ANÁLISIS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD BASADOS EN SOFTWARE LIBRE EN LA RED DE DATOS ADMINISTRATIVA DE LA CORPORACIÓN UNIVERSITARIA DEL HUILA CORHUILA

ALEX RICARDO RINCON SILVA

CORPORACIÓN UNIVERSITARIA DEL HUILA - CORHUILA

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

NEIVA

2018

ANÁLISIS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD BASADOS EN SOFTWARE LIBRE EN LA RED DE DATOS ADMINISTRATIVA DE LA CORPORACIÓN UNIVERSITARIA DEL HUILA CORHUILA

ALEX RICARDO RINCON SILVA

Trabajo de grado presentado como requisito parcial para optar el título de

Ingeniero de Sistemas

Asesor: Eduardo Martínez Vidal

CORPORACIÓN UNIVERSITARIA DEL HUILA - CORHUILA

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

NEIVA

2018

TABLA DE CONTENIDO

LISTA DE IMÁGENES

LISTA DE TABLAS

LISTA DE ANEXOS

1. Introducción

La seguridad de la información está conformada por diversos aspectos, entre ellos la disponibilidad, comunicación, identificación de problemas, el análisis de riesgos, la integridad, confidencialidad y la recuperación de los riesgos.

En un sentido general, seguridad significa proteger nuestros activos. Esto puede significar protegerlos de atacantes que invaden nuestras redes, desastres naturales, ambientes adversos, condiciones ambientales, fallas de energía, robo o vandalismo u otros estados indeseables. En última instancia, intentaremos protegernos contra las más probables formas de ataque, en la medida de lo razonablemente posible, dado nuestro entorno. (Andress, 2011)

Precisamente, la reducción o eliminación de riesgos, asociados a un activo de información, es el objetivo de la seguridad de la información y la seguridad informática. Más concretamente, la seguridad de la información tiene como objeto, los sistemas, el acceso, uso, divulgación, interrupción o destrucción, no autorizada de información. Los términos seguridad de la información, seguridad informática, son usados frecuentemente como sinónimos, porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información.

Además, la seguridad de la información involucra la implementación de estrategias que cubren los procesos, en donde la información es el activo primordial. Estas estrategias deben tener como punto fundamental, el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos, para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y

salvaguardar tanto información, como los sistemas que la almacenan y administran. La seguridad de la información incumbe a gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas con información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o nueva línea de productos caigan en manos de un competidor; o, se vuelva pública de forma no autorizada, podría ser causal de pérdida de credibilidad de los clientes, demandas legales o incluso la quiebra de la misma.

La seguridad de la información cada día tiene más relevancia en nuestra realidad, podemos recordar casos como ***hackeo a la red de juegos de sony-playstation, la fuga de información de la empresa de perfiles de créditos equifax***. También en Colombia cada día se registran en más de 500 mil ataques informáticos (Andress, 2011).

La Corporación Universitaria del Huila - CORHUILA, cuenta con una infraestructura tecnológica dedicada a:

- Procesamiento de información académica (Sistema de información Académico)
- Procesamiento de información administrativa (Talento Humano)
- Procesamiento de información financiera.
- Apoyo a los procesos de enseñanza y aprendizaje a través de Sistemas para la gestión del aprendizaje (LMS)[1].

[1] Un sistema de gestión de aprendizaje es un software instalado en un servidor web que se emplea para administrar, distribuir y controlar las actividades de formación no presencial (o aprendizaje electrónico) de una institución u organización. Permitiendo un trabajo de forma asíncrona entre los participantes. Tomado de: https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_aprendizaje

En consecuencia para reducir el riesgo e impacto de un ataque informático en la infraestructura tecnológica de la Corporación Universitaria del Huila - CORHUILA, este proyecto busca sugerir y en la medida lo posible implementar una serie de controles de seguridad basados en software y hardware libre.

El software libre es un esquema de licenciamiento[2] que garantiza 4 libertades esenciales al usuario:

0 - la libertad de usar el programa, con cualquier propósito (uso).

1 - la libertad de estudiar cómo funciona el programa y modificarlo, adaptándolo a las propias necesidades (estudio).

2 - la libertad de distribuir copias del programa, con lo cual se puede ayudar a otros usuarios (distribución).

3 - la libertad de mejorar el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie (mejora). (www.gnu.org, 2001).

El presente proyecto busca dejar como última meta un registro escrito de una metodología para afrontar el proceso de asegurar y mantener la seguridad de una infraestructura tecnológica, para así apoyar este tipo de estudios en la Corporación Universitaria del Huila – CORHUILA.

[2] Una **licencia** **de *software*** es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribución) y el licenciatario[2] (usuario consumidor, profesional o empresa) del programa informático, para utilizarlo cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas,[3] es decir, es un conjunto de permisos que un desarrollador le puede otorgar a un usuario en los que tiene la posibilidad de distribuir, usar o modificar el producto bajo una licencia determinada. Además se suelen definir los plazos de duración, el territorio donde se aplica la licencia (ya que la licencia se soporta en las leyes particulares de cada país o región), entre otros. Tomado de: https://es.wikipedia.org/wiki/Licencia_de_software

2. Objetivos

2.1 Objetivo General

Realizar un análisis que permita implementar controles de seguridad basados en software y hardware libre para la red de datos administrativa de la Corporación Universitaria del Huila - CORHUILA.

2.2 Objetivos Específicos

- Analizar el nivel de seguridad actual de la red de datos administrativa de la Corporación Universitaria del Huila - CORHUILA.
- Diseñar los niveles de seguridad para la red de datos administrativa de acuerdo a los requerimientos definidos por la Corporación Universitaria del Huila - CORHUILA.
- Implementar los controles de seguridad en toda la red de datos administrativa de la Corporación universitaria del Huila, Corhuila.
- Establecer las herramientas de monitoreo de la red de datos administrativa de la Corporación universitaria del Huila, Corhuila.

3. Definición del problema

Para observar la gravedad del problema de “la falta de controles de seguridad” actualmente a nivel mundial (Forbes, 2017) en su reporte informa que “las empresas enfrentan hoy más retos de seguridad informática que nunca antes” y “el 64% de los empresarios incrementaran sus presupuestos y gastos en estrategias de seguridad informática así como servicios profesionales necesarios para protegerse contra las llamadas amenazas conocidas”, lo anterior es un reflejo a las tendencias de los eventos de seguridad en los últimos años recabados por (Quick, Hollowood, & Miles, 2018).

(Morgan, 2018) en su artículo en “CSO from IDG” “top 5 hechos, figuras y estadísticas de seguridad informática”, recalca:

1. Los daños causados por el crimen informático ascenderán a 6 trillones de dólares para el 2021.
2. Los gastos en seguridad informática excederán 1 trillón de dólares entre 2017 y 2021.
3. Los criminales informáticos triplicaran el número de empleos aun no llenos necesarios para combatirlos.
4. Las personas como superficie de ataque (victimas) alcanzara los 6 billones para el 2022.
5. El ransomware causara pérdidas de más de 5 billones dólares este año.

En el ámbito global tenemos casos como el de Facebook y Google en los cuales por fallas de diseño o vulnerabilidades de código han permitido la fuga de 50 millones y 500 mil registros de personas que utilizan las respectivas plataformas, lo anterior reportados por las

mismas empresas (Wong, 2018) y (Goodin, 2018); Debido a las nuevas legislaciones respecto a la protección de datos personales y privacidad de los usuarios en Unión europea y Estados Unidos, estas grandes empresas de tecnología están en gran riesgo de demanda por parte de millones de personas como demuestra el ejemplo descrito por (Statt, 2018) en su artículo titulado "Facebook enfrenta demandas por nuevo hackeo masivo".

Es de recalcar que, en ambos casos de estas grandes empresas, las funcionalidades implementadas en los sitios fueron explotadas, pero no hay evidencia de quienes son los atacantes, dejando a muchos usuarios con la incertidumbre de si sus datos fueron vulnerados.

Colombia no está exenta a estas tendencias, de los casos reportados a la unidad de delitos informáticos de la dijín el 40% de los casos son a empresas en los sectores de telecomunicaciones, financieros e industrial (MEDINA, 2016), tomemos por ejemplo lo reportado en la prensa "El Tiempo" (Velásquez, 2018) en cual recalcan técnicas que los criminales usan para extorsiona a personas comunes las cuales fueron víctimas en el pasado de fugas o hackeos masivos, con la frase "su contraseña es ****** y se su secreto" intimidan a gran cantidad de ciudadanos.

En Colombia también como todos los gobiernos del mundo fueron objetivos de delincuentes informáticos, un caso de muy sonoro fue el "website defacement" (Romagn & Van Ven Hout, 2017) de la "Procuraduría General De La Nación" , este delincuente con un largo prontuario, aprovechaba las vulnerabilidades de muchos sitios web y luego borraba cualquier rastro que permitiera su identificación en el mundo real, luego del trabajo de las autoridades fue atrapado . (El Tiempo, 2016)

Luego de observar estas tendencias, es claro que las probabilidades de sufrir un ataque informático en una infraestructura tecnológica son muy altas y se hace necesario que toda empresa o entidad gubernamental diseñe e implemente estrategias para contener y evitar la ocurrencia de estos hechos que podrían ser definidos como catastróficos.

Actualmente es una obligación por parte de toda entidad pública y privada, proteger los datos personales. (EL CONGRESO DE COLOMBIA, 2012)

La constante evolución de las tecnologías de la información, promovida por diferentes directivas gubernamentales y/o institucionales, ha creado una metodología de avance feroz y acelerada, en el diseño e implementación de las mismas, orientado únicamente a alcanzar, mejorar o establecer indicadores para satisfacer metas de producción.

Con toda esa premura, se dejan aparte cuestionamientos metodológicos, en los cuales, las acciones para asegurar la información como activo valioso, no son una prioridad o ni siquiera un ítem a tener en cuenta la lista de tareas de los proyectos tecnológicos y/o productivos.

En la actualidad innegable la necesidad de asegurar la información, que una entidad posee de lo contrario el responsable de la información estará expuesto a riesgos operacionales, así como riesgo reputacional (Federal Financial Institutions Examination Council's (FFIEC), 2010) y/o demandas por fallas en cumplir la legislación vigente.

3.1. Pregunta Problema

¿Está la infraestructura tecnológica de la Corporación Universitaria del Huila - CORHUILA dotada de los controles de seguridad necesarios para mantener el riesgo de incidentes de seguridad informáticos en un nivel bajo en una escala de criticidad?

4. Justificación

El propósito de este proyecto es el de reducir el riesgo inherente a la seguridad de la información en las infraestructuras tecnológicas de la Corporación Universitaria del Huila – CORHUILA, estos riesgos por ejemplo : perdida monetaria, daño a la reputación, comprometer la percepción de la marca y las repercusiones legales de las fugas de información privada y sensible de los estudiantes, para lograr ese propósito se enfoca en las vulnerabilidades técnicas presentes en la infraestructura tecnológica de la misma corporación universitaria.

En la actualidad, el manejo de la información de manera segura, y los ataques informáticos a plataformas tecnológicas, en busca de activos sensibles, representan las mayores amenazas en la década, y la tendencia indica que este escenario, es cada vez más riesgoso para las entidades, (entiéndase empresas). La corporación universitaria del Huila CORHUILA necesita implementar medidas de seguridad para afrontar los retos tecnológicos que conllevan manejar la información de miles de estudiante y su propia información financiera. (Richmond, 2011)

La creación e implementación sistemas de seguridad es un componente profundo en las plataformas e infraestructuras tecnológicas. es tanta su importancia, que en caso de no se han implementado controles de seguridad, se han materializado incidentes de seguridad conocidos como fugas de información y violaciones a la integridad de la misma, como son los casos de Sony, RSA y la universidad de los Andes. (entertaiment, 2014)

Obedeciendo a esta tendencia de las empresas o entidades a buscan establecer controles de seguridad para la información que manejan, en respuesta la creciente industria de la seguridad informática, ofrece nuevas soluciones cada vez más simples, pero con un costo

presupuestal muy alto; esto lleva a elegir entre costos, gastos, riesgos y retornos de inversión, los cuales muchas veces en pro de la rentabilidad de la empresa son manejados de manera incorrecta. (DSIT, 2016)

Este proyecto busca demostrar que se puede asegurar una infraestructura como la de CORHUILA con un menor costo al utilizar software libre. primero analizando el estado actual de la corporación universitaria en lo que respecta a seguridad. Ya que este documento estará para uso de la comunidad estudiantil, permitirá señalar los primeros pasos en el camino a aquellos estudiantes que quieran aprender más sobre la seguridad informática.

4.1 Diagnóstico

Actualmente la Corporación Universitaria del Huila - CORHUILA, tiene grandes falencias y un gran número de vulnerabilidades técnicas en sus sistemas, esto debido a una dependencia a software obsoleto y algunos sin soporte, así como también a la falta de políticas y procedimientos de control para las actualizaciones constantes y periódicas de los sistemas.

4.2 Pronóstico

Debido a un vacío en el ciclo de actualizaciones de los sistemas informáticos y a la falta de controles de seguridad en la CORHUILA, la probabilidad de un incidente de seguridad de tipo fuga de información o daño a la reputación es medianamente probable. por ejemplo, el

cambio de la información almacenada en la plataforma de clases virtuales, también como la indisponibilidad de la plataforma de notas.

4.3 Control Del Pronóstico

Si se implementan controles de seguridad propuestos en este proyecto al igual que las recomendaciones del análisis de vulnerabilidades, la probabilidad de que ocurra un evento de fuga de información o daño a la reputación, se ve reducido a muy poco probable y la corporación universitaria del Huila, Corhuila, esté más preparada a afrontar retos de seguridad imprevistos.

5. Metodología

Para el desarrollo del presente trabajo se hace uso parcial de la metodología **Penetration Testing Execution Standard** en su capítulo de modelado de amenazas y análisis de vulnerabilidades (PTES, 2009) esto con el fin primero de determinar que máquinas entrarán en el alcance de las pruebas y segundo determinar las fallas técnicas inherentes en el software de las maquinas dentro del alcance anteriormente definido.

Para determinar la criticidad de los riesgos usaremos el método cuantitativo ampliamente recomendado por estándares como (ISO International Organization for Standardization, 2018), consistirá en multiplicar el valor cuantitativo del impacto con el valor de la probabilidad de este ocurra, es de aclarar que la probabilidad de ocurrencia depende del tiempo desde que la vulnerabilidad técnica se hizo pública, así mismo dependerá si existen pruebas de concepto y exploits (Kennedy, O'Gorman, Kearns, & Aharoni, 2011) ya publicados de la misma vulnerabilidad; el impacto va determinado por el tipo de vulnerabilidad y sus consecuencias, así como la criticidad del activo afectado. Estos cálculos ya vienen integrados en las herramientas de análisis de vulnerabilidades ejemplo (OpenVas, 2009)

De acuerdo con la metodología seleccionada, las diferentes actividades se desarrollaron así: Para alcanzar los objetivos establecidos se seguirán los siguientes pasos

1. Medir los niveles de seguridad de las plataformas tecnológicas

2. Definir niveles de criticidad de los riesgos dependiendo de la importancia de los activos en función a la sensibilidad de información manejada.
3. Implementar y probar los controles definidos en el transcurso del proyecto con ayuda del administrador del sistema.

Como requisito para realizar estas actividades es necesaria la aprobación por parte del administrador y el propietario de los sistemas a con los cuales se va a trabajar.

Las actividades definidas con anterioridad pueden ser ejecutadas en jornadas periódicas de 8 horas. Para no interrumpir actividades de la entidad, se recomienda realizarlas en horario no laboral como son horas nocturnas, fines de semana o feriados.
Se recomienda realizar el mismo durante las festividades, ya sea realizar todas las actividades en 1 sola semana o en 4 fines de semana.
Luego de conseguir se concretarán los cronogramas con fechas según aprobación de la administración de los sistemas.

El administrador del área tecnológica de la corporación universitaria del Huila, luego de entregarnos acceso a la red, procedió a entregar el listado de direcciones ip’s, las cuales conforman una infraestructura que soporta varios servidores virtualizados con un hipervisor de Oracle, la información exacta de la infraestructura no es entregada en este proyecto con el fin de evitar revelar información sensible que pueda usarse para fines maliciosos.

Dentro del proceso se hizo un escaneo de red con NMAP y un escaneo de vulnerabilidades con OPENVAS:

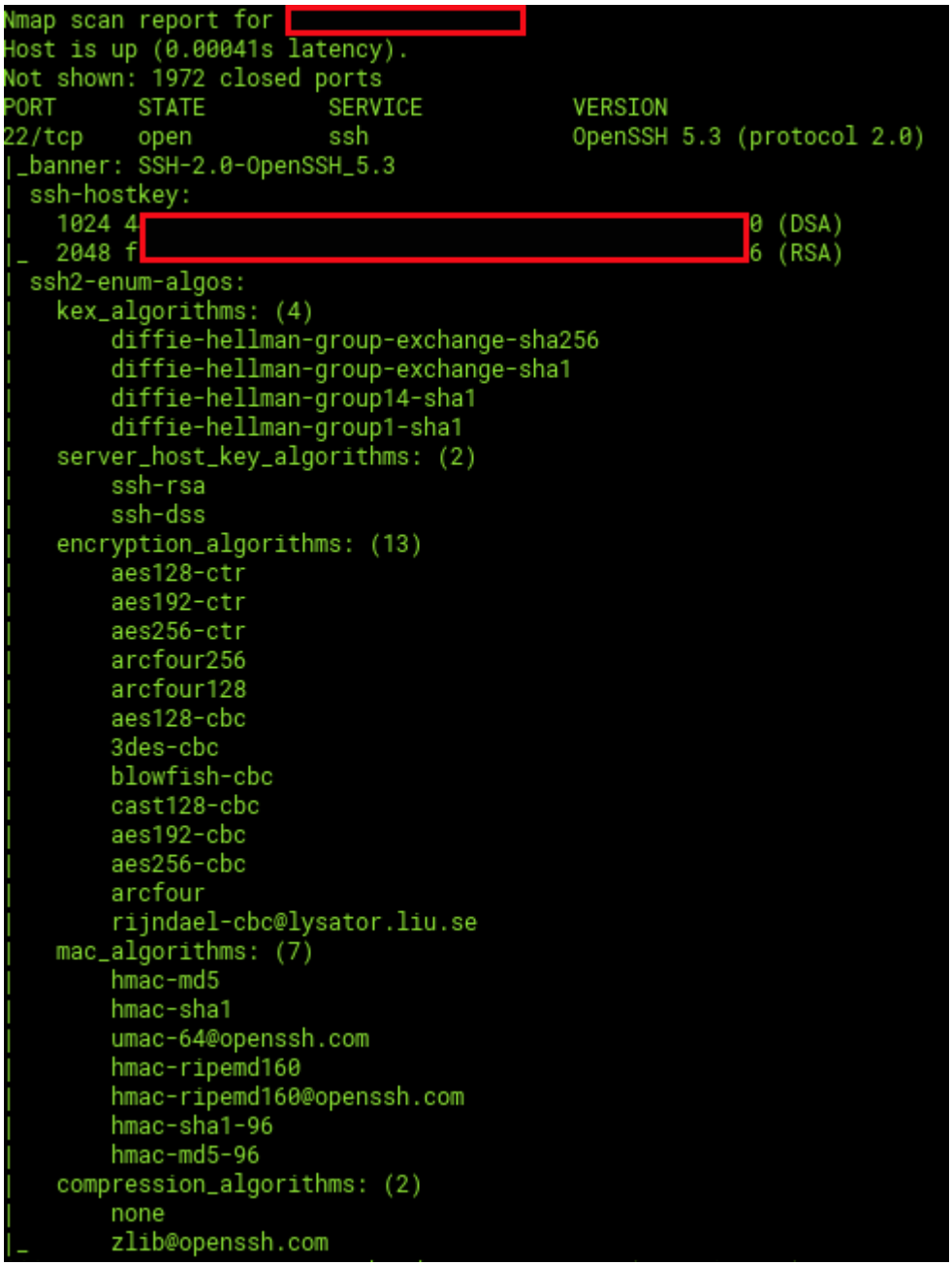


Imagen 1: Escaneo de vulnerabilidades

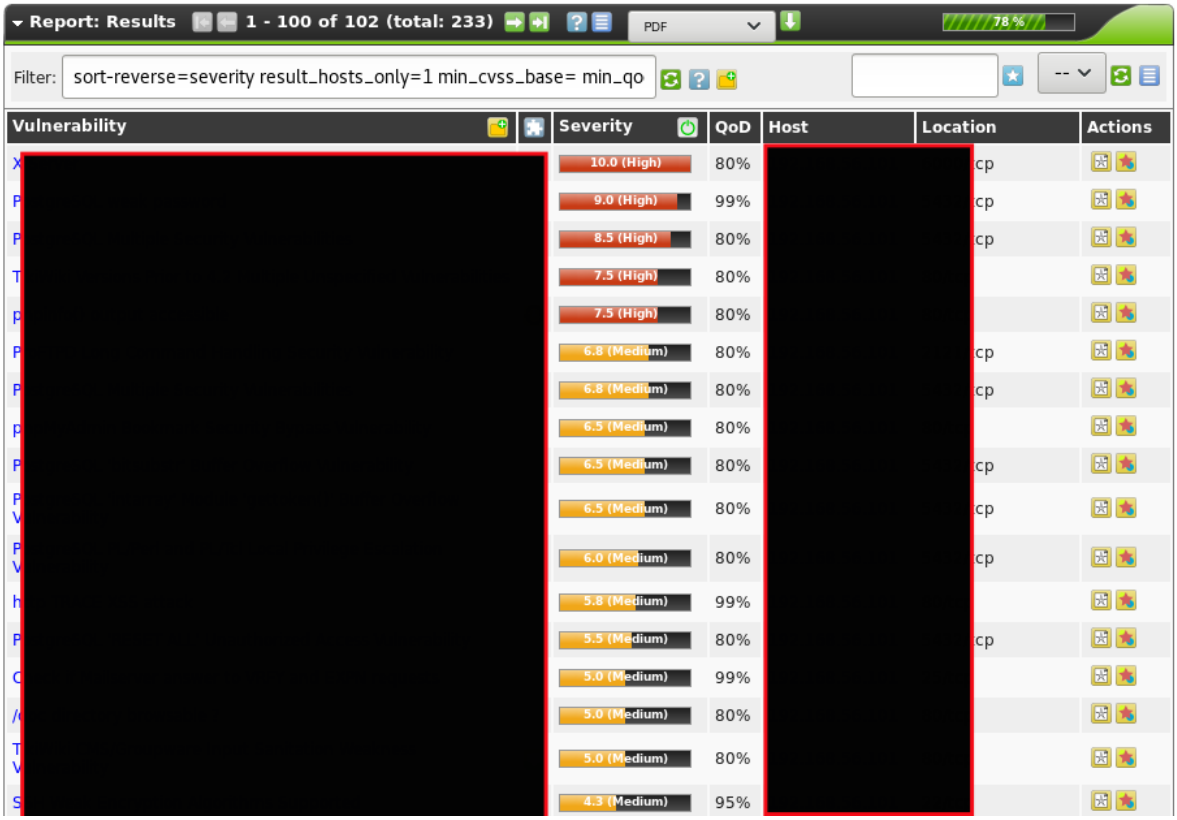


Imagen 2: Reporte de vulnerabilidades

Luego de esto se procedió a informar a los administradores las vulnerabilidades y las remediaciones posibles a seguir para cada una.

6. Marco Referencial

6.1 Marco Teórico

En la actualidad se tienen varios estudios de implementaciones de seguridad combinando y/o basadas en software libre, entre ellos tenemos "*DISEÑO E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, RED Y VIRTUALIZACIÓN APOYADAS CON SOFTWARE LIBRE EN LA COMPAÑÍA TECNOLOGÍA Y REDES S.A.S." por parte de JAVIER ORLANDO ALARCON VARGAS de la FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES*". (Vargas, 2016) En ese proyecto se diseñó y se implementaron políticas y controles de seguridad basados en la norma ISO 27000, COBIT 5 e ITIL 3, para este proyecto será base los controles de iso 27001 (A.14 Adquisición de sistemas de información, desarrollo y mantenimiento, A.16 Administración de los incidentes de seguridad, A.18 Cumplimiento legales, de estándares, técnicas y auditorías). (Kosutic, 2013)

La seguridad de la información es el conjunto de controles de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la integridad, la disponibilidad y confidencialidad de la misma.

En un sentido general, seguridad significa proteger nuestros activos. Esto puede significar protegerlos de atacantes que invaden nuestras redes, desastres naturales, ambientes adversos, condiciones ambientales, fallas de energía, robo o vandalismo u otros estados indeseables. En última instancia, intentaremos protegernos contra las más probables formas de ataque, en la medida de lo razonablemente posible, dado nuestro entorno (Andress, 2011).

6.2 Marco Conceptual

Las actuales guías, estándares y compendios referentes a seguridad de la información son:

- **Controles de seguridad**: Son los mecanismos, lógicos, procedimentales, hardware o software utilizados para manejar riesgos de acuerdo al apetito de riesgo de la organización (Kosutic, 2013).
- **Correlacionador de Eventos de Seguridad**: Es un software destinado a centralizar y correlacionar registros y eventos en dispositivos conectados de una infraestructura, esto se lleva a cabo gracias a reglas y firmas de correlación previamente establecidas. (Dr.dobb's, 2007)
- **CPTE:** Certified Penetration Testing Engineer es una certificación de seguridad de la información respaldada por Mile2. El profesional certificado ha acreditado tener conocimiento en 5 elementos clave del Penetration Testing (Pruebas de Intrusión): recopilación de información, escaneo, enumeración, explotación y reporte (CPTE).
- **DIY:** Los comportamientos de "hágalo usted mismo" (DIY) abarcan un amplio espectro de actividades tales como remodelación de reparación móvil, jardinería y proyectos dirigidos al consumo, tales como muebles hechos a mano. DIYers que producen sus propios bienes y servicios amplían la visión tradicional de los consumidores como compradores y usuarios de productos (McQuitty, 2013).
- **Escaneo de red:** es un proceso que envía solicitudes de clientes a un rango de direcciones de puerto de servidor en un host, con el objetivo de encontrar un puerto activo; este no es un proceso nefasto en sí mismo. La mayoría de los usos de un

escaneo de puertos no son ataques, sino simples sondeos para determinar los servicios disponibles en una máquina remota (Shirey, 2000).

- **Exploit:** es fragmento de código o software completo que permite aprovechar vulnerabilidades técnicas de seguridad en otros servicios informáticos o software. (Kennedy, O'Gorman, Kearns, & Aharoni, 2011)
- **GPL:** significa General Public License («Licencia Pública General»). La más difundida de tales licencias es la Licencia Pública General de GNU, o «GPL de GNU», para abreviar. Puede reducirse aún más, a «GPL», cuando se sobreentiende que nos estamos refiriendo a la «GPL de GNU» (Satllman, 2015).
- **Hardware Libre:** es todo hardware cuyos esquemas de diseño y programación son de dominio GPL, open source o público para la creación de circuitos DIY (Satllman, 2015).

- **ISO 27000:** es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005, y actualizado en 2013 por International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC) (Iso.Org).

- **Openvas:** es un marco de varios servicios y herramientas que ofrece una solución integral y potente de análisis de vulnerabilidades y gestión de vulnerabilidades. El marco forma parte de la solución de gestión de vulnerabilidades comerciales de Greenbone Networks, desde la cual se han realizado desarrollos para la comunidad de código abierto desde 2009. Todos los productos OpenVAS son Software Libre.

La mayoría de los componentes están licenciados bajo la Licencia Pública General de GNU (GNU GPL) (OpenVas, 2009).

- **PTES:** Es un nuevo estándar diseñado para proporcionar tanto a las empresas como a los proveedores de servicios de seguridad un lenguaje común y alcance para realizar pruebas de penetración (es decir, evaluaciones de seguridad). Comenzó a principios de 2009 después de una discusión que provocó entre algunos de los miembros fundadores sobre el valor (o la falta de) de las pruebas de penetración en la industria (PTES, 2009).
- **Vulnerabilidad:** Está íntimamente relacionado con el riesgo y la amenaza y se puede definir como la debilidad o grado de exposición de un sujeto, objeto o sistema. También son aquellas fallas, omisiones o deficiencias de seguridad que puedan ser aprovechadas por los delincuentes (Riesgo).
- **Ransomware:** es un programa diseñado con fines maléficos, su función es restringir el acceso a partes de los sistemas o los archivos alojados en el mismo, esto con el propósito de pedir un rescate (extorsión) para recuperar el acceso.

6.3 Marco Histórico

6.3.1 Historia de la seguridad informática:

“En estos días, la información fluye a través de sistemas informáticos como el flujo de peces a través del mar. Esto presenta una gran cantidad de oportunidades para que las personas roben datos; es por eso que la seguridad de la información es una necesidad. Pero,

¿cómo ha evolucionado la seguridad de la información a lo largo de los años? Echemos un vistazo al historial de seguridad de la información.

1960: las organizaciones comienzan a proteger sus computadoras

Las mayores preocupaciones de seguridad en este intervalo fueron en los puntos de acceso. Cualquier persona con suficiente conocimiento sobre cómo trabajar con una computadora podría entrar en una instalación y comenzar a acceder a datos confidenciales. Para asegurar los terminales, se agregaron contraseñas a las contraseñas y varias capas de protección de seguridad.

1970: Comienzan los primeros ataques de hackers

En este punto de la historia de la seguridad de la información, la informática en red estaba en su infancia (Internet, tal como la conocemos hoy, no existiría hasta finales de la década de 1980). Sin embargo, aunque no existía una red global masiva que conectara todos los dispositivos que querían conectarse, las grandes organizaciones, especialmente los gobiernos, estaban comenzando a vincular computadoras a través de líneas telefónicas. Al reconocer esto, la gente comenzó a buscar formas de infiltrarse en las líneas telefónicas conectadas a las computadoras, de modo que pudieran robar datos. Estas personas se convirtieron en los primeros grupos de piratas informáticos.

Década de 1980: los gobiernos se vuelven proactivos en la lucha contra el delito cibernético

En la década de 1980, la piratería ya había florecido en un problema internacional de delincuencia. Los sistemas limitados de seguridad de la información no podían mantenerse

al día con el aluvión constante de enfoques inteligentes que los hackers usaban para entrar en los sistemas informáticos. Este hecho se volvió extremadamente prominente cuando un pequeño grupo de adolescentes de Milwaukee, conocido como "los 414", irrumpió en más de 60 sistemas informáticos militares y corporativos y robó más de $ 70 millones de los bancos estadounidenses. En respuesta a esta crisis de seguridad de la información, los gobiernos comenzaron a perseguir activamente a los piratas informáticos, incluido el 414s. En este punto en el tiempo, las sentencias eran extremadamente ligeras, desde severas advertencias hasta libertad condicional.

Década de 1990: el crimen organizado se involucra en la piratería

Después de que la red mundial se puso a disposición en 1989, las personas comenzaron a poner su información personal en línea; las entidades del crimen organizado vieron esto como una posible fuente de ingresos y comenzaron a robar datos de personas y gobiernos a través de la web. Los cortafuegos y los programas antivirus ayudaron a protegerse contra esto, pero la red era en su mayor parte no segura y rápidamente floreciente.

2000: el cibercrimen se trata como un crimen

Si bien los gobiernos habían perseguido a los ciberdelincuentes durante décadas, la mayoría de los castigos eran leves, a menudo se limitaban a la confiscación de equipos informáticos y a la prohibición del uso de computadoras durante un período de tiempo determinado. Esto cambió en la década de 2000, cuando los gobiernos comenzaron a reconocer los peligros de la piratería. Los hackers fueron encarcelados durante años como castigo por la actividad del ciberdelincuente. Jeanson James Ancheta, por ejemplo, quien usó la piratería informática para robar menos de una millonésima parte de la cantidad que "los 414s" robaron, fue

sentenciado a cinco años de cárcel. Para 2010, los hackers de alto perfil estaban recibiendo décadas de prisión por delitos informáticos.

2010: la seguridad de la información se vuelve seria

Aunque los enjuiciamientos criminales, los firewalls y el software antivirus habían servido como elementos de disuasión para los ciberdelincuentes, no detuvieron a los piratas informáticos que tenían la habilidad y la audacia suficientes para entrar en las redes informáticas. En este punto de la historia de la seguridad de la información, los expertos en seguridad comenzaron a darse cuenta de que la mejor forma de proteger los datos era hacerlos verdaderamente inaccesibles para los piratas informáticos. Con este fin, el cifrado de datos, que codifica los datos para hacerlos ilegibles para los usuarios no autorizados, se generalizó. En muchos casos, el cifrado se produce en múltiples niveles, incluso en archivos digitales, redes y durante transmisiones de datos. Las organizaciones ahora también implementan políticas integrales de seguridad de la información que evitan que sus empleados cometan errores que hagan que los datos sean accesibles para los intrusos. (Lynett, 2015)"

6.3.2 Historia del software libre:

"El sistema operativo GNU es un sistema completo de software libre compatible con Unix. El término GNU proviene de «GNU No es Unix». Se pronuncia en una sola sílaba: ñu **Richard Stallman** escribió el anuncio inicial del Proyecto GNU en setiembre de 1983. Una versión extendida, denominada el Manifiesto de GNU, se publicó en setiembre de 1985. Se ha traducido a diversos idiomas.

El nombre «GNU» se eligió porque satisfacía unos cuantos requisitos. En primer lugar, era un acrónimo recursivo para «GNU No es Unix». En segundo lugar, era una palabra real. Por último, era divertido de decir (o cantar).

La palabra «libre» en «software libre» se refiere a libertad, no a precio [1]. Se puede o no pagar un precio por obtener software de GNU. De cualquier manera, una vez que se obtiene el software, se tienen cuatro libertades específicas para usarlo: La libertad de ejecutar el programa como se desee; la libertad de copiar el programa y dárselo a amigos o compañeros de trabajo; la libertad de cambiar el programa como se desee mediante el acceso completo al código fuente; la libertad de distribuir una versión mejorada, ayudando así a construir la comunidad (si se redistribuye software de GNU, se puede cobrar una tarifa por el acto físico de efectuar la copia, o bien regalar copias).

El proyecto para desarrollar el sistema GNU se denomina «Proyecto GNU». El Proyecto GNU se concibió en 1983 como un modo de retomar el espíritu cooperativo que prevalecía en la comunidad informática en sus comienzos, posibilitar la cooperación eliminando los obstáculos impuestos por los dueños de software privativo.

En 1971, cuando comenzó su carrera en el MIT, Richard Stallman formaba parte de un grupo de trabajo que usaba exclusivamente software libre. Incluso las compañías informáticas distribuían con frecuencia software libre. Los programadores eran libres de cooperar unos con otros y lo hacían a menudo.

Al inicio de los años ochenta casi todo el software era privativo, lo que significa que tenía dueños que prohibían e impedían la cooperación entre usuarios. De ahí que fuera necesario el Proyecto GNU.

Todo usuario de ordenadores necesita un sistema operativo. Si no existe un sistema operativo libre, ni siquiera se puede comenzar a usar un ordenador sin recurrir al software privativo. Así, el primer elemento en la agenda del software libre tenía que ser un sistema operativo libre.

Decidimos hacer el sistema operativo compatible con Unix porque el diseño en general ya estaba probado y era portable, y porque la compatibilidad facilitaba a los usuarios de Unix el cambio de Unix a GNU.

Un sistema operativo similar a Unix incluye un núcleo, compiladores, editores, procesadores de texto, software de correo, interfaces gráficas, bibliotecas, juegos y muchas otras cosas. Por todo esto, escribir un sistema operativo completo conlleva mucho trabajo. La Free Software Foundation se fundó en octubre de 1985 con el objetivo inicial de recaudar fondos para ayudar a programar GNU.

A principios de 1990 ya habíamos encontrado o programado los componentes principales excepto uno, el núcleo. En 1991 Linus Torvalds programó Linux, un núcleo similar a Unix, y en 1992 lo convirtió en software libre. La combinación de Linux con el sistema GNU, que ya estaba prácticamente completo, formó un sistema operativo completo: el sistema GNU/Linux. Se estima que existen decenas de millones de personas que en la actualidad usan sistemas GNU/Linux, habitualmente mediante distribuciones de GNU/Linux. La versión principal de Linux actualmente contiene elementos binarios de firmware que no son

libres, por eso partidarios del software libre mantienen una versión modificada libre de Linux denominada Linux-libre.

En todo caso, el proyecto GNU no se limita al sistema operativo propiamente dicho. Queremos proporcionar una amplia gama de software, cualquier programa que muchos usuarios quieran tener. Esto incluye programas de aplicación. En el directorio de software libre se puede consultar un catálogo de aplicaciones libres.

También queremos proporcionar software para usuarios que no son expertos en informática. Por ese motivo creamos un escritorio gráfico (llamado GNOME) para ayudar a los principiantes a usar el sistema GNU.

También queremos ofrecer juegos y otros programas de entretenimiento. Algunos juegos libres ya están disponibles.

¿Hasta dónde puede llegar el software libre? No hay límites, excepto cuando leyes como el sistema de patentes prohíben el software libre. El objetivo final es el de proporcionar software libre para realizar todas las tareas que los usuarios de ordenadores quieran llevar a cabo, y lograr así que el software privativo sea cosa del pasado. (www.gnu.org, 2001)”

7. Cronograma de actividades

TIEMPO / Actividades	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5
1. ANALISIS					
Revisar las maquinas del alcance	**x**				
2. **Diseño**					
Diseñar los controles de seguridad necesarios		**x**			
3. Implementación					
Mitigar mediante parche, actualización o configuración las vulnerabilidades			**x**		
Implementar correlacionador de registros				**x**	**x**

Tabla 1: Cronograma de actividades

8. Conclusiones

De la decena aproximada de servidores su distribución de vulnerabilidades es:

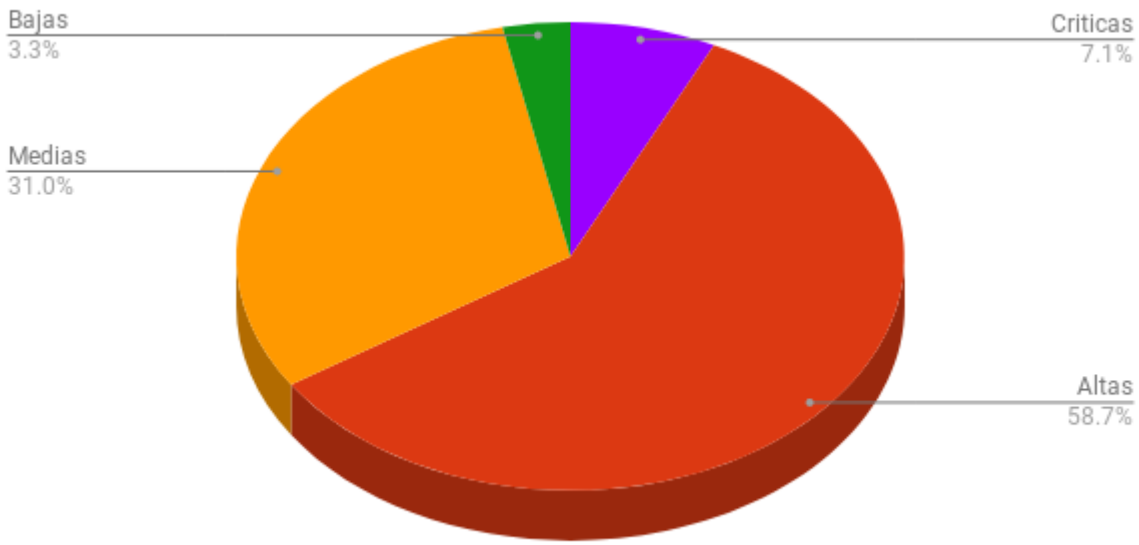


Imagen 3: Gráfico porcentual de vulnerabilidades

Luego de divulgar las vulnerabilidades al administrador de los sistemas de la Corhuila, se procedió a documentar las soluciones y medidas que se deben tomar para reducir estas estadísticas de riesgo.

Las medidas básicamente consisten en

- reducir el área expuesta, desinstalando servicios vulnerables que no se necesiten mantener en funcionamiento.
- migrar o actualizar los servicios, sistemas y aplicaciones vulnerables.
- aplicar parches a los sistemas, servicios y aplicaciones vulnerables.

- restringir el acceso mediante controles de acceso lógico a la red afectada con el sistema vulnerable (aislamiento y bloqueo por firewall).

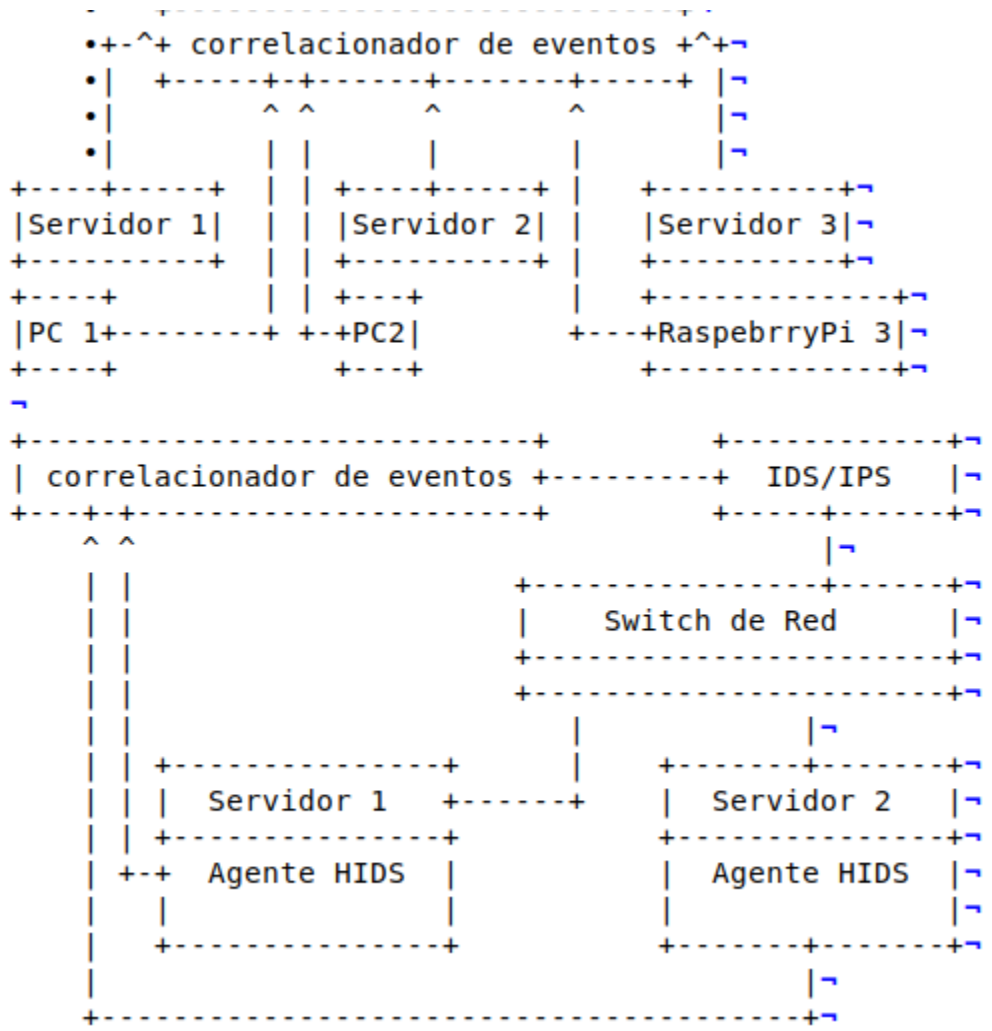
La jerarquía de estas medidas está diseñada para combinar funcionalidad con seguridad empezando de arriba a abajo.

La información de las vulnerabilidades y sus mitigaciones es manejada por el administrador del sistema, para cuyo caso quien quiera leerlos deberá diligenciar el área TIC de la Corporación Universitaria del Huila - CORHUILA los permisos a la para tener acceso a esa data sensible.

los controles por implementarse se basarían en la instalación de un correlacionador de eventos de seguridad basado en software libre “logstash, kibana y elasticsearch (Elastic, 2018)”

El sistema de correlación de eventos será alimentado con por los sistemas operativos, sus servicios y aplicaciones, gracias a sistemas como syslog, rsyslog y netflow.

Por último se recomendara el uso raspberry pi 3 modelo B como sensores de red de un sistema de detección de intrusos SNORT que también alimentarán el sistema de correlación de registros (Raspberry).



De acuerdo con el plan se realizaron las actividades de análisis y diseño, lamentablemente no se pudo realizar la etapa de implementación debido a que actualmente la corporación universitaria del Huila CORHUILA no podrá por motivos ajenos lo que este proyecto tiene permitido revela, instalar “el correlacionador de eventos de seguridad”.

1- se concluye que el administrador luego de seguir las instrucciones de mitigación reduciría la cantidad de vulnerabilidades a solo 5 bajas, reduciendo el riesgo cerca a (97%).

2- se concluye que los sistemas informáticos de la Corhuila tienen sistemas de separación lógica de redes robustos.

3- se concluye que es posible hacer un análisis de vulnerabilidades completamente con herramientas de software libre (nmap, openvas).

4- se concluye que las vulnerabilidades presentadas, el 90% de las vulnerabilidades obedecen a fallas en la actualización de los sistemas utilizados por parte de la Corhuila.

5- se concluye la corporación universitaria del Huila CORHUILA, podrá concluir la implementación con el anexo en este proyecto de un manual de instalación correlacionador de eventos de seguridad.

9. Bibliografía y webiografía

Andress, J. (2011). *The basic of information security second edition.* Oxford: Elsevier.

CPTE. (s.f.). *box.com.* Obtenido de box.com: https://app.box.com/embed/preview/d3bwuo3154z1bphlwxencyejexc9zhrv

Dr.dobb's. (05 de 03 de 2007). *SIEM: A Market Snapshot - Dr.dobb's Journal*. Obtenido de http://www.drdobbs.com/siem-a-market-snapshot/197002909

DSIT, D. d. (06 de marzo de 2016). *www.rcnradio.com.* Obtenido de www.rcnradio.com: https://www.rcnradio.com/tecnologia/hackers-atacan-sitio-web-la-universidad-los-andes

EL CONGRESO DE COLOMBIA. (2012). *Presidencia de la Republica de Colombia.* Obtenido de http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

El Tiempo. (06 de 10 de 2016). *El Tiempo*. Obtenido de https://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232

Elastic. (2018). *www.elastic.co*. Obtenido de www.elastic.co: https://www.elastic.co/elk-stack

entertaiment, S. P. (08 de Diciembre de 2014). Caso SONY Pictures. *SPE.* Culver city, California, EE.UU.

Federal Financial Institutions Examination Council's (FFIEC). (21 de 03 de 2010). *(FFIEC) website*. Obtenido de https://web.archive.org/web/20100221082829/http://www.ffiec.gov/ffiecinfobase/booklets/retail/retail_03b.html

Forbes. (2017). *forbesinsights.* Obtenido de Forbes: http://media.cms.bmc.com/documents/Forbes_Insights_SecOps_Survey.pdf

Goodin, D. (08 de 10 de 2018). *arstechnica*. Obtenido de https://arstechnica.com/tech-policy/2018/10/google-exposed-non-public-data-for-500k-users-then-kept-it-quiet/

ISO International Organization for Standardization. (2018). *ISO 31000 Risk management.*

Iso.Org. (s.f.). *iso.org.* Obtenido de iso.org: http://standards.iso.org/ittf/PubliclyAvailableStandards/

Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. (2011). *Metasploit, The Penetration Tester's Guide.* No Starch Press.

Kosutic, D. (2013). *advisera.com.* Obtenido de advisera.com: https://advisera.com/27001academy/es/knowledgebase/resumen-del-anexo-a-de-la-norma-iso-270012013/

Lynett, M. (25 de Noviembre de 2015). *blog.mesltd.ca.* Obtenido de blog.mesltd.ca: https://blog.mesltd.ca/a-history-of-information-security-from-past-to-present

McQuitty, M. W. (2013). Circumventing Traditional Markets: An Empirical Study of the. En *Journal of Marketing Theory and Practice, vol. 21, no. 2* (págs. 195-205). sharpe.

MEDINA, É. (27 de Enero de 2016). En 2015, cibercrimen generó pérdidas por US$ 600 millones en Colombia . *En 2015, cibercrimen generó pérdidas por US$ 600 millones en Colombia* .

Morgan, S. (2018). *Top 5 cybersecurity facts, figures and statistics for 2018*. Obtenido de www.csoonline.com: https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

OpenVas. (2009). *www.openvas.org*. Obtenido de www.openvas.org: http://www.openvas.org/about.html

PTES. (2009). *pentest-standard.org.* Obtenido de pentest-standard.org: http://www.pentest-standard.org/index.php/FAQ

Quick, M., Hollowood, E., & Miles, C. (2018). *World's Biggest Data Breaches*. Obtenido de informationisbeautiful.net: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Raspberry. (s.f.). *www.raspberrypi.org*. Obtenido de www.raspberrypi.org: https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/

Richmond, R. (02 de abril de 2011). The RSA Hack: How they did it. *The New York times*, págs. https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/.

Riesgo, a. y. (s.f.). *epn.gov.co.* Obtenido de epn.gov.co: http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_riesgo_amenaza_y_vulnerabilidad.html

Romagn, M., & Van Ven Hout, N. (2017). HACKTIVISM AND WEBSITE DEFACEMENT: MOTIVATIONS, CAPABILITIES AND POTENTIAL THREATS. *HACKTIVISM AND WEBSITE DEFACEMENT: MOTIVATIONS, CAPABILITIES AND POTENTIAL THREATS* (pág. 11). La Haya: The Hague University of Applied Sciences, The Netherlands.

Satllman, R. M. (Marzo de 2015). *www.gnu.org.* Obtenido de www.gnu.org: https://www.gnu.org/philosophy/free-hardware-designs.en.html

Shirey, R. (mayo de 2000). *ietf.org.* Obtenido de ietf.org: https://tools.ietf.org/html/rfc2828

Statt, N. (28 de 09 de 2018). *The Verge*. Obtenido de https://www.theverge.com/2018/9/28/17916076/facebook-hack-lawsuit-login-info-50-million-users-affected

Vargas, J. O. (2016). *DISEÑO E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, RED Y VIRTUALIZACIÓN APOYADAS CON SOFTWARE LIBRE EN LA COMPAÑÍA TECNOLOGÍA Y REDES S.A.S.* Bogotá.

Velásquez, A. M. (21 de 08 de 2018). *El Tiempo*. Obtenido de https://www.eltiempo.com/tecnosfera/dispositivos/cibercriminales-manipulan-a-su-victimas-con-informacion-de-estas-y-exigen-un-millonario-pago-258062

Wong, J. C. (2018). *The Guardian*. Obtenido de https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach

www.gnu.org. (24 de abril de 2001). Obtenido de www.gnu.org: https://www.gnu.org/philosophy/free-sw.html

10. Anexos

10.1 Entrevista con jefe de TIC CORHUILA

Entrevista al Administrador de los sistemas y Jefe Tecnologías de la Información y las Comunicaciones Hernán Giovanni Segura de la Corporación universitaria del Huila CORHUILA, las preguntas y sus respectivas respuestas fueron:

1. ¿la corporación universitaria del Huila cuenta con una infraestructura tecnológica propia (servidores y redes) o alquila plataformas y servicios tecnológicos a terceros?

   Respuesta: ambos, tiene servidores y redes para sostener los sistemas contables, de recursos humanos y académicos. Pero también se tiene contratada la página web con un CMS y un hosting externo.

2. ¿La infraestructura tecnológica contratada a externos tiene controles de seguridad?

   Respuesta: El sitio cuenta con un certificado TLS y un balanceador de carga por parte del proveedor.

3. ¿La infraestructura tecnológica propia tiene controles de seguridad?

   Respuesta: Si, tenemos un firewall pfsense, está configurado para mantener seguras y aisladas las redes y los servidores de la corporación universitaria del Huila CORHUILA.

4. ¿En su opinión profesional cree que los controles de seguridad implementados son suficientes para mitigar todos los posibles riesgos inherentes a este tipo de infraestructura?

   Respuesta: No, creo que se deba implementar otros más.

5. ¿Cuáles controles de seguridad tiene planeados implementar?

   Respuesta: Se planeaba implementar firewalls con capacidad ips de fortinet asi como también un correlacionador de registros del mismo fabricante.

6. ¿Por qué no se han implementado estos controles aun?

   Respuesta: En la fase de estudio y cotización se encontró que el presupuesto necesario para implementación excede el presupuesto destinado al departamento de tecnología.

7. ¿Ha buscado otras opciones para implementar controles de seguridad?

   Respuesta: Si. pero lamentablemente otros fabricantes tienden a solicitar mucho más presupuesto que fortinet.

8. ¿Cuál es su opinión del software libre?

   Respuesta: Me parece una corriente de licenciamiento de software muy interesante, ya he administrado muchos sistemas tipo unix como linux y los he encontrado

eficientes, el problema con estos sistemas es el soporte ya que muchos son sustentados solo por una comunidad, pero en un entorno corporativo prefiero distribuciones bien soportadas por amplias compañías como Redhat o Suse.

9. ¿Estaría dispuesto a probar software libre en los controles de seguridad?

   Respuesta: Si, pero no tengo la experiencia necesaria para emprender dicho proyecto.

10. ¿En su opinión cree que tiene los conocimientos necesarios para implementar dichos controles usted mismo?

    Respuesta: No tengo conocimientos avanzados, pero me gustaría aprender más.

11. ¿Le gustaría tener un análisis del estado actual de la infraestructura, así como las recomendaciones para implementar los controles necesarios en software libre?

    Respuesta: Si, eso me ayudaría para mejorar la seguridad de la infraestructura sin recurrir a grandes presupuestos.

10.2 Como Instalar ELK

En este tutorial vamos a repasar cómo es posible instalar y configurar ELK, en sistema debian 9, ELK es una agrupación de software open-source conformado por:

- Elasticsearch (Servidor de búsqueda y análisis RESTfull de Bases de datos NoSQL).
- Logstash (Servicio de procesamiento de logs y eventos mediante información entre pipelines).
- Kibana (Aplicación web para visualizar la información que provee Elasticsearch).

ELK en debian 9 es muy fácil de instalar en sistema debian, seguiremos los siguientes pasos:

1. Requerimientos.

Para completar este tutorial se necesita:

- Un Sistema Debian 9.
- Un usuario con privilegios de administrador (sudo o root)

2. Actualizar el sistema e instalar paquetes necesarios.

Ejecutaremos en este caso los siguientes comandos:

```
sudo apt-get update && apt-get -y upgrade
sudo apt-get install apt-transport-https software-properties-common wget
```

Se recomienda siempre tener el sistema debian 9 al día con las actualizaciones de seguridad y tener activado un sistema de actualizaciones automáticas.

3. Instalar Java.

Elasticsearch requiere al menos de Java 8, para eso instalaremos el paquete OpenJDK pero también es compatible con Oracle Java.

Para instalar OpenJDK ejecutaremos el siguiente comando:

```
sudo apt install openjdk-8-jdk
```

Para revisar la versión instalada y verificar que no hay problemas:

java -version

deberás ver algo similar a:

openjdk version "1.8.0_171"
OpenJDK Runtime Environment (build 1.8.0_171-8u171-b11-1~deb9u1-b11)
OpenJDK 64-Bit Server VM (build 25.171-b11, mixed mode)

4. Instalar y configurar Elasticsearch :

   Para poder instalar el repositorio que nos proveerá Elasticsearch, ejecutaremos los siguientes comandos:

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-6.x.list
sudo apt-get update

Luego de lo anterior podremos proceder a instalar Elasticsearch:

sudo apt-get install elasticsearch

Una vez terminada la instalación, debemos editar el archivo elasticsearch.yml para restringir y configurar el acceso a las instancias de Elasticsearch.

sudo nano /etc/elasticsearch/elasticsearch.yml

```
# ---------------------------------- Network -----------------------------------
#
# Set the bind address to a specific IP (IPv4 or IPv6):
#
#network.host: 192.168.0.1
network.host: localhost
```

Reiniciamos el servicio Elasticsearch y configuramos que el servicio inicie con en encendido del sistema:

sudo systemctl restart elasticsearch
sudo systemctl enable elasticsearch

Para verificar el funcionamiento de Elasticsearch podemos ejecutar una petición al servicio:

curl -X GET http://localhost:9200

Debería mostrar un resultado similar a:

```
{
  "name" : "UHR2XBB",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "Ranc0Jh9QAuuMYhALcZIRA",
  "version" : {
    "number" : "6.2.4",
```

```
    "build_hash" : "ccec39f",
    "build_date" : "2018-04-12T20:37:28.497551Z",
    "build_snapshot" : false,
    "lucene_version" : "7.2.1",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
```


5. Instalación y configuración de Kibana:

Al igual que Elasticsearch, ya teniendo el repositorio activo solo es necesario ejecutar:

sudo apt-get install kibana

Una vez terminada la instalación debemos editar el archivo kibana.yml para restringir el acceso a la instancia de Kibana :

sudo nano /etc/kibana/kibana.yml

```
# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "localhost"
```

Iniciaremos el servicio y lo configuraremos para iniciar en cada encendido:

```
sudo systemctl restart kibana
sudo systemctl enable kibana
```

Kibana correrá ahora en adelante en el puerto 5601 en localhost

6. Instalar y configurar Nginx como proxy reverso:

Usaremos Nginx como proxy reverso para acceder a kibana, para instalarlo simplemente ejecutaremos:

sudo apt-get install nginx

Crearemos un archivo de autenticación básica para el nginx con openssl:

```
echo "admin:$(openssl passwd -apr1 ContraseñaMUY_FUERTE)" | sudo tee -a /etc/nginx/htpasswd.kibana
```

Note: no olvides usar una contraseña fuerte (mínimo 16 caracteres con símbolos, números, mayúsculas y minúsculas)

Borra el perfil por defecto de host virutal de Nginx:

```
sudo rm -f /etc/nginx/sites-enabled/default
```

y crea un perfil de host virtual para la instancia de Kibana:

```
sudo nano /etc/nginx/sites-available/kibana
```

```
server {
    listen 80 default_server;
    server_name _;
    return 301 https://$server_name$request_uri;
}

server {
    listen 443 default_server ssl http2;

    server_name _;

    ssl_certificate /etc/ssl/certs/ssl-cert-snakeoil.pem;
    ssl_certificate_key /etc/ssl/private/ssl-cert-snakeoil.key;
    ssl_session_cache shared:SSL:10m;

    auth_basic "Restricted Access";
    auth_basic_user_file /etc/nginx/htpasswd.kibana;

    location / {
        proxy_pass http://localhost:5601;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
    }
}
```

Activa el perfil de host virtual mediante la creación de un enlace simbolico:

```
sudo ln -s /etc/nginx/sites-available/kibana /etc/nginx/sites-enabled/kibana
```

Prueba la configuración de Nginx:

```
sudo nginx -t
```

Reiniciaremos el servicio Nginx y configuraremos su inicio en los siguientes encendidos:

```
sudo systemctl restart nginx
sudo systemctl enable nginx
```

7. Instlación Logstash:

El paso final será la instalación de Logstash, igual que los servicios anteriores por tener activados los repositorios necesarios para la tarea es simplemente ejecutar:

sudo apt-get install logstash

Una vez terminada la instalación de Logstash podremos reiniciarlo y configurarlo para su ejecucion en cada encendido de sistema:

sudo systemctl restart logstash
sudo systemctl enable logstash

La configuración de Logstash ya depende de que plugins y propósitos este pensada su implantación, hay plugins para snort, modsecurity , etc ...

8. Acceder a Kibana:

Ahora ya puedes acceder con la contraseña **FUERTE** mediante el navegador usando la dirección: https://ipservidor

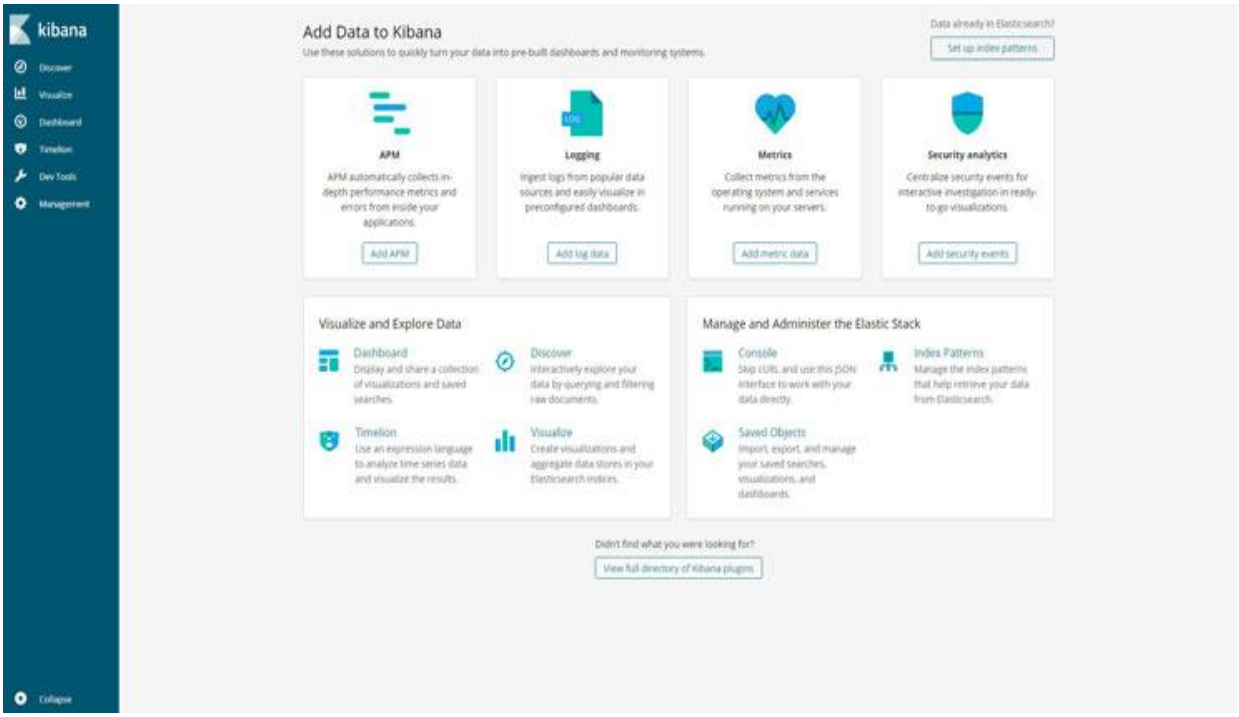


Imagen 4: Acceso a Kibana

También es posible instalarlo en otros sistemas, como windows server o otras distribuciones linux los instaladores podrán ser encontrados en https://goo.gl/n9KMNH o en https://goo.gl/goKtLY

Autor del tutorial: Alex Ricardo Rincon Silva @nemesis545 nemesis@nemesis545.net