades
Niveles de Riesgo	1-3 High 1 Medium 2 Low 3	1-10 Information 0 Low 0-3.9 Medium 4-6.9 High 7-9.9 Critical 10

3.1.5 Interpretación

En base a los resultados de la tabla 1 y analizando el tráfico FTP y HTTP que circuló por la red, se determinó que existe una clara diferencia en el volumen da datos que se analizan entre las dos herramientas, esto es debido a que Snort actúa con reglas por defecto. Así también en algunos casos se cuenta con posibles soluciones cuando se trata de tráfico redundantemente analizado. Cabe mencionar que el óptimo rendimiento de Snort es justamente la configuración de las reglas con “Ruleset” que provengan de diferentes fuentes. Esta evaluación permite inferir que las herramientas no son excluyentes, sino por el contrario, se complementan, con el cual se puede brindar una protección más robusta a nuestra red.

Por tanto, las herramientas se catalogan como complementarias puesto que PVS ayuda en la identificación de vulnerabilidades, lo que permite robustecer los equipos contra ataques informáticos. Paralelamente Snort realiza un rastreo de la red, obteniendo alertas de las reglas que se hayan especificado, lo que posibilita una pronta

reacción ante sucesos invasivos en la red. Los niveles de riesgo establecen que PVS genera valores más específicos, debido a que posee dos categorías más para catalogar la información encontrada. Esta comparación ha servido para establecer que las herramientas PVS y Snort no son iguales. Por lo tanto, se adoptó las dos para generar un sistema que junte las ventajas que cada herramienta brinda.

CAPÍTULO IV
DESARROLLO DE LA APLICACIÓN DE BUSINESS INTELLIGENCE

En este capítulo se explicará todos los componentes que se utilizaron para la construcción de la aplicación Business Intelligence, empleando las fases de la metodología de Ralph Kimball y la metodología ágil Scrum como procesos de desarrollo (ver figura 4), con el fin de generar alertas preventivas antes de un posible ataque informático.

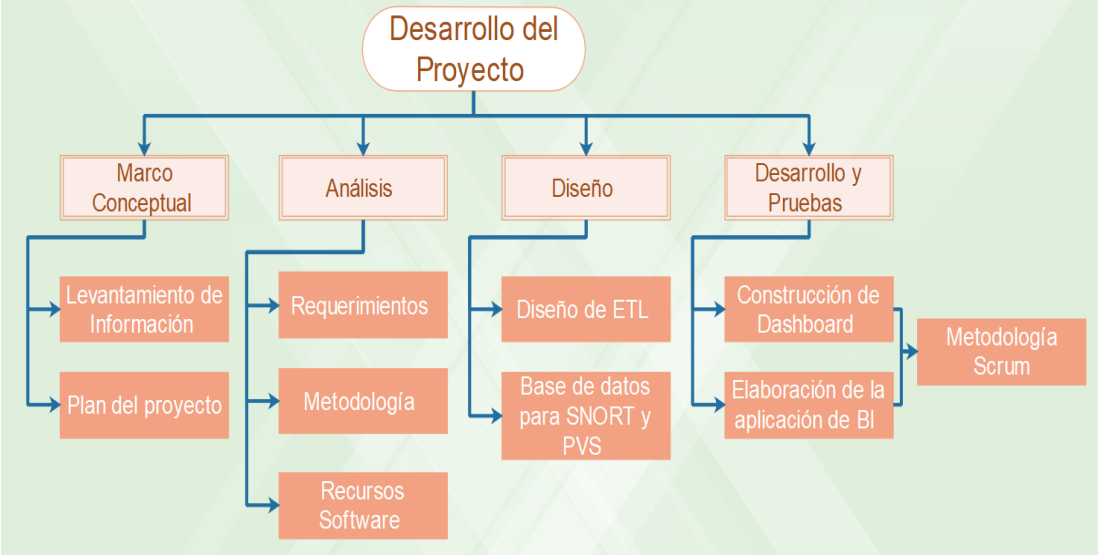


Figura 4. Ciclo del Vida del Proyecto empleando la metodología de Ralph Kimball

Fuente: (Adaptación de Ralph Kimball y Scrum)

4.1 Fase 1: Marco conceptual

La presente investigación se especifica con puntos previos que están basados en la metodología de Ralph Kimball, y los cuales son: planificación del proyecto, descripción de la institución y sustentación de la solución.

4.1.1 Planificación del Proyecto

Con base en los planteado en la metodología de Ralph Kimball, el presente estudio será dividido en marco conceptual, análisis, diseño, desarrollo y pruebas. (i) El marco conceptual contempla la descripción del problema, así como la solución que se ha propuesto; (ii) En el análisis se involucran los requerimientos, las metodologías y el software a ser utilizado; (iii) En el diseño se detalla el desarrollo de ETL's y los modelos dimensionales que se han aplicado para PVS y Snort; (iv) En el desarrollo se involucra la construcción de Dashboard's y elaboración de un aplicativo Web.

4.1.2 Descripción de la institución

Como parte del vínculo que ha generado la Universidad de las Fuerzas Armadas ESPE con instituciones externas, la Fundación Consorcio Ecuatoriano para el desarrollo de Internet Avanzado (CEDIA) ha depositado la confianza en la Universidad para llevar a cabo proyectos destinados con la Ciberseguridad en beneficio de sus miembros.

El objetivo de CEDIA es el "promover y mejorar las actividades en el campo de la investigación científica y aplicada; así como contribuir con la academia, a través del uso de las Tecnologías de la Información y Comunicación (TIC) en el Ecuador" (REDCEDIA, 2014).

"CEDIA se considera a si misma como una vía para que académicos e investigadores accedan a gran variedad de servicios orientados a impulsar y facilitar sus labores de enseñanza e investigación, debido a que cuentan con capacitaciones, infraestructura, repositorios, proyectos, colaboración, eventos, financiamiento y publicación de resultados" (REDCEDIA, 2014).

4.1.3 Sustentación de la solución

Tomando como referencia el análisis preliminar realizado entre PVS y Snort, se determinó que ambos sistemas se complementan. Siguiendo la metodología de Kimball, las fases de análisis, diseño y desarrollo del proyecto contarán con partes específicas para PVS y Snort. La solución propuesta contempló el control en el flujo

de datos (filtros), extracción de información (ETL) y el despliegue amigable de reportes automáticos (Dashboard).

4.2 Fase 2: Análisis

Se describe a continuación las metodologías utilizadas durante el desarrollo del proyecto, se detallan los requerimientos y necesidades de información. Por último se muestra el plan de pruebas que mide la eficacia del proyecto.

4.2.1 Metodología de Desarrollo de Ralph Kimball

El desarrollo del proyecto estuvo basado en la metodología de Ralph Kimball. En la figura 5 se especifica el ciclo de vida que se debe realizar en proyectos enfocados al Business Intelligence.

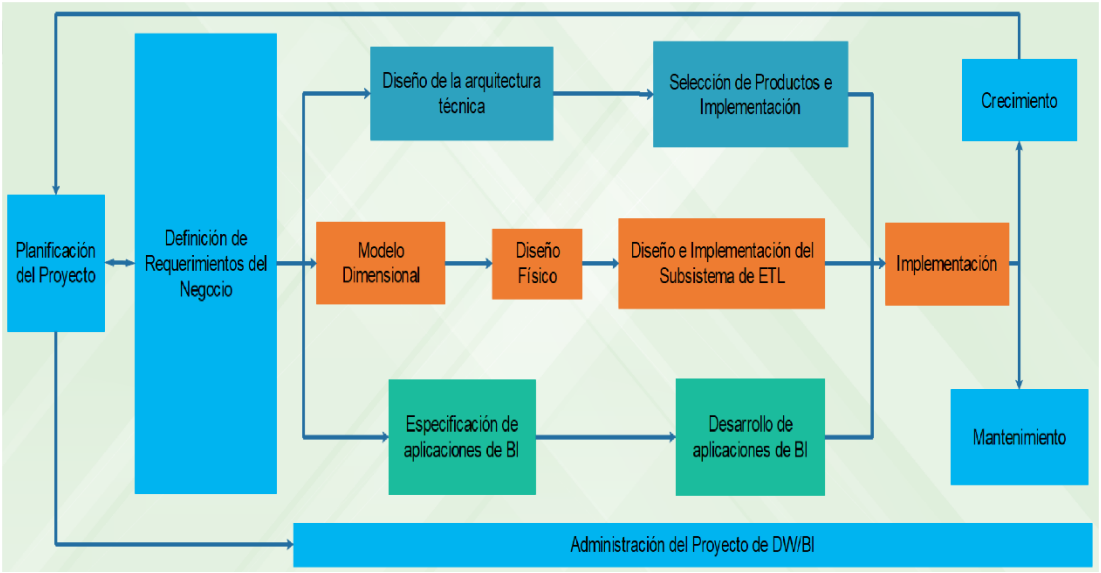


Figura 5. Metodología de Ralph Kimball

Fuente: (Rivadera, 2010)

De la figura 5 se aprecia que la Definición de Requerimientos del Negocio es el punto de origen para la selección tecnológica, la clasificación de los datos y la construcción del aplicativo. Se puede divisar que la metodología establece 3 vías fundamentales por las cuales se deberá desarrollar una solución de Business Intelligence, las cuales son: (i) Fila Superior: selección e implementación de

componentes harware y software; (ii) Fila Media: trabaja con la base de datos destinada al desarrollo de ETL; (iii) Fila Inferior: tareas destinadas a la construcción del aplicativo de Business Intelligence.

Se puede visualizar además que las tres rutas antes especificadas convergen en un punto el cual Kimball establece como “Implementación”. En éste se llega a desarrollar un producto el cual con el tiempo podrá entrar en un proceso de mantenimiento y mejora continua, logrando una libertad para que el producto vaya adquiriendo nuevas características.

Administración de la Metodología de Ralph Kimball

La administración contempla la planificación del proyecto, así como el proceso de levantamiento de requerimientos que se haya generado. Este proceso cuenta con varias tareas, las cuales se detallarán a continuación.

Planificación

En esta primera tarea se realiza el plan del proyecto, con lo cual se llega a especificar el alcance, los objetivos y los principales riesgos, que servirán de sustento para esclarecer el rumbo que tomará todo el proyecto. También consta de actividades organizativas, como son: planificación de uso de los recursos e identificación de actividades para elaboración de cronograma. Por último, para proyectos grandes se puede establecer un monitoreo de estado de los procesos, el rastreo de problemas y un plan de comunicación entre el grupo desarrollador y el cliente. En esta tarea se establece la relación entre el CSIRT-CEDIA y el desarrollador del proyecto

Análisis de Requerimientos

La definición de requerimientos se considera el proceso más importante debido a que de aquí se obtuvieron las necesidades que el cliente quiería solventar con el proyecto. En esta tarea fue crucial realizar reuniones y entrevistas con los principales involucrados. De este modo, la tarea anterior nos ayudó a identificar la/las áreas de las cuales se extraía los requerimientos enfocados al desarrollo del proyecto.

Para este proyecto se han generado reuniones y entrevistas con miembros del CSIRT-CEDIA, los cuales han dado a conocer los requerimientos para el proyecto, así como el alcance que desean obtener, para esto se ha establecido una línea base que sirva de punto de partida.

Modelo Dimensional

Para el modelo de datos fue importante incurrir en el nivel de detalle, el nivel de granularidad y las dimensiones. El proyecto se enfocó con los modelos dimensionales especificados para cada sistema (PVS y Snort), llegando a dividir en el caso de PVS los que son de real-time y los que se enfocaron en reportes.

Diseño Físico

En esta área se especificó el diagrama de almacenamiento con el cual se llevó a cabo el desarrollo del Business Intelligence. También se involucró la manera en la cual los datos podrían ser accedidos. Para el proyecto se utilizó MySQL como base de datos, en razón de ser robusto, open-source, adaptable al diseño físico y por poseer foros de ayuda.

Diseño de ETL y Dashboards

Los procesos ETL ayudaron a tomar la información de varias fuentes, generar una transformación acorde a una necesidad y obtener una salida en un destino específico. Para el proyecto la entrada de datos fueron los archivos de información de PVS y Snort, a continuación, se aplicó un proceso de transformación para obtener una información ordenada, y por último los datos que se han generado serían almacenados en una base de datos MySQL destinada para cada sistema.

Instalación de software

Para el proyecto se procedió con la instalación de la base de datos MySQL. Además, como herramienta de Business Intelligence se seleccionó Pentano. Esto en razón de ser open-source y por poseer herramientas que a través de una interfaz amigable permitan el rápido manejo y aprendizaje.

Para Snort no se utilizó ETL para la extracción de información, ya que esta herramienta cuenta con el sistema Barnyard2, el cual permite exportar de manera eficiente y controlada los registros obtenidos por el sistema a una base de datos específica.

Diseño y construcción de procesos ETL

Los ETL tienen como objetivo principal llegar a obtener una buena calidad de datos con los cuales se pueda lograr una visión global para tomar decisiones estratégicas. Para Kimball los ETL son la parte clave en la generación de un proyecto de Business Intelligence. Debido a que de ellos depende el manejo de los datos y la estructura que será procesada más adelante.

Los ETL están constituidos por tres fases, la primera enfocada en la obtención de los datos, los cuales para el proyecto actual se obtuvo de PVS y Snort. Seguidamente se realizó un proceso de transformación, para lo cual se aplicó filtrado y selección de datos, y finalmente se generó una carga de información, lo cual se originó en MySQL.

Construcción de Dashboards

La construcción de Dashboards se lo realizó con la herramienta Community Chart Components, la cual funciona vinculada al sistema Pentaho Business Analytics Plataform.

Pruebas

Una vez terminado los ETLs, estos fueron sometidos a un proceso de pruebas en los cuales se pueda ver si no poseen errores al momento de generar una ejecución de manera simultánea con los tiempos establecidos.

Aplicación para usuarios finales

Para el usuario final, se realizó un sistema Web, utilizando la metodología Scrum, ya que agiliza el proceso de desarrollo e involucra de una manera activa al

cliente, logrando establecer un diálogo directo para análisis de la información solicitada.

Implantación

Kibmball establece que las organizaciones subestiman esta etapa, y no dedican el tiempo y esfuerzo que ésta solicita (Mendoza, 2017). Ante esto, él propone realizar antes de la implantación un "ckecklist" que permita establecer una infraestructura correcta. Este checklist lo conforma la: (i) Configuración de hardware, (ii) Configuración de base de datos, (iii) Acceso a Internet o Intranet, (iv) Direcciones LAN y (v) Auditorias de sistemas enfocadas en el estado de la configuración inicial de las computadoras.

Para la implantación se desarrolló una máquina virtual, en la cual se pre-instalaron todos los programas necesarios. Además, se provee de manuales para su correcto funcionamiento.

4.2.2 Requerimientos del CSIRT de CEDIA

Los requerimientos serán divididos en dos partes, la primera enfocada al trabajo con ETL para la obtención de datos, y la segunda destinada a las solicitudes recopiladas para el sistema BI. La tabla 5 describe los requerimientos funcionales destinados al desarrollo de los Dashboards, los cuales se levantaron en conjunto con los especialistas del CSIRT de CEDIA. La tabla 6 muestra los requerimientos no funcionales para el desarrollo del ETL, en estos intervienen los factores de mantenimiento y seguridad. Esto fue analizado conjuntamente con los especialistas del CSIRT-CEDIA. La tabla 7 despliega los requerimientos funcionales para el Sistema, en este se presenta las características que el CSIRT-CEDIA cataloga como necesarios para el desarrollo. En la tabla 8 se visualiza los requerimientos no funcionales para el Sistema, estableciendo la seguridad, la visualización de datos y la documentación de ayuda.

Tabla 5

Requerimientos funcionales del CSIRT para ETL

ID	Descripción	Prioridad
01	Los datos en tiempo real, se deberán actualizar automáticamente.	ALTA
02	La plataforma deberá contar con mecanismo de seguridad, ante esto Pentaho es una plataforma segura que permite un control total de la información.	ALTA
03	El sistema permitirá a los usuarios de las Instituciones ver e imprimir los Dashboards creados por el Administrador.	ALTA
04	El sistema permitirá la exportación a Excel de las tablas de los Dashboard creados por el Administrador.	MEDIA
05	Ante errores suscitados en los procesos ETL, este notificará del problema enviando un e-mail al Administrador del sistema.	ALTA
06	El sistema permitirá a los usuarios designar que niveles de seguridad desean registrar, tanto para Snort como para Passive Vulnerability Scanner.	MEDIA
07	Cantidad de eventos por hora: La solución de Business Intelligence permitirá conocer la cantidad de eventos generados en la brecha de tiempo más reciente	ALTA
08	Cantidad y tipo de evento por hora: La solución de Business Intelligence permitirá conocer la cantidad y el tipo de evento suscitado en una hora determinada.	ALTA
09	Cantidad de riesgo por hora: La solución de Business Intelligence permitirá conocer la cantidad de riesgo que se presenta en una determinada hora.	ALTA
10	Cantidad de riesgo por evento: La solución de Business Intelligence permitirá conocer la cantidad de riesgo en un determinado evento.	MEDIA

Continua

11	IP de origen del evento: La solución de Business Intelligence permitirá conocer la/las IP de origen involucradas en un determinado evento	MEDIA
12	IP de destino del evento: La solución de Business Intelligence permitirá conocer la/las IP de destino afectadas por un determinado evento	MEDIA
13	Cantidad de Riesgo en un determinado periodo de tiempo: La solución de Business Intelligence permitirá conocer el riesgo generado en un reporte de una fecha específica y a una determinada hora.	ALTA
14	Cantidad de Ataques por IP en un determinado periodo de tiempo: La solución de Business Intelligence permitirá conocer la cantidad de ataques registrados en un reporte de una fecha específica y a una determinada hora.	ALTA
15	Cantidad de Riesgo producido por mes: La solución de Business Intelligence permitirá conocer la cantidad total de riesgo generado por mes de un reporte.	MEDIA
16	Cantidad de tipo de riesgo por riesgo: La solución de Business Intelligence permitirá conocer de un reporte el tipo de riesgo referente a un riesgo seleccionado	MEDIA

Tabla 6

Requerimientos no funcionales del CSIRT para ETL

ID	Descripción	Prioridad
01	El proyecto se desarrollará utilizando software Open Source, Suite community de Pentaho para el desarrollo de Business Intelligence y NodeJS para el desarrollo de la aplicación.	MEDIA
02	El sistema contará con archivos de configuración para que no se dificulte el arranque del sistema	ALTA
03	El sistema contará con logs en los cuales se pueda divisar posibles problemas que se puedan generar	ALTA
04	El sistema contará con sus respectivos manuales para un correcto funcionamiento y mantenimiento.	ALTA

4.2.3 Plan de Pruebas

En el plan de pruebas se estableció que, por medidas de seguridad, el sistema será desplegado en la infraestructura de CEDIA, ante esto se destinó un área controlada, la cual se caracterizó de poseer una cantidad limitada de tráfico que estuvo analizada por los Sistemas: Snort y PVS.

Desde el punto de vista de Ingeniería de Software, además se usó “pruebas de caja negra”, las cuales tuvieron como finalidad el análisis de la entrada y salida de datos. Cabe señalar que estas no se centraron en el proceso interior que se genera tras el ingreso de la información. Además, se analizó si los servicios ETL que se han creado para el sistema funcionan correctamente, y se verificó el despliegue de las reglas de Snort en la base de datos.

Plan de pruebas de Snort

Para Snort se diseñó una regla específica con la cual se pudo llegar a comprobar el correcto funcionamiento del mismo y del sistema de control de datos Barnyard2. La regla empleada para la prueba fue la siguiente

alert icmp any any -> $HOME_NET any (msg:"ICMP Test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)

En la figura 6 y figura 7 se puede visualizar el despliegue de la regla antes mencionada en la base de datos, además se presenta la salida que se obtuvo en la opción Snort del Sistema BI.

sid	cid	signature	timestamp	hora	sig_id	sig_name
2	1	28901	2017-05-31 11:28:46	11:28:46	28901	ICMP Test detected

Figura 6. Regla en MySQL de Snort

Figura 7. Regla en Dashboard de Snort

Plan de pruebas de PVS

Para las pruebas realizadas con PVS, se trabajó con la herramienta “Pytbull”, la cual generó ataques de tipo “Client side attacks”, a continuación, en la figura 8 se muestra el resultado en PVS de dicho ataque.

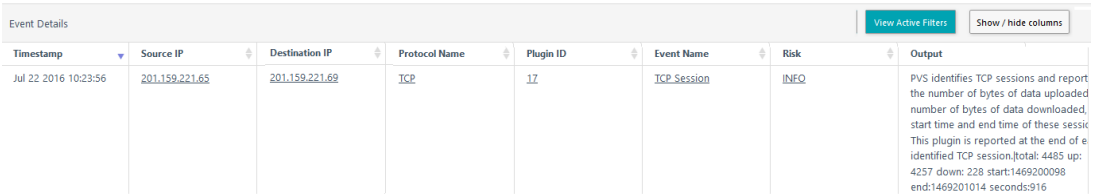


Figura 8. Despliegue de Actividad Maliciosa en PVS

PVS identifica que la actividad se efectúa por el puerto 20814, que ha registrado una carga de 4485 bytes y una descarga de 228 bytes en 916 segundos. Esta no supone un riesgo que deba ser de preocupación.

Tabla 7

Requerimientos funcionales del CSIRT para Sistema BI

ID	Descripción	Prioridad
01	Autenticación de Usuario: Los usuarios tendrán que identificarse para acceder al sistema.	ALTA
02	Registrar Usuarios: Los usuarios deberán registrarse en el sistema para poder acceder, para esto solo los Administradores podrán generar un nuevo registro.	MEDIA
03	Visualizar Tiempo Real PVS: El sistema ofrecerá un vínculo a un Dashboard de Pentaho, el cual porte datos relevantes que se puedan imprimir, además, si se genera alguna tabla, que la misma pueda ser llevada a Excel.	ALTA
04	Visualizar Reportes: El sistema ofrecerá un vínculo a un Dashboard de Pentaho que permita la visualización de reportes, generando una visualización por fecha obtener datos ordenados.	ALTA
05	Visualizar Tiempo Real Snort: El sistema ofrecerá un vínculo a un Dashboard de Pentaho, el cual desplegará los últimos eventos que se han suscitado en el sistema Snort	ALTA
06	Acceder a Pentaho: El sistema proporcionará un vínculo con la herramienta Business Intelligence Pentaho, la cual permitirá acceder a la herramienta Pentaho con las bondades de usuario asignadas en la aplicación (Usuario o Administrador).	ALTA

Tabla 8

Requerimientos no funcionales del CSIRT para Sistema BI

ID	Descripción	Prioridad
01	Interfaz del sistema: El sistema contará con una interfaz de usuario sencilla para que sea de fácil manejo.	ALTA
02	Seguridad de conexión: Debido al manejo de datos sensibles, se deberá acceder por el protocolo HTTPS en el puerto 443	MEDIA
03	Mantenimiento: El sistema deberá contar con un manual de Administrador para facilitar el mantenimiento de la aplicación.	ALTA

4.2.4 Software a utilizar

En esta sección se describen los sistemas a ser usados para la elaboración del proyecto. En primera instancia se describen los sistemas utilizados para la extracción de datos, tanto de PVS como de Snort. Después, se procede a describir las herramientas empleadas en la construcción de Dashboards. Finalmente se enfoca en la herramienta empleadas en la construcción de la aplicación.

Pulled Pork

Es un script desarrollado en el lenguaje Perl para descargar, combinar, instalar y actualizar reglas de diferentes fuentes (rulesets) que pueden ser vinculadas con el IDS Snort. Para la descarga, se podrá acceder al repositorio ubicado en Github (https://github.com/shirkdog/pulledpork).

Uno de los principales proveedores de reglas de manera abierta, es el centro de Investigación de Seguridad Emerging Threats, esta entidad genera feeds de datos con respecto a nuevas amenazas. Lo que hace que este proyecto sea tan eficaz son la aportación de ideas y la revisión por pares de todo el contenido. El objetivo principal es hacer que el desarrollo o actualización de reglas ocurran de manera rápida y abierta para ayudar a los profesionales de la seguridad a responder rápidamente a las amenazas conocidas y desconocidas (Emerging Threats, 2012).

Barnyard2

Es una herramienta open source para trabajar complementariamente con el sistema IDS Snort. Su funcionalidad radica en generar por medio de archivos de salida tipo unified2 una escritura más eficiente en disco. Dicho de otra manera, deja la tarea de analizar datos binarios en varios formatos a un proceso separado que provocará que Snort analice ininterrumpidamente el tráfico de red. Barndyard2 plantea un diagrama conceptual para la base de datos, la cual se visualiza en la figura 9. Para la funcionalidad, se editó las tablas especificadas en la figura 10.

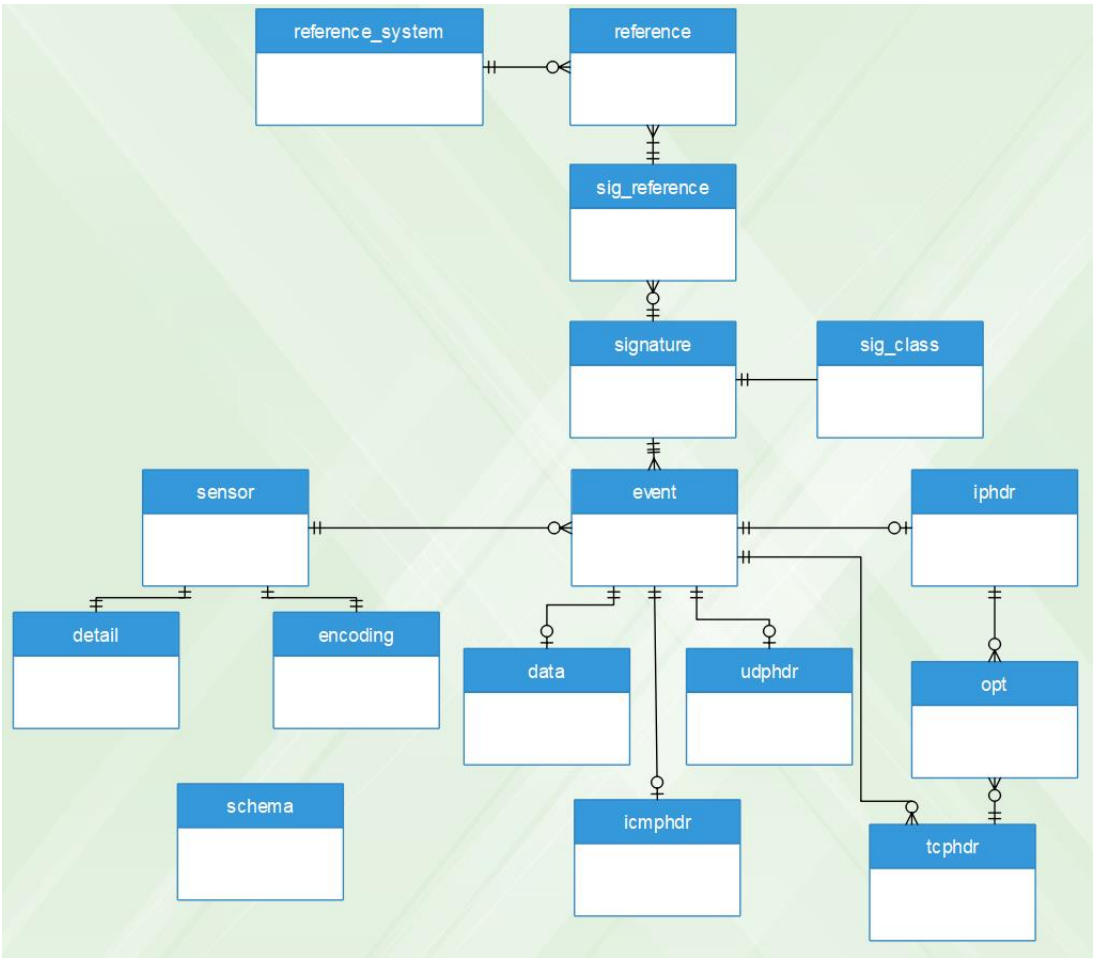


Figura 9. Diagrama Conceptual de Barnyard2

Fuente: (Danyliw, 2002)

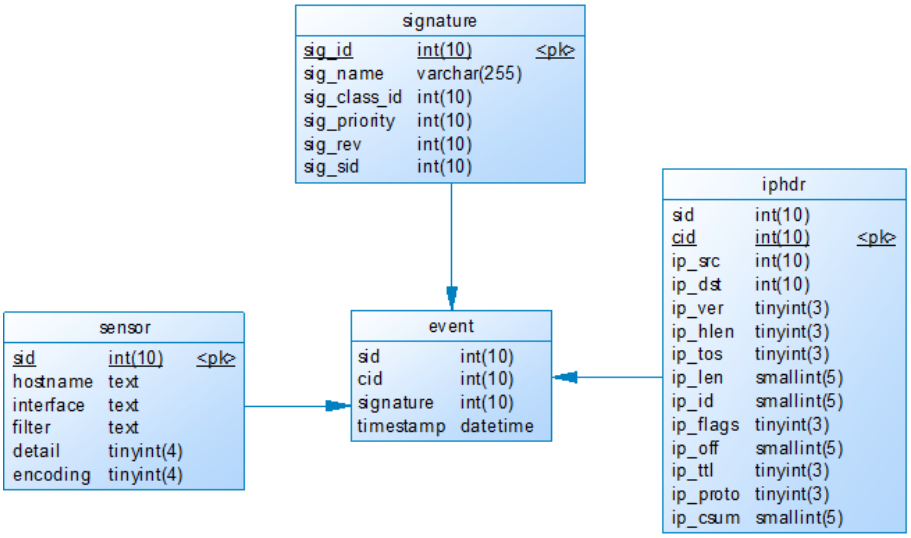


Figura 10. Diagrama Físico de Entidades Modificadas

Gestor de base de datos

En esta sección se detalla el Gestor de base de datos que se empleó en la elaboración del proyecto, tomando en cuenta el requerimiento de Open Source y la necesidad de disponer de una plataforma robusta que soporte la cantidad de registros a ser almacenados. Se procedió a seleccionar la herramienta MySQL.

MySQL es la base de datos de código abierto líder para las aplicaciones basadas en Web, esto debido a su alto nivel en escalabilidad, fiabilidad, seguridad y tiempo de actividad. Al utilizar MySQL se logra reducir: costo, riesgo, tiempo de desarrollo e implementación (Oracle, 2016).

Herramienta de Business Intelligence

El proyecto requiere una herramienta de Business intelligence que sea escalable, de código abierto y que disponga de facilidad de aprendizaje y usabilidad, ante esto se ha seleccionado la herramienta Pentaho.

Pentaho es una herramienta de Business Intelligence desarrollada bajo la filosofía del software libre para la gestión y toma de decisiones empresariales. Es una

herramienta compuesta de diferentes programas que satisfacen los requisitos de BI. Pentaho ofrece soluciones para la gestión y análisis de la información, incluyendo el análisis multidimensional OLAP, presentación de informes, minería de datos y creación de cuadros de mando para el usuario (Gravitar, 2016).

Pentaho ha sido desarrollado bajo el lenguaje de programación Java y tiene un ambiente de implementación también basado en Java, haciendo así que sea una solución muy flexible al cubrir una alta gama de necesidades empresariales (Gravitar, 2016). Dos complementos importantes de mencionar, son el Community Dashboard Framework y el Community Data Access.

El Community Dashboard Framework es un framework Open Source que permite la creación de cuadros de mando altamente personalizables en la parte superior del servidor Pentaho Business Intelligence, además se basa en estándares de desarrollo Web como CSS, HTML5 y JavaScript (aprovechando algunos marcos comúnmente utilizados como jQuery o Bootstrap). Este Framework está destinado a los desarrolladores, debido a que es una solución eficaz para combinar datos con una atractiva capa de visualización (Pentaho, 2016).

El Community Data Access es un plugin de Pentaho diseñado para acceder a datos con gran flexibilidad, además que permite acceder y entregar datos en diferentes formatos a partir de las muchas fuentes de datos de Pentaho. Cuenta con tres propósitos fundamentales: unir datos de diferentes fuentes con solo la edición de un archivo XML, evitar problemas de inyección SQL dentro de CDF y clasificar y paginar datos del lado del servidor (Pentaho, 2016).

Pentaho cuenta con una arquitectura dividida en cuatro capas (ver figura 11): la primera destinada a la generación de informes, vinculando un despliegue interactivo; la segunda enfocada al análisis de la información, involucrando minería de datos y cubos OLAP; la tercera centrada en la generación de Dashboards, con el objetivo de generar pantallas intuitivas y obtener alertas; y para finalizar se abarca un proceso de gestión, que permite controlar metadatos y procesos.

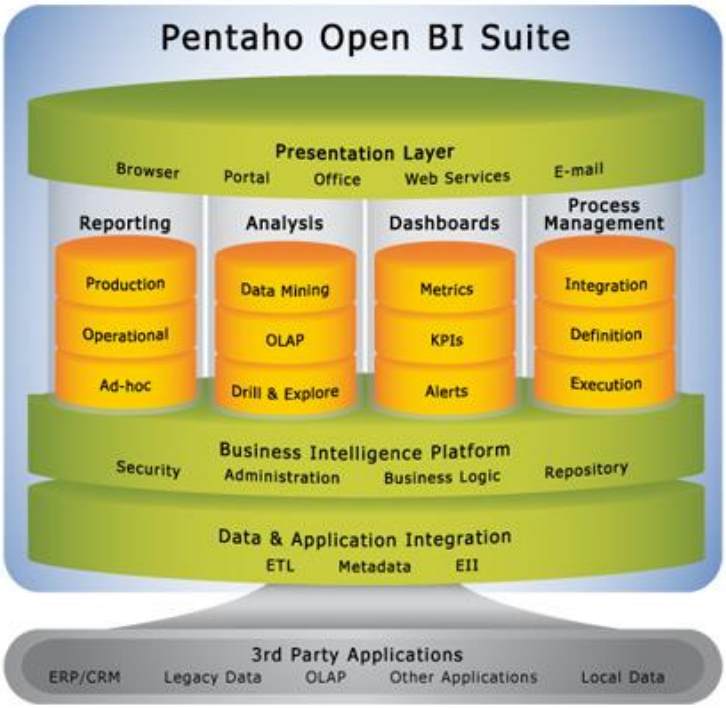


Figura 11. Arquitectura de Pentaho Business Intelligence

Fuente: (DataSwing, 2013)

Pentaho Data Integration

Para el Desarrollo de ETL en el mercado se pueden encontrar varias alternativas de herramientas de código abierto y propietarias, que trabajan de manera robusta y flexible. Sin embargo, una pauta que genera diferencia, es la complejidad de manejo. Ante esto, para el proyecto se utilizó una herramienta de código abierto que sea capaz de vincularse con el sistema Pentaho y que también posea una interfaz amigable para un rápido desarrollo. Kettle estuvo destinada para la integración de datos de Pentaho.

Kettle es una interfaz gráfica de usuario que le permite diseñar transformaciones y trabajos que se pueden ejecutar con las herramientas Kettle (Pan y Kitchen). Pan es un motor de transformación de datos que realiza una multitud de funciones como leer, manipular y escribir datos desde y hacia diversas fuentes de datos. Kitchen es un programa que ejecuta trabajos diseñados por Kettle en XML o en

un repositorio de bases de datos. Los trabajos se programan generalmente en modo por lotes para que se ejecuten automáticamente a intervalos regulares. Las transformaciones y los trabajos pueden describirse usando un archivo de XML o se pueden poner en un repositorio de la base de datos de Kettle. Pan o Kitchen pueden leer los datos para ejecutar los pasos descritos en la transformación o para ejecutar el trabajo. En resumen, Kettle hace que los almacenes de datos sean más fáciles de construir, actualizar y mantener (Wiki Pentaho, 2016).

4.3. Fase 3: Diseño

El diseño contempló la programación ETL empleada para obtener los datos de PVS, los procesos de filtración generados para no sobrecargar la base de datos, y los diagramas con los cuales se realizó el proyecto.

4.3.1 Construcción de ETL

En esta sección se detalla el desarrollo de ETL empleado para la recolección de datos de PVS, empezando por las fuentes de datos que se han analizado, hasta llegar a generar un ETL que trabaje de acuerdo a las especificaciones.

Fuente de Datos

Analizando la herramienta PVS, en la sección de configuración, en la pestaña “Realtime Events” se puede seleccionar la opción “Log Realtime Events To Realtime Log File”, por medio de esta, se pudo visualizar un archivo “.txt” que contenga los eventos que se hayan suscitado. Para los reportes se generó a partir de un archivo con extensión “.nessus”, el cual es un xml enriquecido (ver tabla 9).

Filtrado de Información para PVS y Snort

Para asegurar una carga óptima de datos, enfocada en no sobrecargar con información catalogada como innecesaria, se procedió a desarrollar un método de filtrado para los eventos en tiempo real de PVS y las alertas generadas por Snort.

El proceso empezó con la revisión de la valoración que entrega cada sistema a los eventos suscitados, los cuales se plasman en la tabla 10 para Snort y la tabla 11 para PVS.

Tabla 9

Fuentes de Datos de PVS

Tipo	Fuente de datos	Extensión
Eventos en tiempo real	Archivo de texto	txt
Reportes	Archivo de texto	nessus

Tabla 10

Valoración del Riesgo en Snort

Tipo	Valor
BAJO	3
MEDIO	2
ALTO	1

Tabla 11

Valoración del Riesgo en PVS

Tipo	Valor
MUY BAJO	NONE - INFO
BAJO	LOW
MEDIO	MEDIUM
ALTO	HIGH
MUY ALTO	CRITICAL

Tomando en consideración esta valoración se ha procedido a optar por la creación de un archivo de texto, en el que conste los parámetros que el usuario desea analizar. El archivo de texto tiene el siguiente contenido:

 # Descomentar cada línea que se desee activar para el procesamiento de logs

NONE
INFO
LOW
MEDIUM
HIGH
CRITICAL

Tomando en cuenta que Snort realiza un proceso de transferencia de información por el sistema barnyard2 que se encarga de pasar la información al gestor de base de datos MySQL, únicamente para Snort se ha generado un proceso ETL de filtrado. Para PVS el proceso se lo genera mediante la ejecución de Shell Script al momento de guardar la información en la base de datos. En la figura 12 se visualiza el trabajo realizado en la herramienta Kettle para el filtrado del riesgo para Snort.

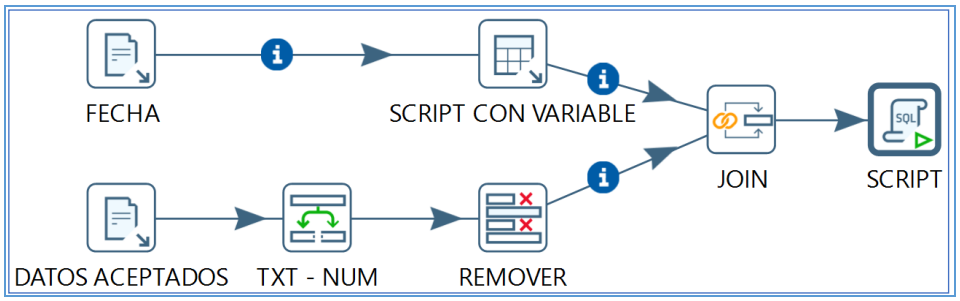


Figura 12. Filtro de Riesgo para Snort

En el proceso de transformación, primero se captura la fecha de guardado, para establecer una línea base de la cual partir. Esta fecha se emplea como parámetro en el script que traerá los datos, simultáneamente se lee el archivo de texto separando los parámetros que se consideran de relevancia. Por último, se vinculan el resultado obtenido en el script con el o los valores de riesgo a ser eliminado. Con la vinculación se ejecuta un script que afecta al almacenamiento de la base de datos de Snort.

ETL para Eventos en Tiempo real

Como se mencionó en la sección “Filtrado de Información para PVS y SNORT”, para PVS el filtrado se lo realizó por medio de un código (expresión regular), el cual analiza cada línea del archivo de texto, lo separa en razón del riesgo y crear un nuevo archivo “.log” con los datos de relevancia. En Kettle se genera una Transformación y un Trabajo, en la figura 13 se presenta la transformación desarrollada.

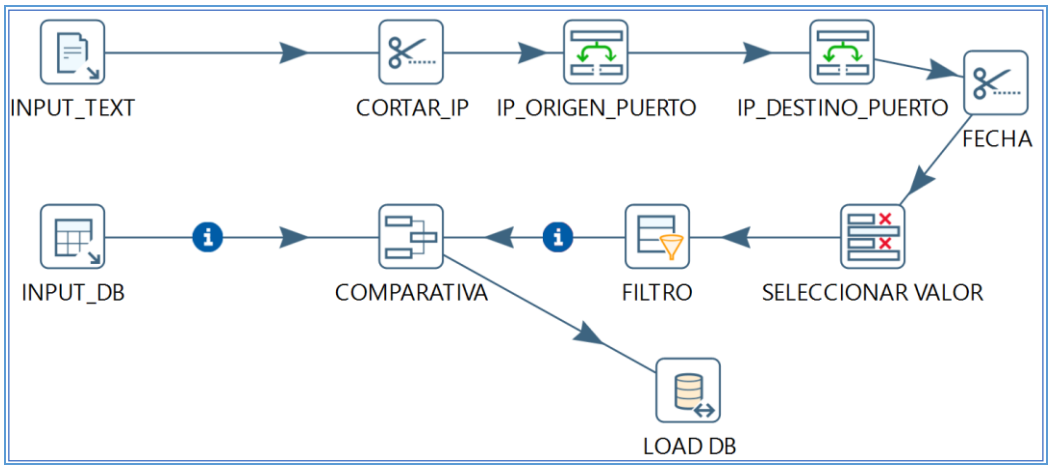


Figura 13. Transformación para procesos en Tiempo Real de PVS

Se inicia extrayendo los datos del archivo de texto con extensión “.log”, se manipula la información obtenida para separar datos que se encuentran unidos, específicamente IP de origen, IP destino y la fecha. Luego se selecciona y se ordena la información obtenida. Además, se aplica un filtro que elimina los datos basura que pueden estar almacenados en el archivo, y se genera una comparativa con todo lo almacenado en la base de datos. Es importante aclarar que la comparativa establece una bandera que cataloga los datos nuevos que se han generado para no incurrir en una redundancia de datos. De este análisis de información se obtiene una base de datos Plana, la cual se presenta en la figura 14. El trabajo que se aplicó a la transformación (ver figura 13), se visualiza en la figura 15.

pvs_realtime	
mes	varchar(9)
dia	varchar(6)
hora	varchar(10)
ip_origen	varchar(16)
p_ip_origen	varchar(7)
ip_destino	varchar(16)
p_ip_destino	varchar(7)
riesgo	varchar(10)
evento	varchar(108)
descripcion	text
output	text
numero_de_protocolo	varchar(12)
plugin_id	varchar(8)
flagfield	text

Figura 14. Base de datos Plana para eventos en PVS de tiempo real

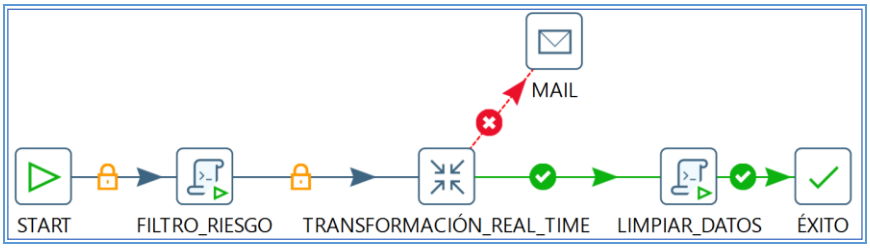


Figura 15. Trabajo para eventos en Tiempo Real de PVS

En el Trabajo se involucra el script generado para el filtrado de la información, el cual genera el archivo ".log" que será analizado en la transformación. Con estos datos se procede a obtener la salida de éxito para lo cual se limpian los datos del archivo ".log". En caso de presentar algún error en la generación de la transformación, se procederá a enviar un e-mail a un destinario definido en una variable la cual podrá ser cambiada una vez que se genere el servicio en el sistema operativo.

ETL para Reportes

Para los reportes se generó una Transformación, la cual podrá ser visualizada en la figura 16. Este proceso inicia con la extracción de datos del xml enriquecido (.nessus), para lo cual se programó la selección de los datos identificando los nodos y los atributos. A continuación, se aplicó una transformación a la fecha y se ordenaron los datos. Después, de manera similar a la transformación de eventos en tiempo real, se generó una comparativa entre los datos previamente almacenados en la base y el archivo ".nessus", obteniendo únicamente datos nuevos que se procederían a almacenar. Como resultado del proceso se generó una base de datos Plana, la cual se visualiza en la figura 17 y está destinada a los reportes en PVS.

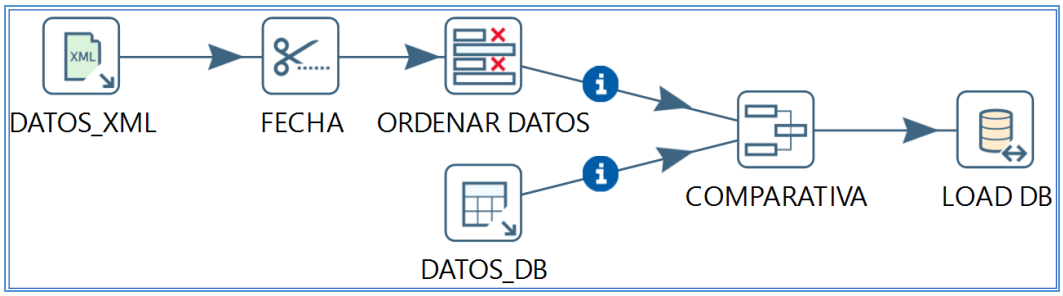


Figura 16. Trabajo para procesos en Tiempo Real de PVS

pvs_report	
anio	varchar(5)
mes	varchar(9)
dia	varchar(6)
hora	varchar(10)
host	varchar(16)
plugin_id	varchar(8)
cve	varchar(15)
cvss	varchar(5)
riesgo	varchar(10)
protocolo	varchar(5)
puerto	int(6)
nombre_plugin	text
sinopsis	text
descripcion	text
solucion	text
output	text
flagfield	text

Figura 17. Base de datos Plana para reportes de PVS

El trabajo aplicado a los reportes generados por PVS y visualizado en la figura 18, es similar a la generada para eventos en tiempo real. Su variación radica en los parámetros de e-mail, el tiempo de ejecución y el no poseer un filtrado, ya que se vio necesario el análisis total de las vulnerabilidades que en este se reportan.

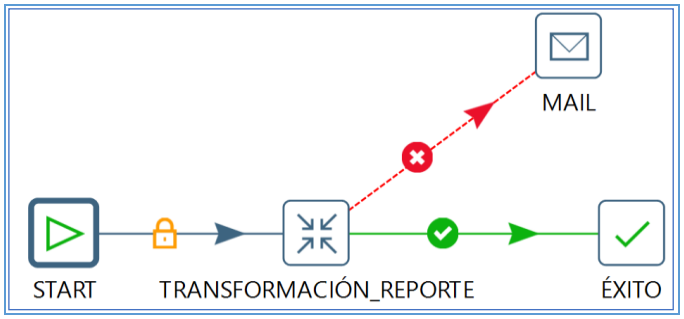


Figura 18. Trabajo para reportes de PVS

4.3.2 Construcción de Dashboards

En esta sección se detalla la construcción de los Dashboards, utilizando para esto los requerimientos que los especialistas del CSRIT-CEDIA han planteado. Los Dashboards contemplan una solución responsive, el cual tienen como objetivo adaptar la apariencia de un contenido.

Dashboard de eventos en tiempo real

Para el desarrollo del Dashboard de eventos en tiempo real, se lo generó en dos partes, la primera enfocada a mostrar de una manera gráfica los eventos que se han presentado, generando un despliegue por dependencia, con el objetivo de generar una mejor comprensión para el usuario. La segunda parte se sustenta en una tabla de resumen, la cual como lo establece el requerimiento N05, permite que la tabla sea exportada a Excel. También se ha instaurado un botón el cual permite la Impresión del mismo. En la figura 19 se muestra la visualización del Dashboard desarrollado.

Figura 19. Dashboard de eventos en tiempo real

Dashboard de Reporte

Para los reportes, se elaboró un Dashboard, el cual se enfoca en informar vulnerabilidades que se susciten en una determinada red. Para este se ha considerado: IP's afectadas, riesgo que posee una determinada IP, cantidad de riesgo generado en el año, el/los eventos que emite determinado riesgo y un valor numérico de las vulnerabilidades que se han presentado en un determinado lapso de tiempo (ver figura 20).

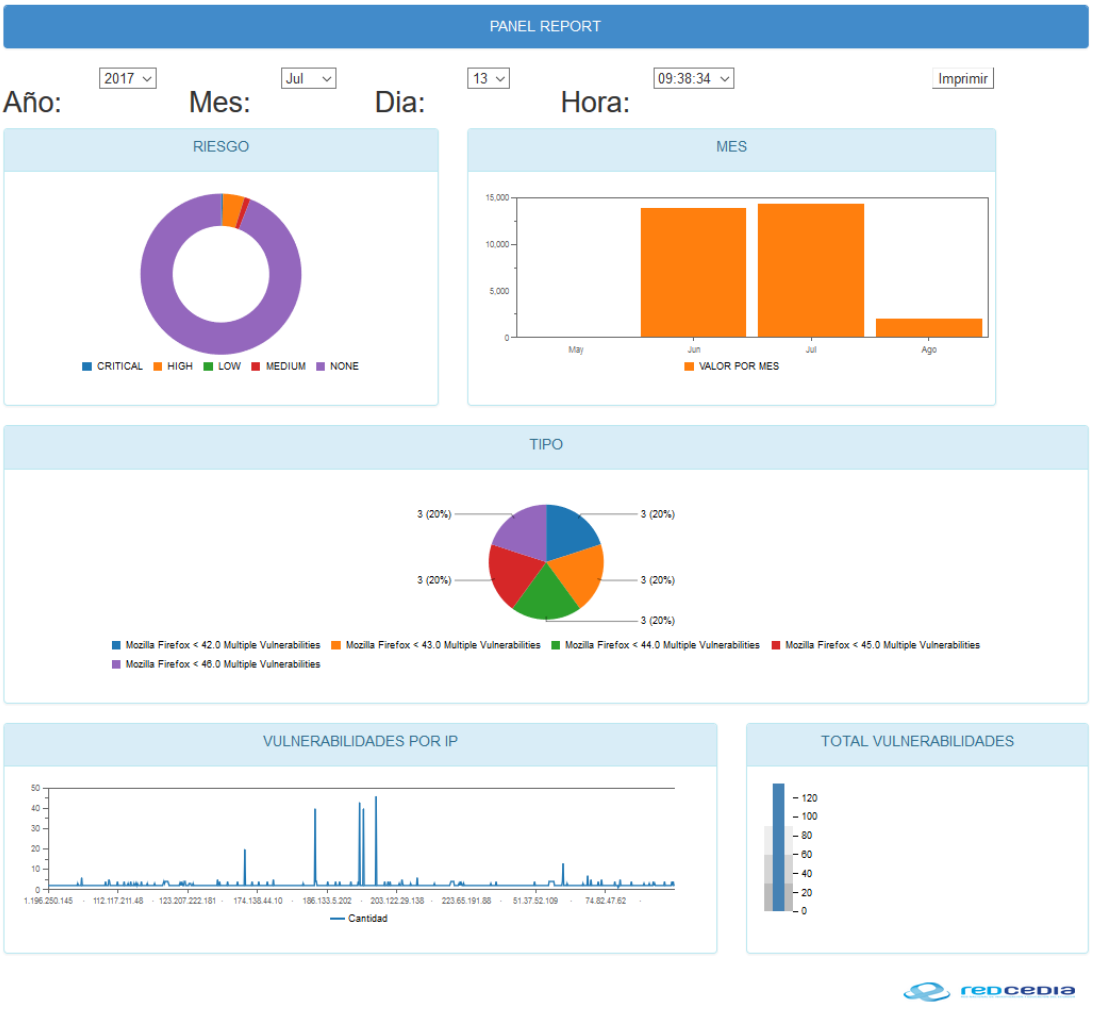


Figura 20. Dashboard de vulnerabilidades en tiempo real

Dashboard de Snort

De Snort se realizó un Dashboard, el cual consta de una tabla que muestra de manera clara las últimas alertas que se han registrado, vinculando la exportación a Excel y el botón mediante el cual se puede realizar una impresión. En la figura 21 se muestra el Dashboard que se ha generado.

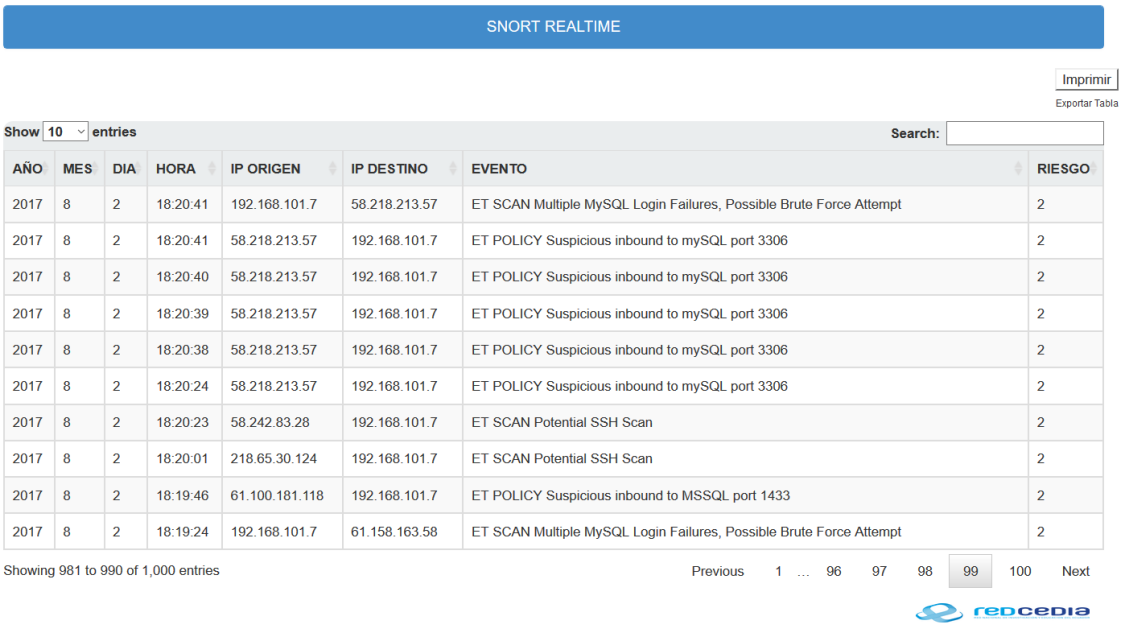


Figura 21. Dashboard de alertas Snort

4.3.3 Desarrollo e Implementación de Aplicación BI

En esta sección se detalla todo el proceso de desarrollo de la aplicación BI, iniciando por las características que poseerá un usuario, hasta llegar a generar el producto final.

Características de los Usuarios

Los usuarios que intervienen en el Sistema BI se muestran en la tabla 12. Aquí se detalla la formación y las características que poseen para la manipulación de la información.

Casos de Uso de Aplicación BI

La aplicación BI se sustenta en los siguientes diagramas de casos de uso (ver figura 22) donde se presenta las relaciones al sistema BI. Por otro lado, los presentados en la figura 23 se refieren al Sistema Pentaho, esto se analiza en razón de visualizar los atributos que tendrá un determinado usuario.

Tabla 12

Características de Usuarios de Aplicación BI

Tipo	Administrador	Usuario
Formación	Ingeniero en Sistemas o afines vinculada a la seguridad informática	Persona suplente o ayudante en el área de seguridad informática
Actividades	Control del sistema en general y acceso a Pentaho en modo Administrador	Visualización del sistema y acceso a Pentaho en modo Usuario

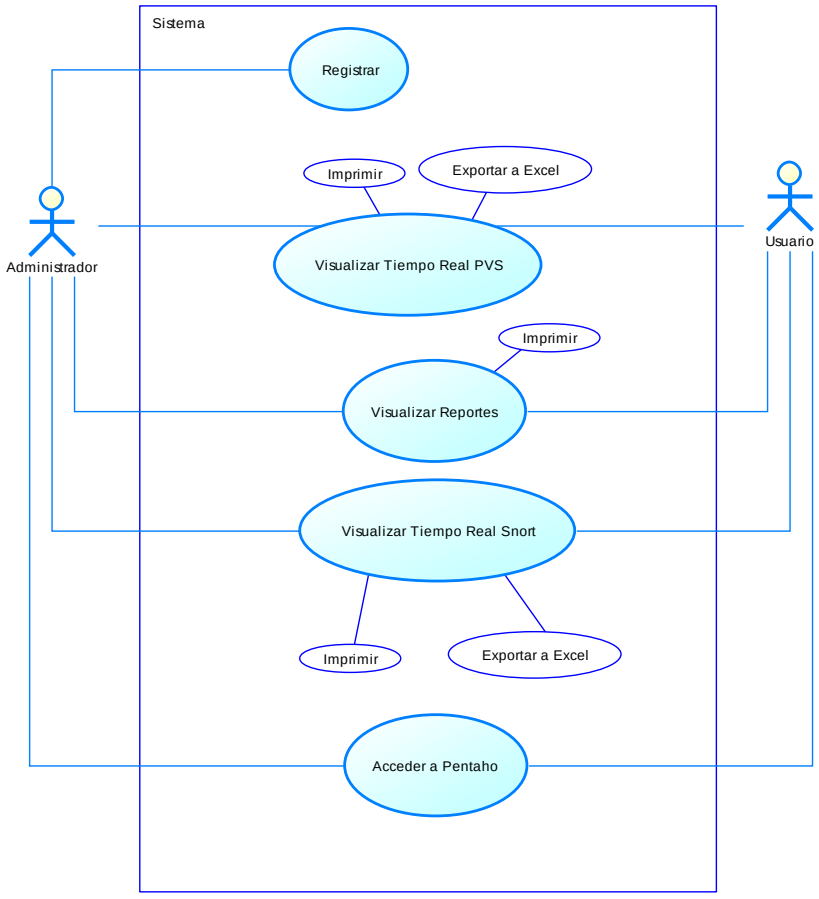


Figura 22. Casos de Uso Sistema BI

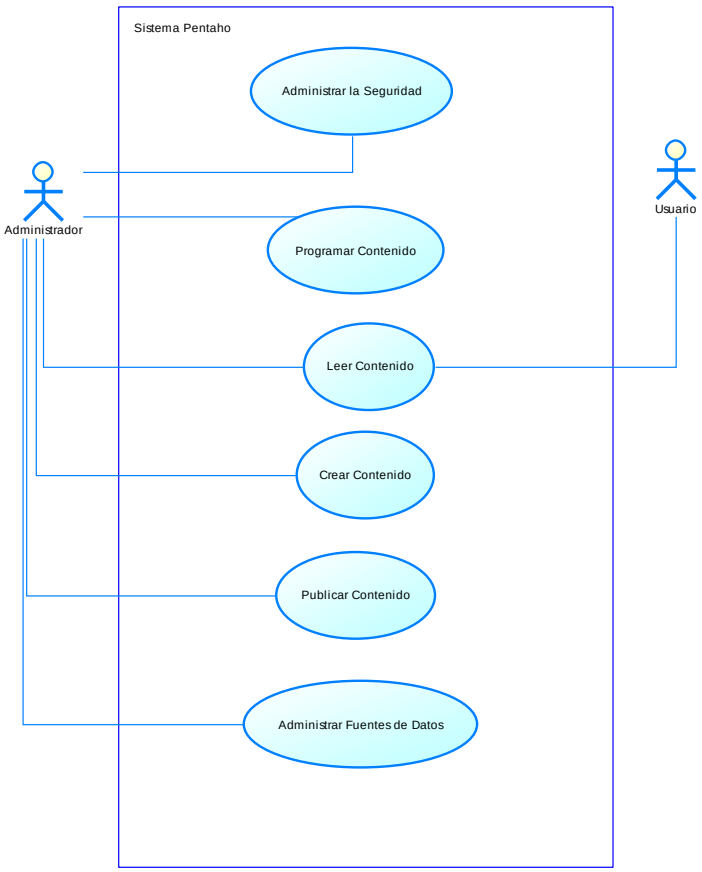


Figura 23. Casos de Uso Sistema Pentaho

Funcionamiento de la Aplicación BI

La figura 24 muestra diseño de la aplicación, la cual cuenta con dos modos de usuario, el primero será administrador, y podrá registrar nuevos usuarios. Además podrá ingresar a Pentaho con todos los permisos, con lo cual obtiene la capacidad de editar y configurar el contenido de Dashboard y de la base de datos. El segundo será usuario, el cual podrá visualizar los Dashboard, así como ingresar al sistema Pentaho únicamente con los permisos otorgados por el administrador. Esto en caso que el administrador desee o necesite asignar una tarea en particular, tomando en cuenta la manipulación de los datos.

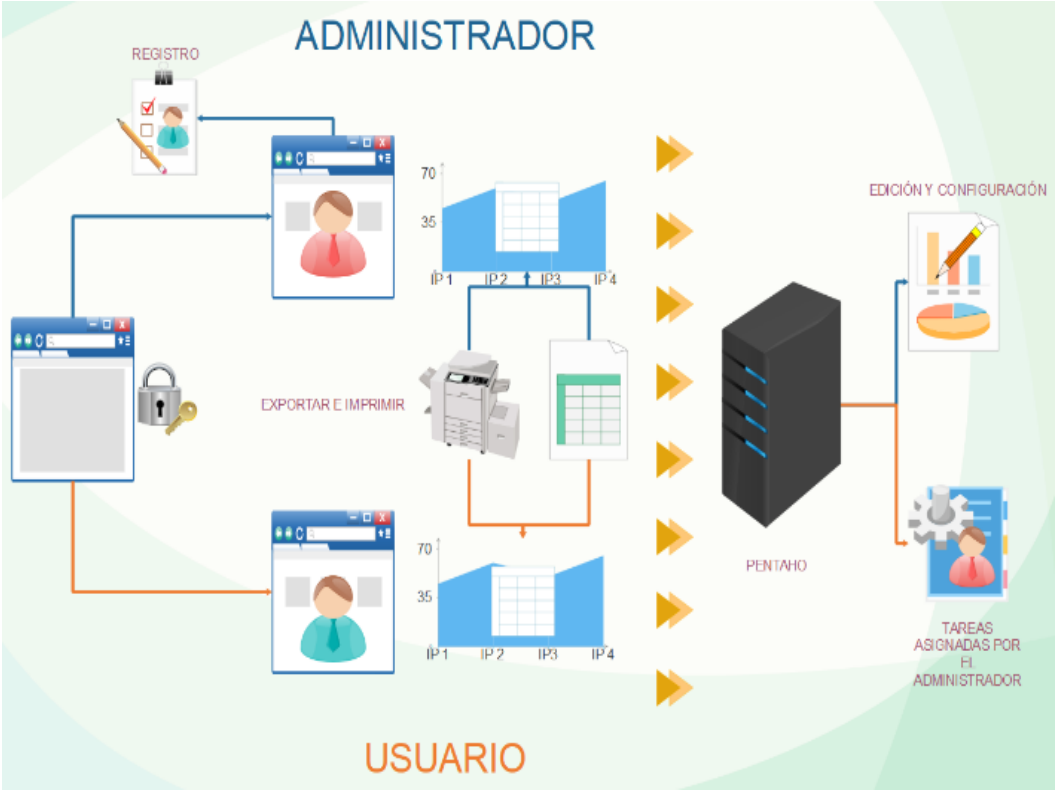


Figura 24. Funcionalidad del Sistema BI

Para la vinculación entre Pentaho y el Sistema BI se utilizará el Plugin *"Integrator"* de Pentaho, el cual, por medio de tokens, establece una conexión segura entre el Servidor de Pentaho, y un sistema que solicite acceso.

Por medio de la metodología Scrum, se logró desarrollar un proyecto enfocado en el cliente, ya que se realizaron reuniones diarias con el equipo de desarrollo, además que se establecían reuniones con el usuario final del CSIRT-CEDIA para constatar funcionalidad, y/o adicionar requerimientos.

Para la aplicación se ha desarrollado las siguientes interfaces. La primera (ver figura 25) se presenta al iniciar el sistema, esta podrá ser editada según necesidad de cada institución. La segunda (ver figura 26) se presenta para iniciar sesión en el sistema. La tercera (ver figura 27) dispone de las opciones: (i) eventos en tiempo real, el cual despliega el Dashboard destinado a los eventos que se han suscitado

recientemente; (ii) reporte de vulnerabilidades, el cual presenta el Dashboard enfocado en las vulnerabilidades; (iii) Snort, el cual presenta el Dashboard generado para este sistema, (iv) Pentaho, el cual genera un enlace a Pentaho tomando en cuenta el usuario con el cual se ha ingresado al sistema. Si se ha iniciado sesión con un usuario Administrador, se podrá genera un nuevo registro (ver figura 28).

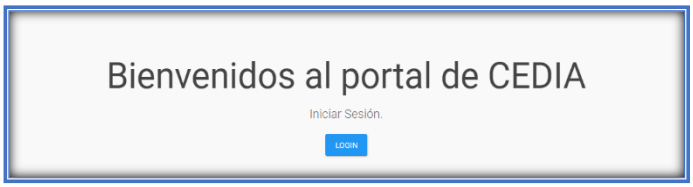


Figura 25. Interfaz de inicio del Sistema BI

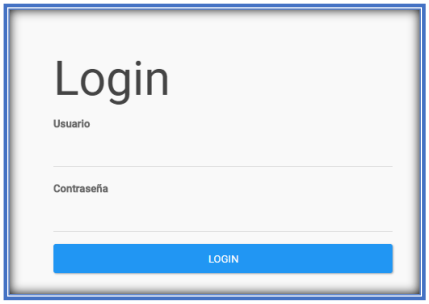


Figura 26. Interfaz de Login del Sistema BI

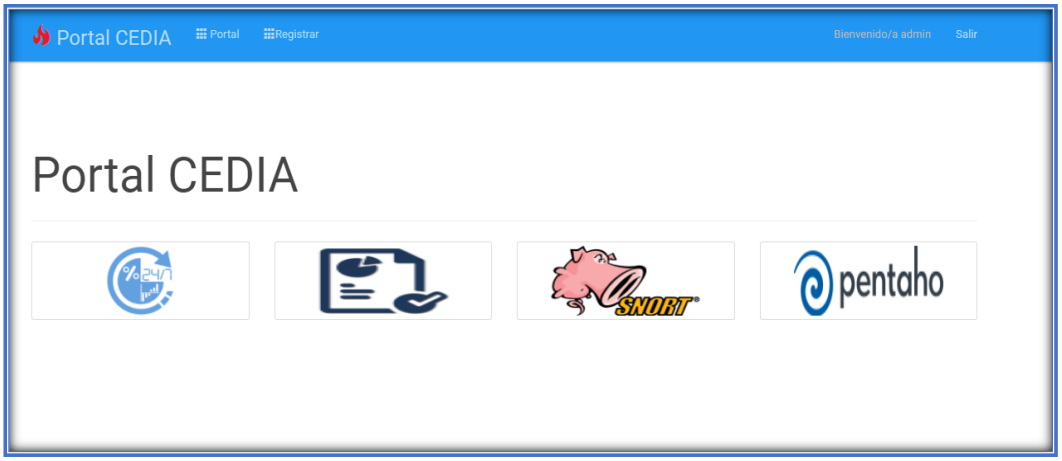


Figura 27. Interfaz de funciones del Sistema BI

Figura 28. Interfaz de registro del Sistema BI

4.4 Fase 4: Desarrollo y pruebas

Esta etapa se vinculó el desarrollo y las pruebas, detallando la instalación y configuración de todo el software, además de los servicios ETL que se han levantado, y por medio de estos, se llegó a generar un ambiente de pruebas para verificar la funcionalidad del producto

4.4.1 Desarrollo

En esta sección se detalla la instalación de todo el software vinculado a la máquina virtual Centos 7 la cual cuenta con arquitectura de 64bits.

Configuración e instalación del software

En esta parte se describe el proceso de instalación de los componentes software, empezando por Snort y PVS, pasando a la instalación del gestor de base de datos,

Pentaho y el sistema BI, por último, puesta en marcha de los procesos ETL (ver Anexo 1).

4.4.2 Pruebas

En esta sección se describen las pruebas realizadas a los sistemas ETL para la carga a la base de datos, y al Sistema BI desarrollado, tomando en consideración los requerimientos establecidos por la parte interesada del CSIRT-CEDIA.

Pruebas a flujos de trabajo ETL

Para los flujos ETL se establecen las pruebas detalladas en la tabla 13, además en las figuras 29, 30 y 31 se puede visualizar la salida sin errores del flujo generado para los trabajos y las transformaciones.

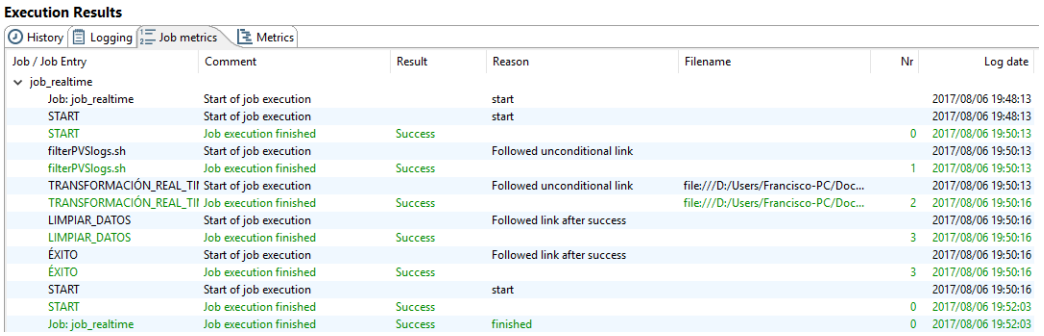
Pruebas al Sistema BI

En la tabla 14 se detalla las pruebas aplicadas al Sistema BI, además en la tabla 15 se presenta el resultado que se ha generado después de la aplicación de las pruebas al Sistema.

Tabla 13

Pruebas a Flujos ETL

Prueba	Descripción
Caja Blanca	Cada transformación y trabajo fue analizado para comprobar su funcionamiento.
Integración	Se analizó la integración del sistema para la recolección de datos y posteriormente el almacenamiento en MySQL.
Funcional	Se verificó que las transformaciones y trabajos ETL se ejecuten de la manera programada y que cumplan con su funcionalidad.

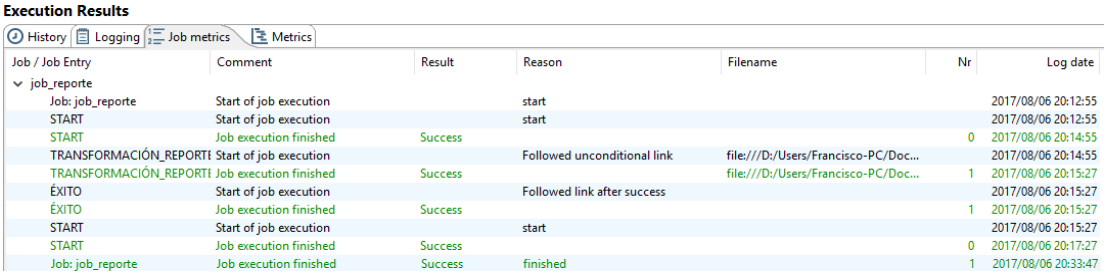


Execution Results

History | Logging | Job metrics | Metrics

Job / Job Entry	Comment	Result	Reason	Filename	Nr	Log date
job_realtime						
Job: job_realtime	Start of job execution		start			2017/08/06 19:48:13
START	Start of job execution		start			2017/08/06 19:48:13
START	Job execution finished	Success			0	2017/08/06 19:50:13
filterPVSlogs.sh	Start of job execution		Followed unconditional link			2017/08/06 19:50:13
filterPVSlogs.sh	Job execution finished	Success			1	2017/08/06 19:50:13
TRANSFORMACIÓN_REAL_TII	Start of job execution		Followed unconditional link	file:///D:/Users/Francisco-PC/Doc...		2017/08/06 19:50:13
TRANSFORMACIÓN_REAL_TII	Job execution finished	Success		file:///D:/Users/Francisco-PC/Doc...	2	2017/08/06 19:50:16
LIMPIAR_DATOS	Start of job execution		Followed link after success			2017/08/06 19:50:16
LIMPIAR_DATOS	Job execution finished	Success			3	2017/08/06 19:50:16
ÉXITO	Start of job execution		Followed link after success			2017/08/06 19:50:16
ÉXITO	Job execution finished	Success			3	2017/08/06 19:50:16
START	Start of job execution		start			2017/08/06 19:50:16
START	Job execution finished	Success			0	2017/08/06 19:52:03
Job: job_realtime	Job execution finished	Success	finished		0	2017/08/06 19:52:03

Figura 29: Trabajo para Real Time PVS

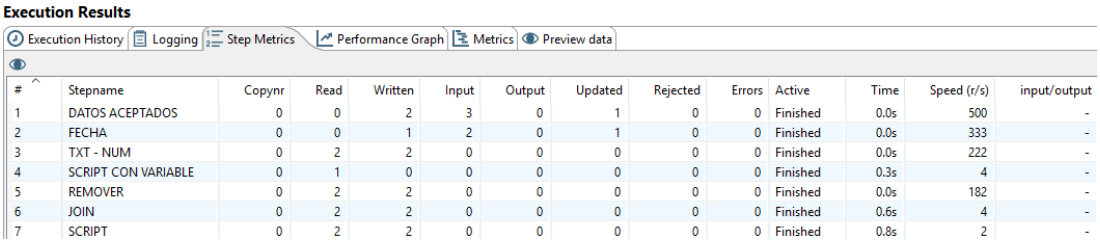


Execution Results

History | Logging | Job metrics | Metrics

Job / Job Entry	Comment	Result	Reason	Filename	Nr	Log date
job_reporte						
Job: job_reporte	Start of job execution		start			2017/08/06 20:12:55
START	Start of job execution		start			2017/08/06 20:12:55
START	Job execution finished	Success			0	2017/08/06 20:14:55
TRANSFORMACIÓN_REPORTI	Start of job execution		Followed unconditional link	file:///D:/Users/Francisco-PC/Doc...		2017/08/06 20:14:55
TRANSFORMACIÓN_REPORTI	Job execution finished	Success		file:///D:/Users/Francisco-PC/Doc...	1	2017/08/06 20:15:27
ÉXITO	Start of job execution		Followed link after success			2017/08/06 20:15:27
ÉXITO	Job execution finished	Success			1	2017/08/06 20:15:27
START	Start of job execution		start			2017/08/06 20:15:27
START	Job execution finished	Success			0	2017/08/06 20:17:27
Job: job_reporte	Job execution finished	Success	finished		1	2017/08/06 20:33:47

Figura 30: Trabajo para Reporte PVS



Execution Results

Execution History | Logging | Step Metrics | Performance Graph | Metrics | Preview data

#	Stepname	Copynr	Read	Written	Input	Output	Updated	Rejected	Errors	Active	Time	Speed (r/s)	input/output
1	DATOS ACEPTADOS	0	0	2	3	0	1	0	0	Finished	0.0s	500	-
2	FECHA	0	0	1	2	0	1	0	0	Finished	0.0s	333	-
3	TXT - NUM	0	2	2	0	0	0	0	0	Finished	0.0s	222	-
4	SCRIPT CON VARIABLE	0	1	0	0	0	0	0	0	Finished	0.3s	4	-
5	REMOVER	0	2	2	0	0	0	0	0	Finished	0.0s	182	-
6	JOIN	0	2	2	0	0	0	0	0	Finished	0.6s	4	-
7	SCRIPT	0	2	2	0	0	0	0	0	Finished	0.8s	2	-

Figura 31: Transformación para filtrar Snort

Tabla 14

Pruebas Sistema BI

Prueba	Descripción
Funcional	Se analizó la funcionalidad del Sistema BI, verificando las pantallas y los enlaces generados con el Sistema Pentaho Business Intelligence.

Tabla 15

Casos de Prueba Sistema BI

Módulo	Prueba	Resultado
Snort	Verificación de generación de reglas	Aprobado
Barnyard2	Conexión con Snort	Aprobado
	Almacenamiento en Gestor de Datos MySQL	Aprobado
Sistema Pentaho BI	Login de Usuarios	Aprobado
	Conexión a base de datos	Aprobado
	Modificación de Dashboards	Aprobado
	Establecer reglas para Usuario	Aprobado
Procesos ETL	Ejecución de eventos en tiempo real PVS	Aprobado
	Ejecución de reportes	Aprobado
	Ejecución de alertas Snort	Aprobado
	Ejecución de filtro Snort	Aprobado
Sistema BI	Login de Usuarios	Aprobado
	Registro de nuevo Usuario	Aprobado
	Ejecución de enlaces a Dashboards	Aprobado

4.5 Fase 5: Evaluación y resultados

Para la finalización del proyecto se realizó la etapa de evaluación y resultados. En esta etapa el sistema se enfrenta a un ambiente real, que además ha sido utilizado como prueba de concepto, que se explica a continuación.

4.5.1 Prueba de concepto

En la figura 32 se describe la prueba de concepto. Para este punto se partió con los datos de Snort y PVS ya almacenados en el gestor de datos MySQL. El ambiente en el cual se ha procedido a instalar todos los componentes del sistema, es un sistema

operativo Centos 7 con arquitectura de 64bits. Los sistemas que se han instalado son: Snort, Barnyard2, PVS, Pentaho Business Intelligence, Pentaho Data Integration y NodeJS. Para la prueba de concepto se ha descartado el análisis de None y Info en PVS y de Low-3 en Snort, esto con el objetivo de no cargar la base con datos incensarios o de poco valor de análisis.

El Sistema comprueba que el ingreso sea de Administrador o de Usuario, posteriormente el cliente que ha ingresado podrá visualizar los Dashboards y si así lo desea podrá imprimir o exportar las tablas a Excel. También cuenta con la opción de acceder a Pentaho, para lo cual, se toma en cuenta el tipo de usuario, ya que solamente los Administradores podrán tener control total de la aplicación Pentaho. Por control total se refiere específicamente: editar Dashboard, editar conexiones a la base de datos y administrar la seguridad. Además, el modo Administrador permite crear usuarios nuevos para el Sistema BI.

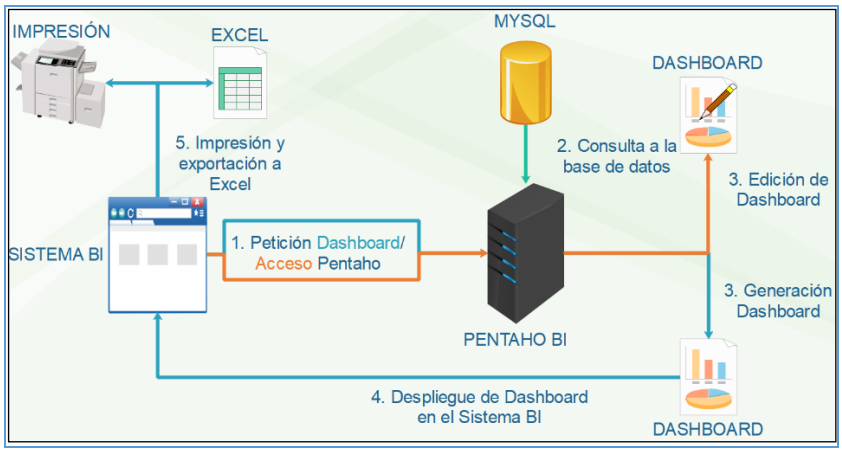


Figura 32. Diagrama para la prueba de concepto

4.5.2 Evaluación de resultados

Una vez finalizado el flujo de trabajo que se aplicó con la metodología de Kimball, los datos se han almacenado de manera exitosa en MySQL, y a través de estos se ha podido generar Dashboards que muestren valores de interesares para las instituciones miembros de CEDIA. A continuación, se analizan los Dashboard que se ha generado para los diferentes sistemas, además se incurre en el análisis de los resultados totales que se han generado.

Dashboard de Eventos en tiempo real de PVS

En la figura 33 se puede visualizar el despliegue del Dashboard para eventos en tiempo real de PVS, en este Dashboard se puede ver el flujo de la red, y ante cambios en el flujo de datos, se presenta un diagnóstico. En este caso se puede constatar que la red 192.188.58.20 está presentado una fuga de información (nombre de usuario y contraseña), ya que posiblemente se encuentre en texto plano.

Dashboard de Reporte de Vulnerabilidades de PVS

En el Dashboard plasmado en la figura 34 se describe la IP que más vulnerabilidades posee, así como el tipo de vulnerabilidad y la cantidad de vulnerabilidades por mes y totales que se han registrado en una fecha y hora específica. Del análisis se puede concluir que el domingo 11 de junio del 2017 a las 14:50:40, se presentó un total de 136 vulnerabilidades totales, de las cuales el host 192.168.102.7, registró el valor más alto, esto debido principalmente a desactualizaciones en los sistemas: Chrome, OpenSSH y MacOS.

Dashboard de Alertas de Snort

En el Dashboard de la figura 35 se visualiza una tabla con las últimas alertas que se han desplegado en el sistema Snort. De este se puede analizar que a las 23:58:53 del 12 de junio del 2017 se presentó un escaneo por SSH de la dirección 58.218.198.162 a la dirección 192.168.102.7, lo que ha surgido por una regla generada por emerging threats.

Figura 33. Dashboard de eventos en tiempo real de la prueba de concepto

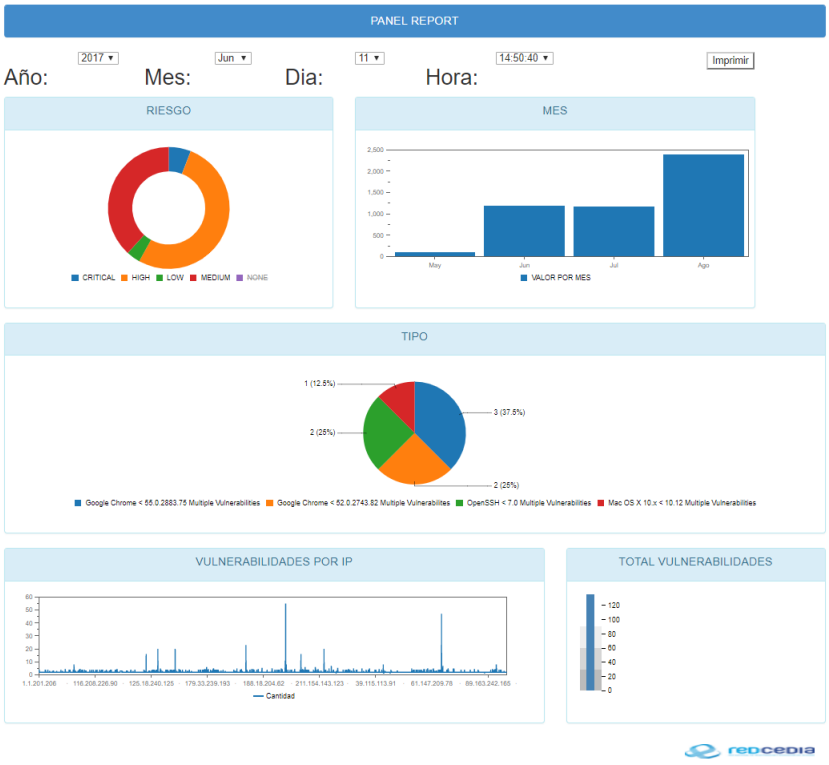
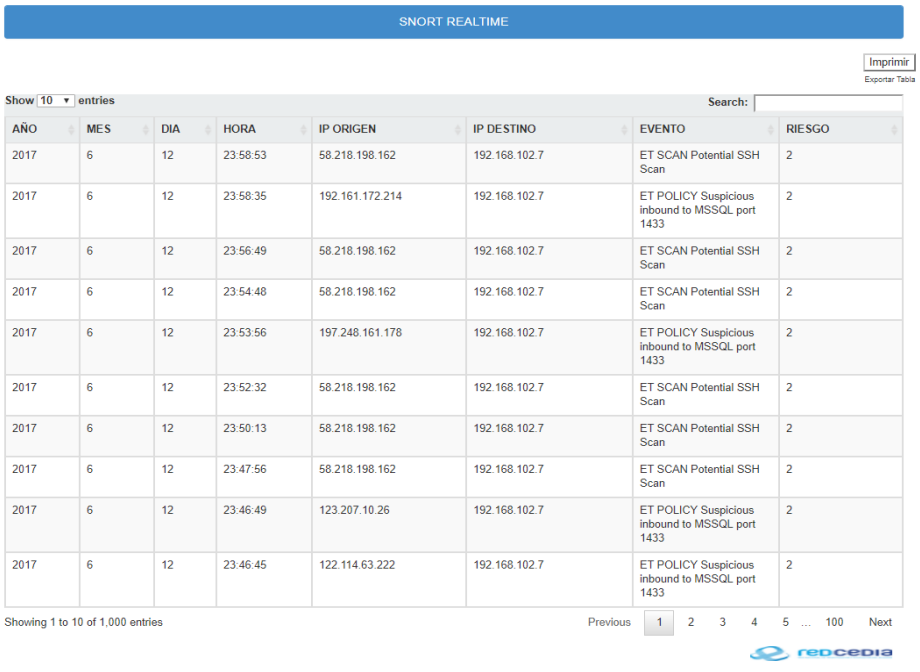


Figura 34. Dashboard de vulnerabilidades de la prueba de concepto



AÑO	MES	DIA	HORA	IP ORIGEN	IP DESTINO	EVENTO	RIESGO
2017	6	12	23:58:53	58.218.198.162	192.168.102.7	ET SCAN Potential SSH Scan	2
2017	6	12	23:58:35	192.161.172.214	192.168.102.7	ET POLICY Suspicious inbound to MSSQL port 1433	2
2017	6	12	23:56:49	58.218.198.162	192.168.102.7	ET SCAN Potential SSH Scan	2
2017	6	12	23:54:48	58.218.198.162	192.168.102.7	ET SCAN Potential SSH Scan	2
2017	6	12	23:53:56	197.248.161.178	192.168.102.7	ET POLICY Suspicious inbound to MSSQL port 1433	2
2017	6	12	23:52:32	58.218.198.162	192.168.102.7	ET SCAN Potential SSH Scan	2
2017	6	12	23:50:13	58.218.198.162	192.168.102.7	ET SCAN Potential SSH Scan	2
2017	6	12	23:47:56	58.218.198.162	192.168.102.7	ET SCAN Potential SSH Scan	2
2017	6	12	23:46:49	123.207.10.26	192.168.102.7	ET POLICY Suspicious inbound to MSSQL port 1433	2
2017	6	12	23:46:45	122.114.63.222	192.168.102.7	ET POLICY Suspicious inbound to MSSQL port 1433	2

Figura 35. Dashboard de Snort

Diagramas Totales de Información

De los datos almacenados, se ha puesto en consideración que la prueba de concepto se la realizó del 7 al 30 de junio del 2017. De la prueba se ha obtenido los siguientes resultados totales.

Se puede ver que la variación en los eventos no es muy considerable, exceptuando el día 27 que es en donde se presentan una cantidad superior en relación a los otros días, no obstante se corrige el origen (Escaneo potencial de SSH) hasta obtener en los días subsiguientes valores similares a los iniciales (ver figura 36 y 37).

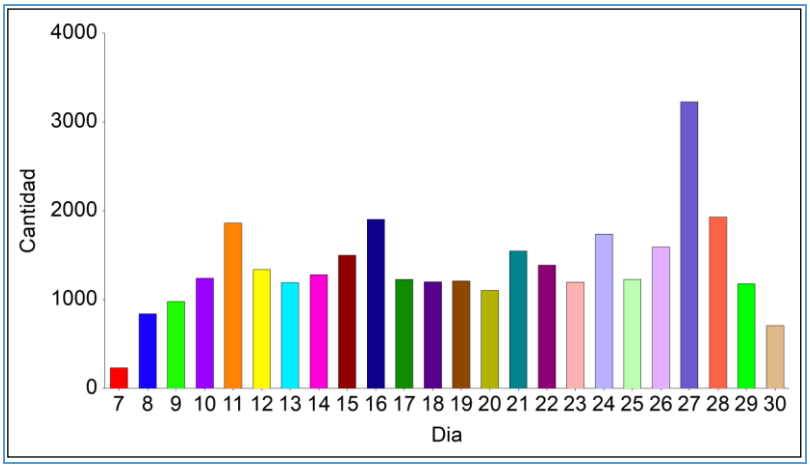


Figura 36. Evaluación eventos por día

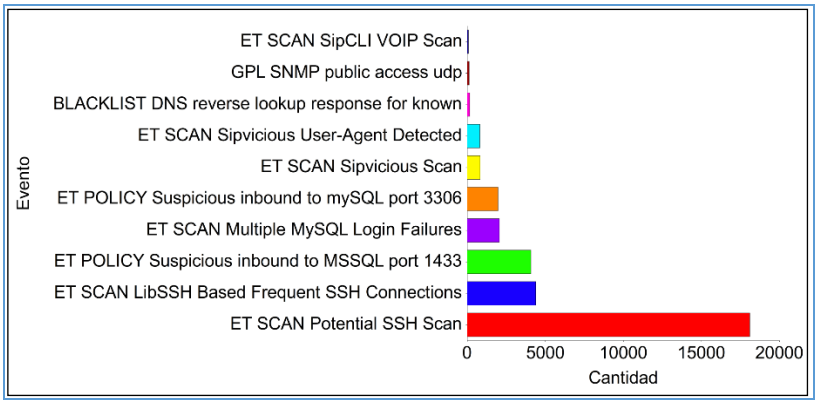


Figura 37. Evaluación tipo de evento y frecuencia

Consecutivamente, se halló un valor exponencial en relación a las direcciones IP en las cuales se encontraron vulnerabilidades. Estas corresponden a servidores que cuentan con puertos y servicios abiertos, y a los cuales por temas de funcionamiento no se los puede cerrar. En los días también se puede visualizar un exponencial que tiene su máxima elevación el día 14, y que a continuación comienza a tener un desenvolvimiento variable, esto debido al incremento en los hosts de análisis (ver figura 38 y 39).

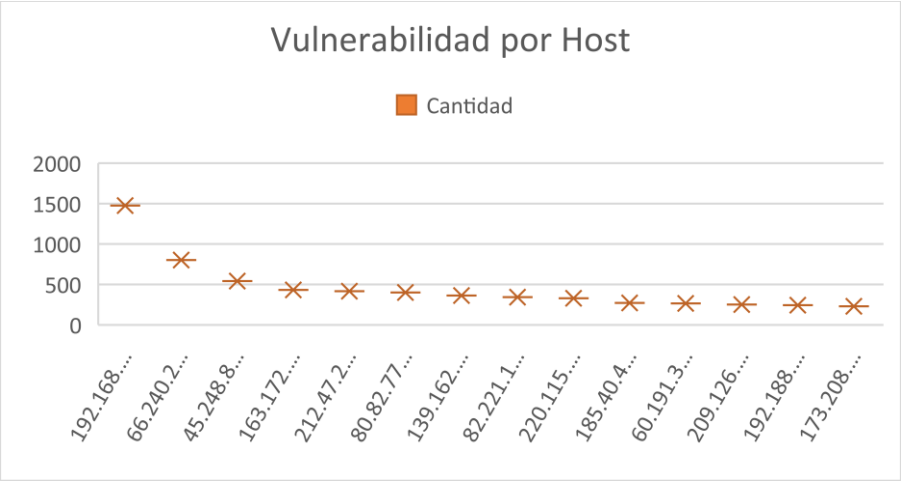


Figura 38. Evaluación vulnerabilidad por host

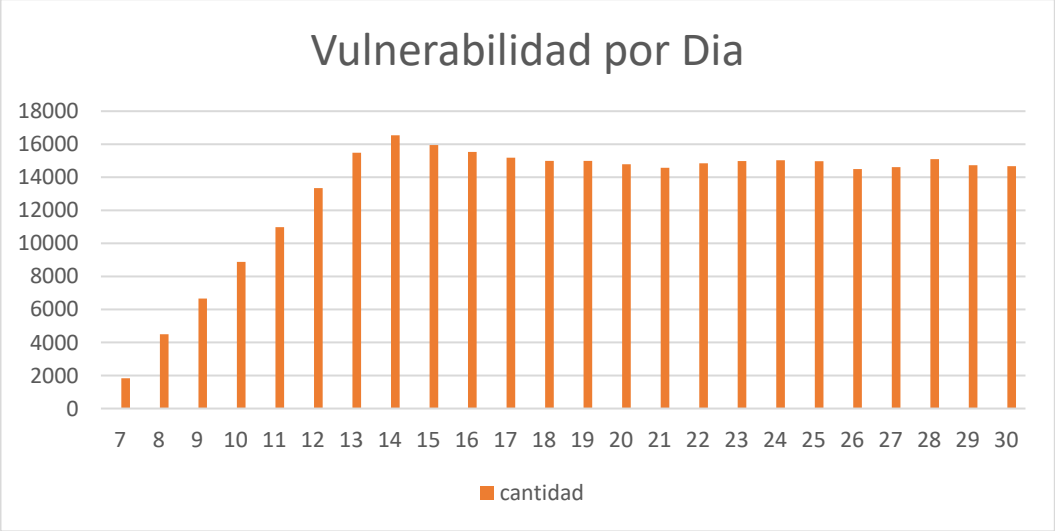


Figura 39. Evaluación vulnerabilidad por día

Por último, se aprecia un gran número de alertas con etiqueta Medium y un valor muy reducido de alertas importantes de analizar. Debido a esto, se puede precisar más atención a la actividad catalogada como Medium, para lograr obtener un valor aceptable de alertas.

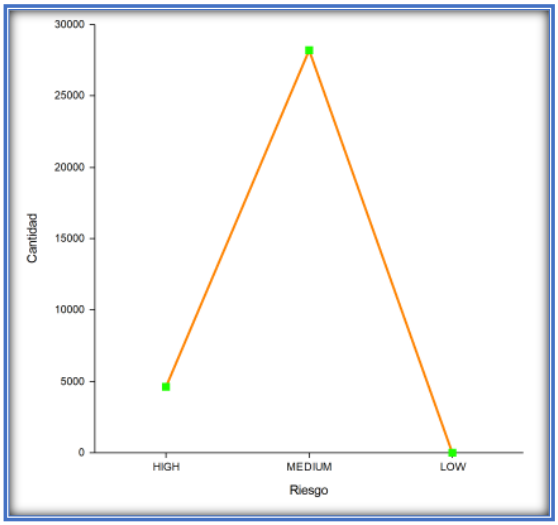


Figura 40. Evaluación Total Riesgo

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El presente estudio se originó con el fin de desarrollar una aplicación que de soporte a un CSIRT académico para identificar de manera rápida los incidentes que se susciten en su respectiva red. Se ha logrado generar una respuesta inmediata para mitigar los posibles daños que el incidente podría ocasionar.

En el presente estudio se diseñó e implementó una solución mediante Business Intelligence que actúe como un factor estratégico en el análisis de vulnerabilidades de un CSIRT académico. Para lograrlo fueron aplicadas la metodología de Investigación-acción y las fases de Ralph Kimball. Se realizó una evaluación de Passive Scanner y Snort las cuales ofrecen una administración de seguridad basada en el tráfico de la red y personalización de sus configuraciones con el fin de reducir los falsos positivos y así mejorar la respuesta a incidentes de seguridad. Se desarrollaron varios algoritmos que permitan aplicar el proceso "Extraer, Transformar y Cargar" de los logs no normalizados que fueron procesados por una interfaz gráfica. Finalmente, se construyó una aplicación de software mediante Scrum, que permita vincular los logs obtenidos en Pentaho BI, con el propósito de generar alertas tempranas como un factor estratégico para el CSIRT de CEDIA. Los resultados muestran que esta aplicación ha logrado captar la atención de los responsables del CSIRT, para establecer prioridades inmediatas y destinar recursos a áreas clave que podrían ser víctimas potenciales de ataques informáticos.

El aporte de este proyecto es la generación de Dashboard empleando Business Intelligence que involucren los dos sistemas (PVS y Snort) para generar una actuación rápida ante incidentes informáticos. Esto es de vital importancia para los miembros de CEDIA, los cuales necesitan estar alertas ante el incremento de ataques a las redes IP.

El proyecto finalizó con la puesta en producción del aplicativo en la infraestructura del CSIRT de CEDIA, quienes firmaron la carta de Aceptación del mismo.

Como resultado de esta investigación, se ha derivado un artículo técnico titulado “Aplicación de Inteligencia de Negocios para el Análisis de Vulnerabilidades para incrementar el Nivel de Seguridad en un CSIRT Académico”, el mismo que ha sido aceptado para publicación en el V Encuentro Internacional y IX Nacional de Investigación en Ingeniería de Sistemas e Informática EIISI 2017, que será desarrollado en la Universidad Pedagógica y Tecnológica de Colombia - UPTC, Tunja Colombia entre el 4 y 6 de octubre de 2017. Además, será publicado en la Revista Facultad de Ingeniería, indexada en LATINDEX, con ISSN 0121-1129 (Ver Anexo 2 y 3).

5.2 Recomendaciones

La utilización total (sin filtros) del sistema supone la disposición de un equipo de computación robusto que ayude en el análisis y almacenamiento de la información generada.

El uso de software libre con respaldo de asistencia comunitaria llega a ser una solución viable en el desarrollo de proyectos, pero a futuro si se desea obtener más ventajas de una herramienta se debe considerar el uso de una versión de pago para optar por trabajar con mejores funciones.

Se debe destinar recursos como talento humano, software, hardware, procesos, etc, en la resolución de los incidentes detectados, ya que, si no se dispone de esto, poco o nada servirá el despliegue del sistema.

Como trabajo futuro se plantea la integración de los aplicativos desarrollados con aquellas herramientas que forman parte del CSIRT y por estudios anteriores relacionados al presente estudio, como el de (Valladares, 2017).

REFERENCIAS BIBLIOGRÁFICAS

Acosta, N., Buitrago, R., Newball, M., Ramírez, M. A., & Sánchez, J. (2004). *Análisis de Vulnerabilidades.*

Analítica. (2013, Junio 26). *www.analitica.com*. Obtenido de http://www.analitica.com/noti-tips/nueva-guia-de-cobit-5-identifica-los-tres-factores-de-cambio-de-la-ciberseguridad/

Armendáriz, R. N., Urdiales, M. V., Corral, J. V., Salcido, M. T., Favela, J. A., & Ávila, R. L. (2016). *CULCYT Cultura Científica y Tecnológica.* Obtenido de http://erevistas.uacj.mx/ojs/index.php/culcyt/article/download/788/852

Azuaje, A. (2014, Diciembre). Obtenido de https://docs.google.com/document/d/1qtaKD91OjqDAIHmCq-hcp2AjT922FTAgP8j9cbdadpU/edit

Bustamante, A. G. (2016). *Universidad Industrial de Santander* . Obtenido de file:///D:/Users/Francisco-PC/Downloads/5575-26814-1-PB.pdf

Canal News Ecuador. (2016, Febrero 18). *canalnews.ec*. Obtenido de http://canalnews.ec/category-seguridad/175-gms-presento-recomendaciones-para-prevenir-ataques-ciberneticos-en-instituciones-educativas

CCM Benchmark. (2008, Octubre 16). *CCM.net*. Obtenido de http://es.ccm.net/contents/18-escaneres-de-vulnerabilidad-analisis-de-puertos

CERT. (2016, Noviembre 1). *CERT*. Obtenido de http://www.cert.org/about/

CSIRT-CEDIA. (2014). *Descripción del CSIRT de CEDIA*. Obtenido de https://csirt.cedia.org.ec/quienes-somos/descripcion-del-csirt-cedia/

Danyliw, R. (2002, Septiembre 13). *Snort Database Plugin Documentation*. Obtenido de

http://www.andrew.cmu.edu/user/rdanyliw/snort/acid_db_er_v102.html#schema

DataSwing. (2013). *http://dataswing.us*. Obtenido de http://dataswing.us/bi/summary.php

Dertiano, V. (2015, Abril 6). Obtenido de http://blog.mirai-advisory.com/?p=545

Díaz Vico, J., Fírvida Pereira, D., & Lozano Merino, M. A. (2013, Diciembre). *www.incibe.es.* Obtenido de https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/int_cnpic_identificacion_reporte_incidentes.pdf

ECU-CERT. (2014). *ITU*. Obtenido de https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/Ecuador_EcuCERT_2014.pdf

ecucert. (2015, Marzo 3). *www.ecucert.gob.ec.* Obtenido de https://www.ecucert.gob.ec/manejo_de_incidentes.html#ANCHOR_Box1

ecucert. (2015, Marzo 3). *www.ecucert.gob.ec.* Obtenido de https://www.ecucert.gob.ec/incidente.html

EcuCERT. (2015, Marzo 3). *www.ecucert.gob.ec*. Obtenido de https://www.ecucert.gob.ec/incidente.html

EcuCERT. (2016, Julio 25). *EcuCERT*. Obtenido de https://www.ecucert.gob.ec/nosotros.html#ANCHOR_Box1

EducaLab. (2014, Marzo 14). *descargas.pntic.mec.es.* Obtenido de http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html

Emerging Threats. (2012, Marzo 3). *Emerging Threats*. Obtenido de http://doc.emergingthreats.net/bin/view/Main/AboutEmergingThreats

ETHACK. (2014, Septiembre 15). *ETHACK Inteligencia en Ciberseguridad y TI.* Obtenido de https://ethack.com/los-20-controles-criticos-en-seguridad/

etic-solutions. (2013). Obtenido de http://www.etic-solutions.net/etic/servicios/analisis-de-vulnerabilidad

European Telecommunications Standards Institute TR 103 305. (2015, Mayo 7). *www.etsi.org.* Obtenido de http://www.etsi.org/deliver/etsi_tr/103300_103399/103305/01.01.01_60/tr_103305v010101p.pdf

FIRST. (2017, Junio 10). *FIRST*. Obtenido de http://www.first.org/about

Freire, J. (2015, Octubre 3). *Ecuador, el cuarto país de la región que recibe más ataques cibernéticos.* Obtenido de http://www.doctortecno.com/noticia/ecuador-cuarto-pais-region-que-recibe-mas-ataques-ciberneticos

Gálvez, A. P. (2016). *Business Intelligence y las Tecnologías de la Información: 2ª Edición.* IT Campus Academy.

Gomez, A. R., & Bautista, D. R. (2010, Abril). *Universidad Tecnológica de Pereira.* Obtenido de http://revistas.utp.edu.co/index.php/revistaciencia/article/viewFile/1803/1209

Gravitar. (2016). *Gravitar.com*. Obtenido de http://gravitar.biz/pentaho/

Gula, R. (2013, Abril 29). *Tenable*. Obtenido de http://www.tenable.com/blog/is-the-passive-vulnerability-scanner-an-intrusion-detection-system

Importancia.org. (2016, Enero 18). *Importancia.org*. Obtenido de http://www.importancia.org/tecnologia.php

ISOTools Excellence. (2015, Marzo 31). *www.pmg-ssi.com.* Obtenido de http://www.pmg-ssi.com/2015/03/iso-27001-establecer-los-objetivos-para-la-ciberseguridad/

Lanfranco, E., Macia, N., Venosa, P., Molinari, L., & Díaz, J. (2010). *Tendencias en incidentes de seguridad atendidos por el CERT académico Cert-UNLP*.

Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/19431/Documento_completo.pdf?sequence=1

Leon, M. (2014, Febrero 9). Obtenido de http://luisleonin.blogspot.com/2014/02/ciclo-de-vida-de-ralph-kimball.html

Lyon, J. (2015). *GITS Ciberseguridad*. Obtenido de http://www.gitsinformatica.com/ciberataques.html

Marchena, N. S., & Reinoso, A. J. (2016). *Universidad Alfonso X El Sabio.* Obtenido de http://www.uax.es/publicacion/herramientas-basadas-en-business-intelligence-bi-para-la-toma-de-decisiones.pdf

Márquez, D., & Marcano, A. V. (2012, Julio 23). *laccei.org*. Obtenido de http://www.laccei.org/LACCEI2012-Panama/RefereedPapers/RP099.pdf

Mendoza, M. (2017, Junio 9). *issuu.com.* Obtenido de https://issuu.com/marcomendoza04/docs/02_material

Mifsud, E. (2012, Marzo 26). *recursostic.educacion.es.* Obtenido de http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=3

National Institute of Standards and Technology - Framework. (2017, Enero 10). Obtenido de https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Navarro, J. (2014, Septiembre 4). *http://www2.deloitte.com.* Obtenido de http://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/CISO/Ley_CiberSeguridad.pdf

NTE INEN-ISO/IEC 27032. (2014). *Instituto Ecuatoriano de Normalización, INEN*. Obtenido de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2015/07/nte_inen_iso_iec_27032.pdf

Oracle. (2016). *MySQL.com*. Obtenido de https://www.oracle.com/es/mysql/index.html

Ortega, D. (2014, Enero 16). Obtenido de http://calidadtic.blogspot.com/2014/01/los-20-controles-de-seguridad-criticos.html

Pentaho. (2016). *CDA*. Obtenido de http://community.pentaho.com/ctools/cda/

Pentaho. (2016). *CDF*. Obtenido de http://community.pentaho.com/ctools/cdf/

Porrúa, M., & Contreras, B. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?*

Proyectos agiles - Funcionamiento. (2017, Julio 11). Obtenido de https://proyectosagiles.org/como-funciona-scrum/

Proyectos agiles - Introducción. (2017, Julio 14). Obtenido de https://proyectosagiles.org/que-es-scrum/

Recomendación UIT–T X.1205. (2010, Septiembre 20). *http://www.itu.int*. Obtenido de http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

REDCEDIA. (2014, Mayo 28). *cedia.edu.ec*. Obtenido de https://www.cedia.edu.ec/es/inicio-es/quienes-somos

REDCEDIA. (2014, Mayo 28). *Quíenes somos CSIRT CEDIA*. Obtenido de https://csirt.cedia.org.ec/quienes-somos/

Registro de Direcciones de Internet para América Latina y Caribe. (2009). *lacnic.net*. Obtenido de http://www.lacnic.net/web/lacnic/csirts

Rivadera, G. (2010). *La metodología de Kimball.* Obtenido de http://www.ucasal.edu.ar/htm/ingenieria/cuadernos/archivos/5-p56-rivadera-formateado.pdf

Sánchez Cali, F. G. (2014, Noviembre 11). *www.academia.edu.* Obtenido de https://www.academia.edu/9252886/Norma_ISO_IEC_27032

TechTarget. (2012, Noviembre). *Searchdatacenter*. Obtenido de http://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT

Torruela González, J. (2017). *ANCIBE*. Obtenido de http://www.ancibe.com/documents/GuiaCCFC.pdf

Valladares, P. (2017). Obtenido de http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/13123/T-ESPE-057254.pdf?sequence=1&isAllowed=y

Wiki Pentaho. (2016). *http://wiki.pentaho.com*. Obtenido de http://wiki.pentaho.com/display/EAI/.01+Introduction+to+Spoon