

Facultad De Ingeniería

Ingeniería en Computación e Informática

**Propuesta de Infraestructura de bajo costo para la DETECCIÓN DE ANOMALÍAS Y ATAQUES EN UNA RED CORPORATIVA de micro y pequeñas empresas**

Proyecto de título para optar al título de

Ingeniero en computación e informática

Autor:

Jonathan Armijo

Profesor Guía:

Romina Torres

VIÑA DEL MAR, CHILE

2020

**Resumen**

Actualmente empresas en general están siendo comprometidas por Ciberdelincuentes, los cuales en su afán de conseguir principalmente un beneficio económico, cometen ciberdelitos.

Los ciberataques unidos a una escasa adopción de medidas de seguridad, han propiciado la aparición de brechas de seguridad relacionadas por ejemplo con información personal, información de estados, datos bancarios, entre otros. Uno de los mayores incidentes de robo de datos personales tuvo lugar en la India, donde la base de datos de identificación del gobierno, Aadhaar, sufrió múltiples incidentes de seguridad que comprometieron los datos de 1.100 millones de ciudadanos registrados.

Existen herramientas costosas para poder proteger, donde a pesar de igual forma es necesario invertir en recursos humanos, lo importante es que esta inversión se vea reflejada en el producto final, en la mitigación de un incidente informático y en las medidas que se tomaron a nivel Gerencial.

Las pequeñas y medianas empresas en Chile, no cuentan con el presupuesto necesario para poder destinar parte de su capital a Seguridad TI, siendo que ellas de igual forma podrían verse afectadas por algún incidente informático, es por eso que se hace presente lograr llegar a una solución de bajo costo y que cumpla con el objetivo de protección.

Esta tesis busca proponer una solución a esta problemática construyendo una herramienta tecnológica que permita entre otras cosas entregar información vital y procesada, con el objeto de que el o los encargados de Seguridad TI del lugar donde se implemente este sistema tengan una visión general de como se encuentra la red y puedan tener las herramientas necesarias para mitigar un posible incidente informático.

La infraestructura que se presenta y con la cual se detectarán ataques informáticos dentro de la red, esta compuesta por:

1. Correlacionador de eventos Open Source (Graylog).
2. Cortafuegos Open Source (pfSense).
3. Servidor de correo Open Source (Postfix - Dovecot).
4. Servidor DNS (Bind).
5. Herramienta generadora de ataques.
6. Modulo de detección y categorización de ataques.

# **Introducción**

# **1.1 Introducción**

Hoy en día en Chile y el mundo se hace imprescindible el contar con herramientas y sistemas de Tecnologías de la Información (TI) que simplifiquen, optimicen, depuren y agilicen, ya sea procesos industriales a gran y a pequeña escala. Como es de conocimiento público, todo cambio produce un quiebre o brecha en lo que ya se encuentra implementado, de modo que estos posibles incidentes se mitiguen o no existan.

Cuando hablamos de un Ciberataque, nos referimos a la acción ofensiva que se lleva a cabo sobre determinados sistemas informáticos de una empresa, entidad o persona, comúnmente estos ataques buscan o tienen por objetivo tomar el control de un equipo(s), también la desestabilización de los sistemas informáticos o el robo de datos. Normalmente las personas que realizan este tipo de ataques son denominados como “Ciberdelincuentes”.

Cuando hablamos de una amenaza del tipo Ransomware, nos referimos a grandes rasgos a un Malware que busca secuestrar nuestro equipo y cifrar todo lo que corresponde a ofimática, para posteriormente solicitar un rescate a través del pago de dinero.

En mayo del año 2017, se produjo un ciberataque a escala mundial mediante una combinación de ataque de un gusano, procedente del código filtrado por Shadow Brokers (Grupo de Hackers) del exploit EternalBlue desarrollado por la NSA, junto con un Ransomware denominado WannaCry. El ataque se desplegó de forma simultánea y a nivel global, afectando a más de 300.000 máquinas en 150 países.

<https://www.xataka.com/seguridad/wannacry-un-ano-despues>

Los daños causados por este ataque, en parte, fueron causados por la falta de información oportuna que permitiera a los encargados de Seguridad TI de cada entidad tomar decisiones y acciones correctas como medidas de mitigación y contingencia.

Aunque actualmente Chile cuenta con entidades que están preocupadas y trabajando con el objetivo de detectar y mitigar este tipo de ataques, se hace necesario que cada organismo cuente con herramientas que le permitan visualizar, monitorear y mitigar acciones adversarias hostiles.

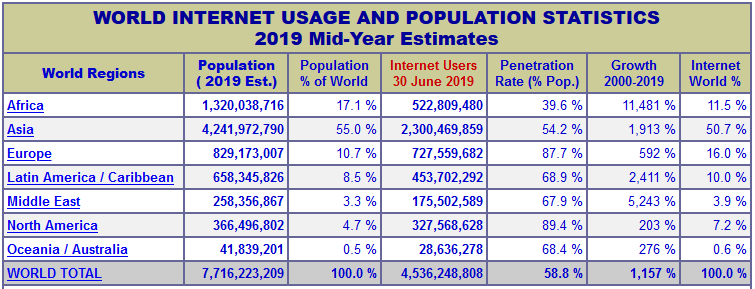
Es por esto que se propone un sistema que permita:

1. Visualizar tráfico de forma centralizada que se encuentra circulando en la red, a través de paneles de control adaptables.
2. Detectar incidentes que afecten a la Seguridad TI de la red donde se despliegue el sistema.
3. Generar informes bajo demanda, los cuales permitan una mejor toma decisiones.

# **1.2 Contexto**

A mediados del presente año el número de usuarios de internet a nivel mundial sobrepasa los cuatro mil quinientos millones de personas, sobre un universo estimado de más de siete mil quinientos millones de habitantes. En pocas palabras casi el 59% de la población mundial utilizan internet.

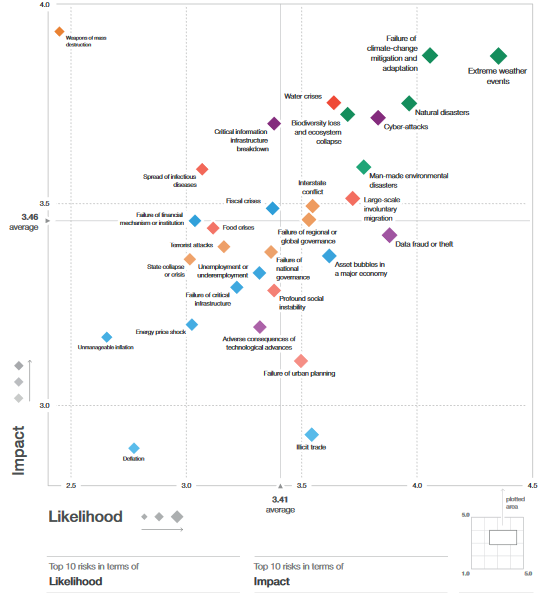
La ilustración N° 1 muestra el desglose de los usuarios mundiales de internet atendiendo a su ubicación geográfica.



**Ilustración N° 1: “World internet usage and population statistics 2019”**

Fuente: https://www.internetworldstats.com/stats.htm

A continuación el World Economic Fórum (WEF) ubica a los ciberataques entre los riesgos globales más significativos, como muestra la siguiente figura:



**Ilustración 2: World Economic Forum**

http://www3.weforum.org/docs/WEF\_Global\_Risks\_Report\_2019.pdf

Actualmente la tecnología sigue ocupando un papel importante en la configuración del panorama de riesgos globales para los individuos, los gobiernos y las empresas. En el informe citado anteriormente, el "fraude y robo masivo de datos" fue clasificado como el cuarto riesgo más importante a nivel mundial, de acuerdo al “The Global Risks Report 2019 14th Edition” en un periodo de 10 años, situando los "ciberataques" en la quinta posición, lo que mantiene el patrón del año 2018. A pesar de todo esto, la mayoría de las personas hoy en día estiman un crecimiento de los riesgos de ciberataques en el 2020, especialmente en lo relativo a la sustracción de dinero y/o datos (82%) y la interrupción de las operaciones (80%). A su vez se debe considerar la aparición de nuevas fuentes de inestabilidad a medida que se incrementa la penetración de las tecnologías digitales en la vida cotidiana. Gran parte de las personas hoy en día esperan que los riesgos asociados a las noticias falsas y el robo de identidad aumenten en el 2020, mientras que un grupo no menor de personas auguran lo mismo en relación con la pérdida de privacidad.

A principios de este año 2019 se detectó que los delincuentes estaban vendiendo el acceso a la base de datos, asociada a información biométrica y personal. En este ultimo tiempo India ha escaneado el iris y la huella dactilar de los residentes en el país como parte de la iniciativa Aadhaar, el mayor proyecto biométrico del planeta, con el fin de identificarlos para que tengan acceso a la red de la seguridad social y a otros servicios, a un precio de 500 rupias cada 10 minutos. En marzo de este mismo año, una brecha de seguridad de una empresa estatal de servicios públicos permitía el acceso indiscriminado a nombres y números de identificación, fueron alrededor de 1.000 millones de ciudadanos indios afectados.

Ref. <https://www.pandasecurity.com/spain/mediacenter/noticias/india-robo-datos/>

En otros lugares del planeta, las violaciones de datos personales afectaron a 150 millones de usuarios de la aplicación MyFitnessPal4 y a alrededor de 50 millones de usuarios de Facebook. Esto comprometió efectivamente los datos personales de estos usuarios, los cuales vieron vulnerados su seguridad personal por acción o no acción de terceros.

Como se ha mostrado en años anteriores, las vulnerabilidades pueden provenir de orígenes absolutamente inesperados. Así lo evidenciaron, entre otras, las amenazas Meltdowny Spectre, que pusieron de manifiesto graves debilidades en el hardware, en lugar de en el software, como venía siendo lo habitual.

El año pasado también fuimos testigos de ciberataques dirigidos a las infraestructuras críticas, de acuerdo a lo expuesto en <https://www.fayerwayer.com/2019/11/infraestructuras-criticas-pais-ataques/>, lo cual nos muestra un gran vector de ataque, del los cual los ataques están sacando provecho.

Las potenciales vulnerabilidades tecnológicas se han convertido en un gran problema a nivel mundial.

A continuación se detallará la taxonomía de las principales vulnerabilidades y ataques presentes hoy en día.

**Taxonomía de Vulnerabilidades y Ataques**

La taxonomía empleada se basa en la Taxonomía de Referencia para la Clasificación de Incidentes de Seguridad, desarrollada coordinadamente por un grupo internacional de equipos de respuesta a incidentes.

1. **Contenido abusivo**
   * **SPAM**: Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
   * **Delito de odio**: Contenido difamatorio o discriminatorio. Ejemplos: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
   * **Pornografía infantil, contenido sexual o violento inadecuado**: Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
2. **Contenido dañino**
   * **Sistema infectado**: Sistema infectado con malware. Ejemplo: sistema, computadora o teléfono móvil infectado con un rootkit.
   * **Servidor C&C (Mando y Control)**: Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
   * **Distribución de malware**: Recurso usado para distribución de malware. Ejemplo: recurso de una organización empleado para distribuir malware.
   * **Configuración de malware**: Recurso que aloje ficheros de configuración de malware. Ejemplo: ataque de inyección de código malicioso a través de la web.
   * **Malware dominio DGA**: Nombre de dominio generado mediante DGA (Algoritmo de Generación de Dominio), empleado por malware para contactar con un servidor de Mando y Control (C&C).
3. **Obtención de información**
   * **Escaneo de redes (scanning)**: Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ejemplos: peticiones DNS, ICMP, SMTP, escaneo de puertos.
   * **Análisis de paquetes (sniffing)**: Observación y grabación del tráfico de redes.
   * **Ingeniería social**: Recopilación de información personal sin el uso de la tecnología. Ejemplos: mentiras, trucos, sobornos, amenazas.
4. **Intento de intrusión**
   * **Explotación de vulnerabilidades conocidas**: Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado. Ejemplos: desbordamiento de buffer, puertas traseras, Cross Site Scripting (XSS).
   * **Intento de acceso con vulneración de credenciales**: Múltiples intentos de vulnerar credenciales. Ejemplos: intentos de ruptura de contraseñas, ataque por fuerza bruta.
   * **Ataque desconocido**: Ataque empleando exploit desconocido.
5. **Intrusión**
   * **Compromiso de cuenta con privilegios**: Compromiso de un sistema en el que el atacante ha adquirido privilegios.
   * **Compromiso de cuenta sin privilegios**: Compromiso de un sistema empleando cuentas sin privilegios.
   * **Compromiso de aplicaciones**: Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ejemplo: inyección SQL.
   * **Robo**: Intrusión física. Ejemplo: acceso no autorizado a Centro de Proceso de Datos y sustracción de equipo.
6. **Disponibilidad**
   * **DoS (Denegación de Servicio)**: Ataque de Denegación de Servicio. Ejemplo: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
   * **DDoS (Denegación Distribuida de Servicio)**: Ataque de Denegación Distribuida de Servicio. Ejemplos: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
   * **Sabotaje**: Sabotaje físico. Ejemplos: cortes de cableados de equipos o incendios provocados.
   * **Interrupciones**: Interrupciones por causas externas. Ejemplo: desastre natural.
7. **Compromiso de la información**
   * **Acceso no autorizado a información**: Acceso no autorizado a información. Ejemplos: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
   * **Modificación no autorizada de información**: Modificación no autorizada de información. Ejemplos: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante Ransomware.
   * **Pérdida de datos**: Pérdida de información. Ejemplos: pérdida por fallo de disco duro o robo físico.
8. **Fraude**
   * **Uso no autorizado de recursos**: Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ejemplo: uso de correo electrónico para participar en estafas piramidales.
   * **Derechos de autor**: Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ejemplos: Warez.
   * **Suplantación**: Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
   * **Phishing**: Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
9. **Vulnerable**
   * **Criptografía débil**: Servicios accesibles públicamente que pueden presentar criptografía débil. Ejemplo: servidores web susceptibles de ataques POODLE/FREAK.
   * **Amplificador DDoS**: Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ejemplos: DNS open-resolvers o Servidores NTP con monitorización monlist.
   * **Servicios con acceso potencial no deseado**: Servicios accesibles públicamente potencialmente no deseados. Ejemplos: Telnet, RDP o VNC.
   * **Revelación de información**: Acceso público a servicios en los que potencialmente pueda revelarse información sensible. Ejemplos: SNMP o Redis.
   * **Sistema vulnerable**: Sistema vulnerable. Ejemplos: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
   * **APT**: Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.
   * **Ciberterrorismo**: Uso de redes o sistemas de información con fines de carácter terrorista.
   * **Daños informáticos PIC**: Borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica. Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.
   * **Otros:** Todo aquel incidente que no tenga cabida en ninguna categoría anterior.

Por otra línea tecnológica, la utilización de las técnicas de aprendizaje automático (Machine Learning) o el uso de modelos de Inteligencia Artificial (IA) son, cada vez, más frecuentes y sofisticados, evidenciando un creciente potencial para amplificar los riesgos existentes o la creación de nuevos riesgos; especialmente, cuando el Internet de las Cosas (IoT) es capaz de conectar cientos de millones de dispositivos.

A continuación detallaremos algunos de estos términos mencionados en el parrafo anterior:

1. **Machine Learning (ML):**

Machine Learning es una disciplina científica del ámbito de la Inteligencia Artificial que crea sistemas que aprenden automáticamente. Aprender en este contexto quiere decir identificar patrones complejos en millones de datos. La máquina que realmente aprende es un algoritmo que revisa los datos y es capaz de predecir comportamientos futuros. Automáticamente, también en este contexto, implica que estos sistemas se mejoran de forma autónoma con el tiempo, sin intervención humana. Veamos cómo funciona.

1. **Inteligencia Artificial (IA):**

Es la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano. Una tecnología que todavía nos resulta lejana y misteriosa, pero que desde hace unos años está presente en nuestro día a día a todas horas.

1. **Internet de las Cosas (IoT):**

Es “la interconexión a través de Internet de dispositivos informáticos integrados en objetos cotidianos, lo que les permite enviar y recibir datos”. En otras palabras, IoT conecta tus dispositivos a Internet o a otros aparatos, para que puedan realizar nuevas funciones, como por ejemplo controlar elementos inteligentes de forma remota y recibir alertas y actualizaciones de estado. Se refiere a los miles de millones de dispositivos físicos en todo el mundo que ahora están conectados, recolectando y compartiendo datos.

En una investigación realizada por Brookings, el 32% de los encuestados señaló que considera la IA como una amenaza para la humanidad, frente al 24%,que opinaba en sentido contrario. El año pasado, IBM detectó un código dañino dirigido, basado en técnicas IA, capaz de "ocultar" una amenaza ya conocida “WannaCry”, en una aplicación de videoconferencia, la cual se activaba solamente cuando reconocía el rostro del objetivo.

Es probable que aparezcan novedades del mismo perfil en otros campos, por ejemplo acciones en biología sintética, para utilizar la IA en la creación de nuevos agentes patógenos.

Uno de los Future Shocks para lo que resta del año 2019 y siguientes son las consecuencias de la "computación afectiva", entendida como los modelos de IA capaces de reconocer, responder y manipular las emociones humanas. Entre los impactos más generalizados y perturbadores de la IA de los últimos años, se encuentra su capacidad como mecanismo de ejecución de "cámaras de eco y noticias falsas", un riesgo que se espera que aumente en los próximos años.

La computación afectiva a modo de ejemplo, en variadas películas en las que aparecen robots e inteligencias artificiales con emociones, como por ejemplo ‘I Robot’, ‘2001’, ‘Wall E’, o ‘Eva’. Algunas veces, estos robots emocionales generan problemas inesperados por su comportamiento que, en ciertas circunstancias, es menos predecible de lo que sería el comportamiento de una máquina puramente racional, en otras ocasiones, sin embargo, es el hecho de tener una componente emocional el que permite a los robots actuar de forma razonable. Una de la interrogantes que se trata de aclarar a través de la computación afectiva es, ¿Puede un robot o una maquina tener empatía?.

Como resumen la computación afectiva es la disciplina que estudia cómo crear máquinas que puedan reconocer, interpretar y responder apropiadamente a las emociones humanas.

Fuente: <http://informatica.blogs.uoc.edu/2019/04/01/computacion-afectiva/>

Fuente: <https://www.ccn-cert.cni.es>

Durante el año 2018, diversos equipos de investigación estudiaron el despliegue de 126.000 tweets y descubrieron que aquellos que contenían noticias falsas superaban a aquellos otros que contenían información verdadera, alcanzando la superficie de ataque (las personas) seis veces más rápido. Parece claro que la interacción entre las emociones y la tecnología se convertirá, probablemente, en una fuerza cada vez más disruptiva.

Aunque no ha habido nuevas oleadas de Ransomware, este vector de ámbito global, sigue siendo especialmente peligroso, tal como quedó demostrado en los ataques Petya / NotPetya en la segunda mitad de 2017.

Aquí de acuerdo a lo informado por FireEye, todo parece apuntar a que el vector de infección de esta campaña es la actualización de la suite MeDoc, un software de contabilidad de uso recurrente en compañías ucranianas.

De acuerdo a esto existen fuentes no confirmadas que apuntan a posibles correos de phishing en los que se promovía el actualizar a versiones troyanizadas de este software de contabilidad, como este ejemplo:

Fuente: <https://www.virustotal.com/es/file/fe2e5d0543b4c8769e401ec216d78a5a3547dfd426fd47e097df04a5f7d6d206/analysis/>

Fuente:

<https://www.securityartwork.es/2017/06/28/petya-notpetya-esa-la-cuestion/>

Pese a todo, nuevas familias de Ransomware siguen surgiendo permanentemente (como Bad Rabbiten octubre de 2017). Sea como fuese, el código dañino ha seguido aumentando en 2018, hay más de 800 millones de programas conocidos de este tipo y alrededor de 390 mil nuevas variantes se suman diariamente a esa cifra. En el entorno móvil, ya se contabilizan más de 27 millones de programas de malware, solo para Android. Los métodos de distribución masiva de código dañino también se han desarrollado en los últimos años. Por ejemplo, en 2017, el malware se distribuyó en varias ocasiones (como en el caso de NotPetya) al comprometer los archivos o los servidores de actualización de software comercial.

Además, y pese a ser conocidas, las familias de malware se modifican continuamente, incorporando funcionalidades maliciosas adicionales. Desde septiembre de 2017, el malware Emotet que comenzó su propagación en 2015 como un troyano bancario, ha venido añadiendo módulos para spam, DDoS, espionaje de datos, robo de identidades, detección de sandbox, entre otros, el cual ha sido el vector usado en varios ataques en Europa. Las botnets de IoT continúan evolucionando, aunque las nuevas instancias como Hajimey IoT\_reaper / IoTroop no han sido tan significativas como por ej. Mirai.

Fuente: <https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/>

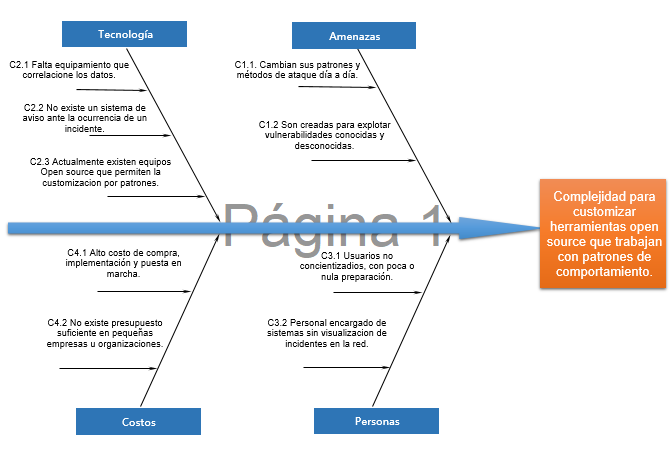
No obstante, es de esperar la aparición de nuevas y grandes botnets que perpetran ataques de alto impacto y todo ello como resultado del rápido crecimiento en el número de móviles y dispositivos IoT vulnerables (características que deben observarse para determinar que un dispositivo es vulnerable). En diciembre de 2017 y principios de 2018, la botnet Andrómeda distribuyó código dañino troyanos bancarios, especialmente en millones de ordenadores de todo el mundo. Como funcionan esos botnet – tratar de explicar a nivel algorítmico su actuar.

**1.3 Definición del problema**

Actualmente en las distintas empresas u organizaciones existen grandes volúmenes de datos que circulan por sus redes sin que exista un control y monitoreo de lo que esta pasando, por ellas, aquí podemos ver desde fuga o robo de información de datos personales y sensibles, datos que podrían tener una alto grado de confidencial y también podríamos encontrarnos con equipos comprometidos con algún Malware ya sea conocido o desconocido (0-day).

Es por esto que actualmente las empresas, instituciones, Pequeñas y Medianas empresas (pymes), organizaciones se encuentran con la necesidad de proteger su información, esto muchas veces lo intentan realizar con herramientas que pueden mitigar una parte de la brecha, pero no la totalidad de esta. Para esto normalmente se utilizan herramientas que permiten la detección de vulnerabilidades y amenazas.

Si debemos tomar en cuenta que estos servicios o herramientas tienen un alto costo para empresas, entidades, etc. que están recién partiendo con la formación de estas, pero que al igual que las empresas que llegan años en el mercado, son demandantes de un nivel mínimo de Seguridad TI. También se debe considerar que muchas de estas herramientas son difíciles de implementar, operar, customizar y mantener; muchas veces este tipo de antecedentes hace que estas empresas pierdan el interés en contar con este tipo de sistemas esta decisión es una muy mala decisión y practica; ya que tarde o temprano se verán envueltos en un incidente de seguridad, que podría perjudicar gravemente a su empresa.



**Ilustración 1: Diagrama Ishikawa**

**Resumen de causas identificadas**

C1 – Las amenazas actuales son cada día mas peligrosas.

C1.1 Debido a que cambian sus patrones y métodos de ataque día a día.

C1.2 Debido a que son creadas para explotar vulnerabilidades conocidas y desconocidas.

C2 – La tecnología no logra detectar las amenazas

C2.1 Debido a la falta de equipamiento para correlacionar los datos.

C2.2 Debido a que no existe un sistema de aviso ante la ocurrencia de un incidente.

C2.3 Actualmente existen equipos Open Source que permiten la customización por patrones.

C3 – Las personas son un blanco de ataque importante.

C3.1 Debido a usuarios no concientizados, con poca o nula preparación.

C3.2 Debido a que el personal encargado de sistemas, no tiene visualización de los incidentes en su red.

C4 – El alto costo de estos sistemas

C4.1 Debido a un alto costo monetario en la compra, implementación y puesta en marcha de los equipos.

C4.2 Debido a que no existe presupuesto suficiente para pequeñas empresas y organizaciones.

# **Objetivo General acorde al problema**

# Disminuir los costos de la infraestructura y personal necesarios para tomar acción y mitigar un incidente informático dentro de una micro y pequeña empresa con bajo presupuesto en esta área.

Los incidentes son:

1. Infección por Malware a través de una descarga de archivo infectado.
2. Que el equipo sea parte de una Botnet y este siendo utilizado para estos fines.
3. Equipo comprometido a través de un correo electrónico malicioso.

Para complementar los incidentes mencionados definiremos algunos términos como, el término malware es una contracción de malicious software (“software malicioso”). En pocas palabras, el malware es un programa que se crea con la intención de dañar dispositivos, robar datos y, en general, causar problemas. Los virus, los troyanos, el spyware y el Ransomware son algunos de los distintos tipos de malware.

El malware lo crean a menudo equipos de hackers que, normalmente, solo intentan conseguir dinero, ya sea extendiendo el malware por su cuenta o vendiéndolo al mejor postor en la “red oscura” (Dark o Deep web). Sin embargo, existen otras razones para crear malware. Se puede utilizar como herramienta de protesta, como un modo de probar la seguridad o incluso como arma de guerra entre gobiernos. A continuación detallaremos algunos tipos de amenazas informáticas, que actualmente rondan en nuestras redes informáticas:

**Malware:**

Es un término muy amplio, y su efecto y modo de funcionamiento varían de un archivo a otro. La siguiente lista describe tipos comunes de malware, aunque existen muchos más:

**Virus:**

Al igual que sus homónimos biológicos, los virus se adhieren a archivos limpios e infectan otros archivos limpios. Pueden propagarse con total descontrol, llegando a dañar las funciones esenciales de un sistema, así como a eliminar o inutilizar archivos. Normalmente, tienen la apariencia de archivos ejecutables (.exe).

**Troyanos:**

Esta clase de malware se hace pasar por software legítimo o se oculta en un programa legítimo que se ha manipulado. Suele actuar de forma discreta y crear puertas traseras en la seguridad para permitir el acceso de otro malware.

**Spyware:**

La finalidad de este malware es, como el propio nombre indica, espiarle. Acecha desde las sombras y va tomando nota de lo que hace en Internet, incluyendo, entre otras cosas, contraseñas, números de tarjetas de crédito y hábitos de navegación.

**Gusanos:**

Los gusanos infectan redes enteras de dispositivos, que pueden ser locales o de Internet, mediante el uso de interfaces de red. Utilizan los equipos infectados para seguir atacando otros equipos.

**Ransomware:**

Esta clase de malware suele bloquear el equipo y sus archivos, y amenaza con borrarlo todo si no se paga un rescate.

**Adware:**

El software publicitario, si bien no es de naturaleza maliciosa, cuando es agresivo puede socavar la seguridad con el único fin de mostrar anuncios, lo cual puede abrir un camino sencillo a otros tipos de malware. Además, para qué negarlo, las ventanas emergentes son verdaderamente molestas.

**Botnets:**

Las botnets son redes de equipos infectados forzados a trabajar en colaboración bajo el mandato de un atacante.

**Como proteger redes informáticas del ataque de un Malware.**

Cuando hablamos de malware, prevenir es mejor que mitigar. Por fortuna, algunos comportamientos sencillos y de sentido común minimizan la posibilidad de toparse con algún software malicioso.

1. No confíe en extraños en Internet, la “Ingeniería Social”, que puede incluir correos electrónicos extraños, alertas repentinas, perfiles falsos y ofertas tentadoras, es el principal método de difusión del malware. Si ve algo que no sabe exactamente qué es, no haga clic.
2. Compruebe dos veces las descargas, tanto en sitios de piratería como en el de tiendas oficiales, el malware suele estar acechando siempre, en espera. Por tanto, antes de descargar algo, compruebe que el proveedor es fiable leyendo con atención las reseñas y comentarios.
3. Obtenga un bloqueador de anuncios, el “malvertising”, el uso por parte de hackers de banners o anuncios emergentes para infectar su dispositivo, está en alza. No es posible saber qué anuncios son peligrosos, así que es más seguro bloquearlos todos mediante un bloqueador de anuncios fiable.
4. Cuidado con las páginas que visita, el malware puede encontrarse en cualquier parte, pero es más frecuente en sitios web con poca seguridad en el servidor, como los sitios web pequeños y locales. Si se limita a los sitios grandes y reputados, reducirá en gran medida el riesgo de encontrarse con malware.

# **1.5 Objetivos Específicos**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Objetivos específicos | Situación actual | Situación esperada | Métrica | Criterio de éxito |
| OE1 | Visualizar comportamientos anómalos de los equipos y usuarios de una determinada red. | No existe un sistema de visualización de posibles amenazas en la red. | Detectar incidentes de seguridad informática a través de patrones anómalos de comportamiento. | Aumentar en un 70% la capacidad de detección de  amenazas dentro de la red | Obtener hasta 10% de error en la detección de anomalías |
| OE2 | Automatizar la detección de amenazas a través de patrones customizados y en tiempo real. | No existe monitoreo constante sobre las redes de las pymes. | Visualizar posibles amenazas sin tener que estar constantemente observando el equipamiento. | Aumentar en un 80% la capacidad de detectar lo anómalo que esta circulando por la red de la organización. | Detección con un margen de error de un 10%. |
| OE3 | Disminuir la probabilidad de que los datos y Dashboards mostrados entreguen datos erróneos, no acordes a la realidad. | No existe una plataforma que permita customizar las reglas y patrones de comportamiento, de acuerdo a la realidad de la organización. | Lograr la Visualización de los incidentes ocurridos en la red y corroborar que estén funcionando correctamente. | Lograr un 80% en el éxito de visualizar incidentes de seguridad | Obtener eventos con un 90% de exactitud. |
| OE4 | Aumentar los tiempos de respuesta ante un incidente informático por parte del personal de Seguridad TI. | No existe una capacitación formal del personal de Seguridad TI o no existe personal de Seguridad TI. | Lograr aumentar los tiempos de reacción y mitigación de los incidentes informáticos. | Aumentar los tiempos de respuesta en un 50% de parte del equipo de seguridad TI la mitigación de un incidente informático. | Mitigar los incidentes informáticos con un margen de error del 10%. |
| OE5 | Aumentar o generar la visualización de los diferentes logs que circulan por una red, a través de un sistema de correlación de eventos. | En muchas Pymes no existe un sistema de visualización de los logs que circulan por sus redes.. | Permitir la visualización de los logs que circulan por una determinada red. | Aumentar en un 50% la visualización de lo que esta sucediendo en una red informática. | Obtener logs y visualización de estos con un 85% de certeza. |

**Tabla de objetivos específicos**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **C1** | **C2** | **C3** | **C4** |
| **OE1** | **X** |  |  |  |
| **OE2** |  | **X** |  |  |
| **OE3** |  | **X** |  |  |
| **OE4** |  |  | **X** | **X** |
| **OE5** |  | **X** |  | **X** |

**Trazabilidad de objetivos y causas**

# **1.6 Alcances**

1. El sistema se implementará en un servidor físico o en su defecto se podría usar virtualización.
2. Se considerará que el sistema debe tener una consola de monitoreo y visualización.
3. El sistema será diseñado para ser implementado a modo de marcha blanca en un laboratorio de computación en producción.
4. El sistema debe ser capaz de detectar patrones anómalos en la red.
5. El sistema utilizará mecanismos de parseo y customización de acuerdo a demanda.
6. En caso de no contar con hardware entregado por el cliente, se realizar pruebas en ambientes virtuales.
7. Los datos almacenados serán de propiedad del laboratorio en donde se implemente.

# **1.7 Limitaciones**

1. Los datos que se utilizarán en la fase de pruebas se generarán desde un ambiente virtualizado.
2. Para la fase de pruebas no se tomarán datos reales desde la organización donde se implemente, a no ser que el cliente esté de acuerdo.
3. La implementación final será efectuada en servidores Linux.
4. Se debe tener claridad de la infraestructura de red en donde se implementará el sistema.
5. Se deben crear motores customizados para la detección de patrones anómalos de comportamiento.

## 2 Fundamentación

A continuación se presentan algunas alternativas para dar solución a la problemática.

## Alternativas de solución

1. **SolarWinds Security Event Manager** (SEM)

Se deben hacer pruebas objeto determinar si es la opción correcta para el cliente. Esta es una solución SIEM de uso múltiple con un énfasis particular en el cumplimiento de HIPAA, PCI DSS , SOX y más. SEM tiene una sólida funcionalidad lista para usar, lo que hace que la implementación sea fácil. Mucho de esto proviene del hecho de que es muy autónomo. Los parámetros de automatización incluidos bloquean variados tipos de amenazas, y la búsqueda avanzada brinda una funcionalidad similar a un motor de búsqueda para registrar el análisis.

1. **Threat Monitor**

Es una opción SIEM centrada en la seguridad con la misma gran experiencia y soporte de SolarWinds. Al instalarla estará protegido de las últimas vulnerabilidades recientemente descubiertas en tiempo casi real con sus evaluaciones de amenazas y capacidades de detección de intrusos constantemente actualizadas.

Hay más respuestas automatizadas y más control sobre la programación de sus propias respuestas automatizadas con Threat Monitor. Además, aún obtiene informes de cumplimiento e índices altamente detallados y fáciles de buscar.

Una de las desventajas para nuestro modelo es que el producto está basado en la nube.

1. **Splunk Free**

Por funcionalidad, el producto Splunk completo es uno de los mejores software SIEM del mercado. Ofrece descripciones completas de seguridad y es muy fácil de navegar a pesar de su complejidad. Las capacidades de visualización y análisis de activos son particularmente útiles. Sin embargo, asegúrese de tener en cuenta que la versión gratuita, si bien es similar a la licencia completa, le permite indexar solo hasta 500 MB por día. Obviamente, esto no funciona para muchas empresas. La versión gratuita también tiene otras limitaciones, por lo que no es una gran solución a largo plazo.

1. **OSSEC**

OSSEC es un sistema de detección de intrusos de código abierto popular entre todos excepto la multitud de Windows. Está disponible para macOS, Linux, Solaris y BSD. Las ventajas incluyen los modos sin servidor y de agente de servidor, y una funcionalidad casi completa en la versión de código abierto. El análisis de registro de OSSEC, que analiza muchas fuentes diferentes, incluidos FTP, servidores de correo, bases de datos y más. Además, OSSEC es óptimo para monitorear varias redes desde un mismo punto.

Pero el sistema tiene algunas desventajas, solo está disponible para Windows en modo servidor-agente. Además, los usuarios han informado de problemas al actualizar a medida que el software vuelve a las reglas listas para usar. Incluso si descarga y vuelve a cargar su configuración, puede causar caos durante la actualización misma.

1. **OSSIM**

OSSIM es una de las opciones de código abierto más potentes y completas disponibles. Tiene prácticamente toda la funcionalidades descritas anteriormente, incluidos el registro y monitoreo a corto plazo (SEM) y la evaluación de amenazas a largo plazo, el archivo y análisis de datos, y las respuestas automatizadas (SIM).

Sin embargo, OSSIM es inflexible y difícil de manejar. Los administradores de sistemas se quejan de configuraciones laboriosas, especialmente en Windows, y grandes inversiones de tiempo para personalizar el software. (El soporte de OSSIM también es prohibitivamente costoso).

1. **Elasticsearch**

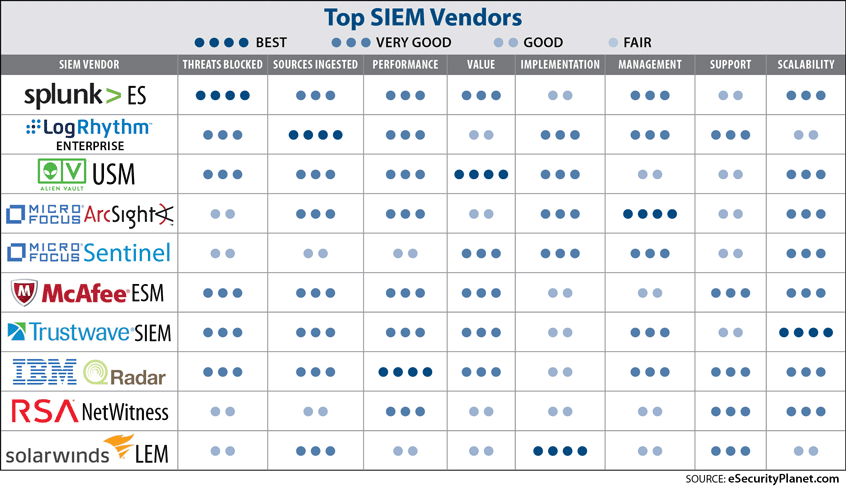
Elasticsearch, anteriormente conocido como ELK Search, es un paquete de soluciones de software. (ELK es un acrónimo de los programas componentes Elasticsearch, Logstash y Kibana). Como tal, Elasticsearch es un conjunto potente y versátil, pero carece de algunas funcionalidades importantes.

Logstash y Beats proporcionan los registros de registro. Beats son expedidores y recolectores de datos rápidos y simples, mientras que Logstash filtra esos datos y permite numerosos complementos personalizados. Elasticsearch es el motor que impulsa la exploración de los datos, y Kibana proporciona visualización.

Elasticsearch carece de algunas características importantes que lo convertirían en un SIEM completo. En particular, es débil en la correlación, no proporciona alertas listas para usar y no puede proporcionar gestión de incidentes por sí solo. Aún así, con su poderosa arquitectura, personalización y naturaleza de código abierto, no sorprende que Elasticsearch sea tan poderoso y también proporcione la base para varias de las otras selecciones en esta lista.

1. **Graylog**

Graylog captura, almacena y permite la búsqueda y el análisis de registros en tiempo real contra terabytes de datos de máquina de cualquier componente en la infraestructura de TI y las aplicaciones.​ El software utiliza una arquitectura de tres niveles y un almacenamiento escalable basado en Elasticsearch. Graylog se ha hecho un espacio como una alternativa rápida, asequible y viable.



**Tabla comparativa Vendors Siem**

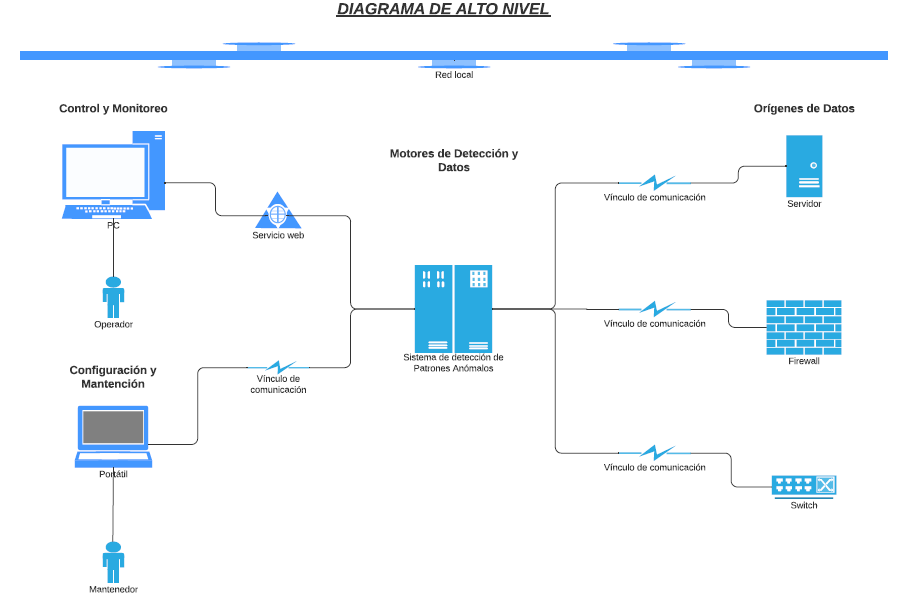
## Factibilidades

**Factibilidad Económica**:

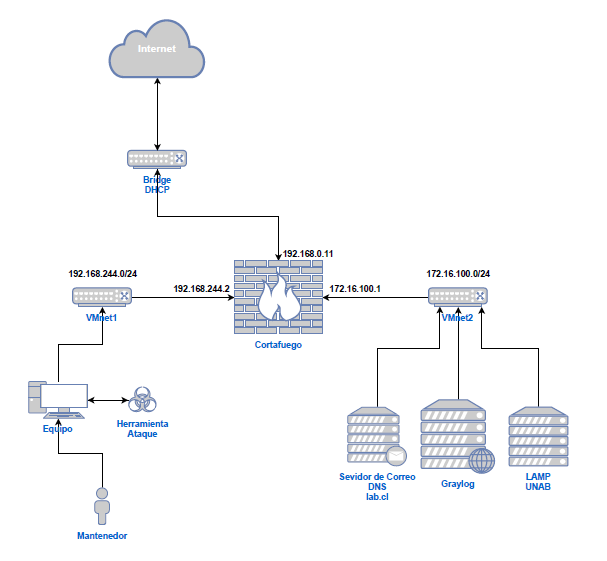
En vista de que este proyecto esta basado principalmente en herramientas OpenSource, no debería haber un costo económico de por medio, esto asumiendo de que se implemente en maquinas virtuales, las cuales debieran estar alojadas en servidores facilitados por el cliente. Por todo esto no esta considerada la factibilidad económica para este proyecto.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Correlacionador de eventos** | **Costo** | **Fuente** |
| 1 | SolarWinds Security Event Manager | Desde los **US$4,665** para monitorear 30 nodos. | https://www.networkmanagementsoftware.com/solarwinds-security-and-event-manager-review/ |
| 2 | Threat Monitor | Desde los **US$4,075** por mes (suscripción). | https://www.getapp.com/security-software/a/solarwinds-threat-monitor/pricing/ |
| 3 | Splunk Free | El costo de Splunk por 100gb es de alrededor de **$1500 USD**.  Por 10gb el valor es de **$2500 USD**.  Por 1gb el valor es de **$4500 USD**. | https://www.learnsplunk.com/splunk-pricing---splunk-licensing-model.html |
| 4 | OSSEC | **Free**, cobros por módulos adicionales (valores no entregados) | https://www.ossec.net/ |
| 5 | OSSIM | Parte en **US$0.645 p/hr – US$468 p/mes** (suscripción) | https://aws.amazon.com/marketplace/pp/AlienVault-OSSIM/B00BIUQRGC#pdp-pricing |
| 6 | Elasticsearch | **Free** | https://www.elastic.co/ |
| 7 | Graylog | **Free** | https://www.graylog.org/products/open-source |

**Tabla comparativa de precios sistemas de correlación**



**Diagrama de alto nivel**



**Arquitectura del sistema**

**Factibilidad Técnica:**

A pesar de que actualmente no se cuenta con los datos reales y la estructura de red en la cual se desplegara el sistema, se tiene considerado hacerlo en servidores Linux, en los cuales se instalaran las herramientas necesarias para el correcto funcionamiento del sistema.

Herramientas a utilizar serán de código abierto; por lo tanto documentación de estos dispositivos esta disponibles en los respectivos repositorios, a su vez también hay foros, comunidad, GitHub, etc. en donde se puede recopilar información.

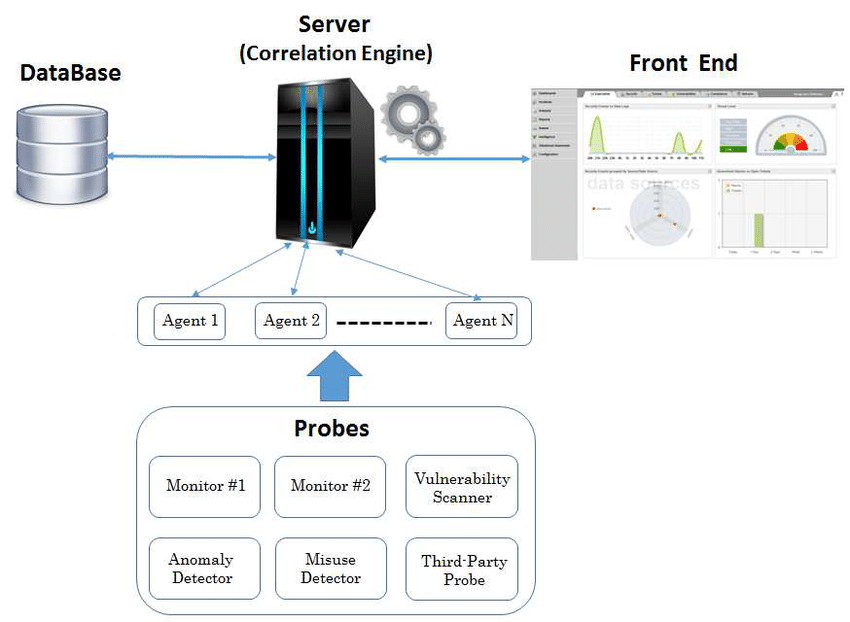
**Factibilidad operativa:**

En vista de que este proyecto se realizara con herramientas de código abierto, los mantenedores, administradores y operadores de estos tendrán la ventaja de contar con un sistema que puede ser customizado de acuerdo a los requerimientos de cada realidad.

A su vez existen bastantes repositorios en la web, en donde se puede obtener información y paso a paso de las herramientas de código abierto.

## Propuesta

Dentro del server representado por el engranaje esta el engine de patrones



**Ilustración 2: Esquema del sistema propuesto**

**Requisitos no funcionales del sistema.**

Los principales requisitos no funcionales definidos para este proyecto son:

|  |  |
| --- | --- |
| **Nombre RNF – 1** | **Usabilidad** |
| Descripción del RNF | El sistema y visualización de los distintos Dashboards del sistema, debe ser amigable con el usuario y de fácil interpretación, esto con el objeto de realizar una buena gestión de los eventos, con el objetivo de tomar las correspondientes medidas de mitigación. |
| Requisito para la aprobación | El usuario debe ser capaz de utilizar el sistema y obtener información útil y en tiempo real con al menos de cuatro horas de entrenamiento previo. |

|  |  |
| --- | --- |
| **Nombre RNF – 2** | **Usabilidad** |
| Descripción del RNF | Al ser un sistema que colecta grandes volúmenes de datos, este deberá contar con una base de datos acorde al almacenamiento de recolección diaria. |
| Requisito para la aprobación | El sistema debe ser capaz de al menos guardar datos por un periodo de 2 años, sin recurrir a la sobre escritura de los datos.  El sistema debe responder a solicitudes a servicios web en menos de 5 segundos. |

|  |  |
| --- | --- |
| **Nombre RNF – 3** | **Usabilidad** |
| Descripción del RNF | Al ser un sistema que recolecta y almacena grandes volúmenes de datos y que requiere una base de datos acorde a estos requerimientos. |
| Requisito para la aprobación | El sistema debe responder a consultas y filtros de búsqueda efectuados en no mas de 30 segundos. |

|  |  |
| --- | --- |
| **Nombre RNF – 4** | **Usabilidad** |
| Descripción del RNF | El sistema será desplegado en ambiente web, por lo que debe ser capaz de ejecutarse sin problemas en browsers de diferentes sistemas operativos como Windows, MacOS y Linux. |
| Requisito para la aprobación | El sistema debe ser visualizado sin problemas en a lo menos Internet Explorer, Firefox y Chrome. |

# **Materiales y Métodos**

## 3.1 Plan de proyecto (incluir planificación otras métricas).

**Metodología Seleccionada.**

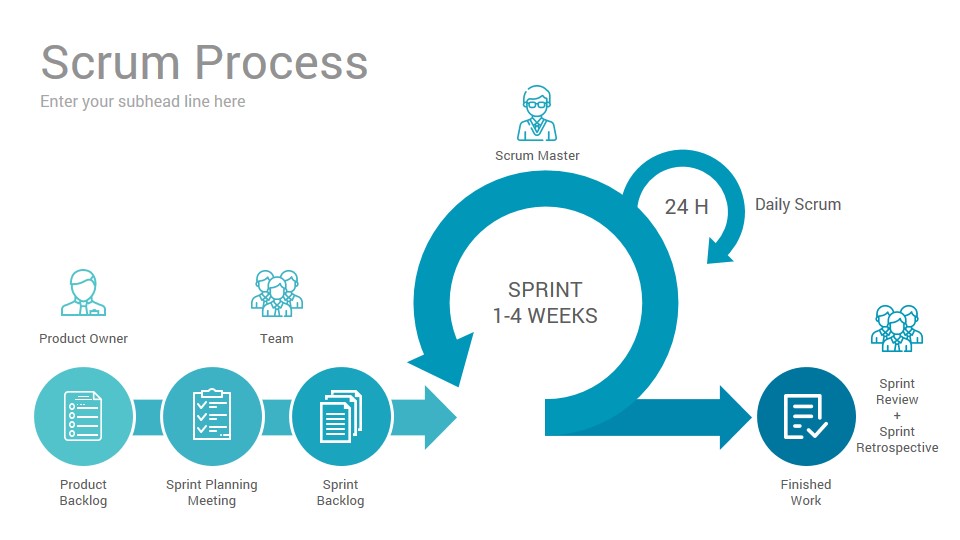
Con el objeto de llevar a cabo una metodología acorde a la implementación de este proyecto se seleccionaron las siguientes metodologías considerando la naturaleza del proyecto y los tiempos asociados a este, estas son:

* Metodología de gestión de proyecto: **SCRUM**
* Metodología de desarrollo: **Iterativo / Incremental**

**Metodología de Gestión de proyecto**

En este proyecto se decidió por utilizar la metodología SCRUM en base al tipo de implementación propuesto, se debe tener en cuenta que una metodología ágil debiera ser la más útil para este proyecto ya que el equipo que desarrollara el proyecto será reducido y además es flexible ya que se adapta fácilmente a los cambios de requerimientos por parte del parte del cliente.

La metodología SCRUM organiza el desarrollo del proyecto y la entrega del producto en ciclos cortos llamados Sprint los que al final del día, hacen posible entregar una parte del producto, SCRUM permite minimizar los riesgos, ya que la planificación y revisión del avance puede cambiar al inicio y durante cada sprint. En este caso y como es lo recomendado la duración de cada sprint de este proyecto será de 4 semanas.



**Ilustración 3: Proceso Scrum**

La metodología SCRUM define roles para las personas que participaran durante el desarrollo del proyecto. Los roles están definidos como se detalla a continuación:

* Product Owner: Romina Torres. Establecerá la priorización de los elementos o requisitos que se desarrollaran en cada iteración (Sprint para el caso de SCRUM) y realizara la trazabilidad de estos con el avance del proyecto.
* Scrum Master: Jonathan Armijo. Encargado de llevar las historias de usuario a tareas y será el encargado de estimar los tiempo para cada una de estas, confeccionara además todo lo relacionado con esta etapa como el Product Backlog y Sprint Backlog, a su vez realizara el control y monitoreo del avance de estos.
* Equipo de desarrollo: Jonathan Armijo. Sera el encargado de realizar la ejecución de las tareas programadas para el sprint y se asignará a si mismo cada una de estas, tomando en cuenta sus competencias.

**Priorización de historias de usuarios** .

En este proyecto los requerimientos que será especificados en el Product Backlog se estimaran de acuerdo a su dificultad, utilizando la serie de Fibonacci asignar un valor dependiendo de la complejidad del requerimiento, los números que se utilizaran son: 8, 5, 3, 2 donde 8 es el requerimiento de mayor dificultad y 2 el de menor dificultad.

Para la priorización de las historias de usuario detalladas en el Product Backlog, se utilizará la técnica “MoSCoW”, donde el Product Owner asignará un valor de prioridad a cada H.U. Los valores que se utilizaran para este proyecto son:

* Letra “M” (Must): H.U que debe ser implementada ya que es de importancia vital para el funcionamiento del sistema.
* Letra “S” (Should): H.U que debería ser idealmente implementada, pero se puede prescindir de ella en el sistema.
* Letra “C” (Could): H.U que podría ser implementada, pero se puede prescindir de ella.
* Letra “W” (Won’t): H.U que no se necesita implementar inmediatamente, pero podría ser incluida en el futuro.

**Composición de los Sprint**

**Entregables**

Al término de cada sprint, se entregará un avance de la implementación. Esta incluirá un avance o modulo implementado, el cual debe ser aceptado por el Product Owner, en base a los criterios de aceptación definidos al inicio del Sprint.

**Plantillas y formatos**

A continuación, se presenta la plantilla que se utilizara para registrar las historias de usuario con sus respectivos criterios de aceptación.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Product Backlog** | | **Historias de Usuario** | |  | |
| N° | Rol | Objetivo | Razón | Prioridad | Peso |
| XX | Como admin | Quiero Tener | Para Generar | M | 8 |
| XX | Como Operador | Quiero Ver | Para Entregar | C | 5 |
| XX | Como Dueño | Quiero Desplegar | Para Decidir | S | 3 |
| XX | Como Gerente | Quiero Agregar | Para Notificar | W | 2 |

Plantilla Product Backlog

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criterios de Aceptación** | | | | | |
| **N° HU** | **N°**  **Escenario** | **Criterio de Aceptación** | **Contexto** | **Evento** | **Resultado/Comportamiento esperado** |
| A | 1 | Escenario | En caso de <contexto> y/o <contexto> | Cuando <evento> | El sistema <resultado / comportamiento> |
|  | 2 | Escenario | En caso de <contexto> y/o <contexto> | Cuando <evento> | El sistema <resultado/comportamiento> |
| B | 1 | Escenario | En caso de <contexto> y/o <contexto> | Cuando <evento> | El sistema <resultado/comportamiento> |
|  | 2 | Escenario | En caso de <contexto> y/o <contexto> | Cuando <evento> | El sistema <resultado/comportamiento> |

**Plantilla Criterios de aceptación**

**Planificación del proyecto**

Al llegar al final de cada sprint, se realizará una reunión con el Product Owner, donde se entregará el producto resultante del sprint, en el cual se efectuara la trazabilidad con el Sprint Backlog y los criterios de aceptación definidos en conjunto con el Product Owner.

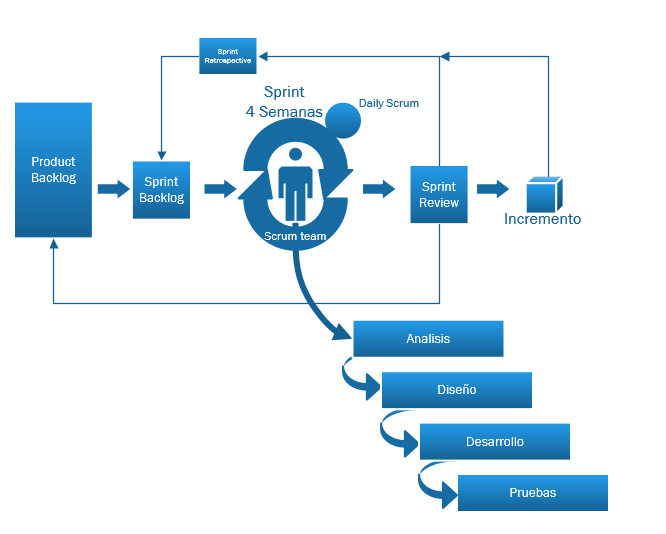
El Product Owner será encargado de aprobar o rechazar el sprint o parte de él, a su vez se acordarán las tareas pendientes del sprint para la ejecución en el próximo sprint o en otro momento dentro del ciclo de vida del proyecto.

**Metodología de Desarrollo**

Para este proyecto se decidió por la metodología iterativa incremental, la cual permite utilizar las etapas como es el análisis, diseño, desarrollo y pruebas del proyecto. Se compone de bloques definidos según las etapas antes descritas que iteran cada vez que termina un ciclo completo, al final de cada iteración se agrega un incremento al producto donde la idea principal perfeccionar el producto en cada iteración.

De acuerdo a lo visto esta metodología de desarrollo encaja con el tipo de implementación a desarrollar ya que se recomienda utilizarla cuando los requerimientos están completamente definidos y que, al combinarlo con SCRUM, permite adaptarse a los cambios de requerimientos que puedan existe durante el transcurso del avance del proyecto.

Para este proyecto se combinarán ambas metodologías (SCRUM e iterativo incremental) donde la metodología de desarrollo se ejecutará dentro de cada sprint.



**Ilustración 4: Metodología de Desarrollo aplicada a la metodología de gestión**

**Plan de Proyecto**

Product Backlog

A continuación, se presentan las historias de usuario que permitirán confeccionar el Product Backlog para el proyecto.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID HU** | **Rol ¿Quien?** | **Característica Funcionalidad Objetivo ¿Quiero?** | **Razón Resultado ¿Para qué?** | **Prioridad** | **Pts Hist HU** | **# Sprint** |
|  | - |  |  |  |  |  |
| HU-PA01 | Como operador | Quiero visualizar alertas en caso de que ocurra una anomalía en la red. | Para tener una visualización rápida de las anomalías. | M | 8 | 1 |
|  | - |  |  |  |  |  |
| HU-PA02 | Como operador | Quiero recibir un correo electrónico en el cual se indique el incidente informático. | Para en caso de no estar en las dependencias, saber que incidente esta ocurriendo. | S | 13 | 2 |
|  | - |  |  |  |  |  |
| HU-PA03 | Como Mantenedor | Quiero generar y visualizar ataques en la sistema de correlación de eventos. | Para poder discriminar entre un incidente y un falso positivo. | M | 13 | 3 |
|  | - |  |  |  |  |  |
| HU-PA04 | Como operador | Quiero poder visualizar el estado de los dispositivos conectados a la red. | Para poder determinar que dispositivo se encuentra con problemas. | M | 13 | 9 |
|  | - |  |  |  |  |  |
| HU-PA05 | Como administrador | Quiero poder integrar de forma correcta el modulo de detección de patrones de comportamiento con el actual sistema de correlación de eventos. | Para poder detectar y mostrar lo desconocido en la red a los encargados. | M | 13 | 5 |
|  | - |  |  |  |  |  |
| HU-PA06 | Como administrador | Quiero poder implementar dicho sistema y que sea escalable, en el sentido de que se puedan agregar mas dispositivos. | Para poder tener una mejor visualización del estado de la red. | M | 13 | 1 |
|  | - |  |  |  |  |  |
| HU-PA07 | Como administrador | Quiero implementar un modulo que logre detectar patrones anómalos de comportamiento dentro de una red corporativa. | Para entregar una mejor visualización a los encargados de Seguridad TI. | M | 26 | 5 |
|  | - |  |  |  |  |  |
| HU-PA08 | Como administrador | Quiero crear reglas de detección de patrones anómalos de comportamiento. | Para poder detectar comportamientos anómalos en la red. | M | 13 | 6 |
| HU-PA09 | Como administrador | Quiero implementar un sitio web en donde se de a conocer el trabajo en Ciberdefensa y tenga la capacidad de generar una autoevaluación a las Pymes. | Para poder detectar el estado actual de la red de una Pyme. | M | 20 | 4 |

**Sprint Backlog**

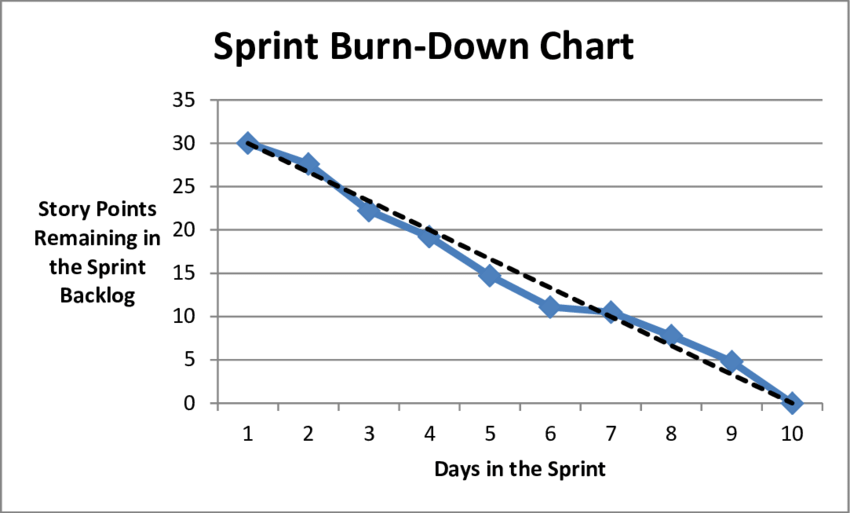
De acuerdo a las historias de usuario descritas en el Product Backlog, se realizará el desglose de tareas que corresponderán a cada iteración, por ej. para la realización del primer sprint se completaran las H.U. que se documentaran en el Anexo Sprint 1.

**Burn Down chart**

Mientras se mantenga el desarrollo de cada sprint se realizará un seguimiento del avance para cada una de las tareas descritas en el Sprint Backlog. Para esta tarea se utilizará una plantilla, la cual se llenará con las tareas asignadas para cada sprint con la estimación en horas trabajadas y horas restantes para terminar la tarea/sprint.

A su vez la plantilla utilizada genera un gráfico que referencia el avance esperado con el avance real del proyecto. De esta forma es posible ajustar los tiempos de avance y estimación de horas de trabajo para cada tarea.

El ajuste del tiempo de avance y la medición del avance del proyecto en horas, permite una mejor estimación de la capacidad real de avance del equipo de desarrollo. De esta manera es posible hacer estimaciones cada vez más precisas para cada iteración del proyecto.



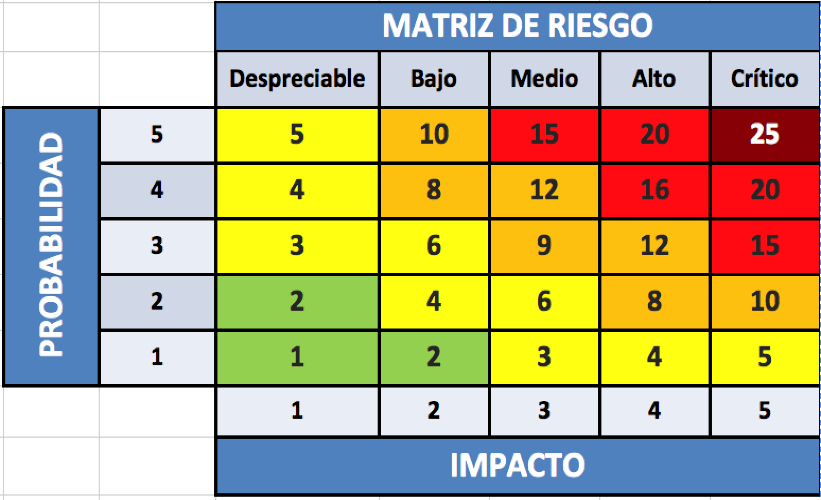
**Ilustración 5: Ejemplo de Sprint Burn-Down**

## Plan de Gestión de Riesgos

**Análisis y gestión de riesgos**

Para llevar a cabo el análisis y gestión de riesgos esta se realizará utilizando el siguiente cronograma:

1. Planificación de la gestión de riesgo: Se elaborara un plan general según la identificación de riesgos y su mitigación.
2. Identificación de los riesgos: Se incluye una lista de riesgos que pueden afectar el avance del proyecto.
3. Análisis Cualitativo: Se evalúa la probabilidad de los riesgos utilizando una matriz de probabilidad e impacto del riesgo.
4. Análisis Cuantitativo: Se evalúa el nivel de riesgo utilizando la matriz de riesgo con los valores obtenidos del análisis cuantitativo del riesgo.
5. Plan de mitigación de riesgo: Define una respuesta al riesgo según el resultado del añiláis cuantitativo.
6. Seguimiento y control de riesgo: Lleva control de la mitigación de los riesgos y la aplicación de las medidas correctivas de estos. Además, evalúa nuevos riesgos que puedan aparecer durante el avance del proyecto.



**Ilustración 6: Matriz de riesgo**

**Identificación de riesgo técnico**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Análisis de Riesgos Técnicos** | | | | | | | |
| **N°** | **Riesgo** | **Posible resultado** | **Plan de Mitigación** | **Plan de Contingencia** | **Evidencia** | **Estado** |
| 1 | Desconocer el como crear patrones de detección de anomalías. | Retraso en la puesta en marcha del proyecto. | Efectuar búsqueda de tutoriales y documentación al respecto. | Efectuar cursos de capacitación y/o Contratar especialista externo. | Certificado del curso realizado y/o  Patrones creados en equipamiento. | En proceso de resolución e investigación |
| 2 | Desconocer la confección de reglas Yara. | Retraso en la puesta en marcha del proyecto. | Efectuar búsqueda de tutoriales y documentación al respecto. | Efectuar cursos de capacitación y/o Contratar especialista externo. | Certificado del curso realizado y/o  Patrones creados en equipamiento. | En proceso de resolución e investigación |
| 3 | Desconocer como funciona una red de datos, topología, arquitectura, protocolos, etc. | Retraso en la puesta en marcha del proyecto. | Efectuar búsqueda de tutoriales y documentación al respecto. | Efectuar cursos de capacitación y/o Contratar especialista externo. | Certificado del curso realizado y/o  Patrones creados en equipamiento. | En proceso de resolución e investigación |
| 4 | Desconocer el trabajo con servidores Windows y Linux. | Retraso en la puesta en marcha del proyecto. | Efectuar búsqueda de tutoriales y documentación al respecto. | Efectuar cursos de capacitación y/o Contratar especialista externo. | Certificado del curso realizado y/o  Patrones creados en equipamiento. | En proceso de resolución e investigación |
| 5 | Desconocer el como se implementar, operan y administran herramientas de correlación de eventos. | Retraso en la puesta en marcha del proyecto. | Efectuar búsqueda de tutoriales y documentación al respecto. | Efectuar cursos de capacitación y/o Contratar especialista externo. | Certificado del curso realizado y/o  Patrones creados en equipamiento. | En proceso de resolución e investigación |
| 6 | Desconocimiento del tipo de datos y logs que circulan por la red en donde se implementara el sistema. | Retraso en la puesta en marcha del proyecto. | Efectuar visita en terreno y consultar a encargado de red estos antecedentes. | Efectuar visitas guiadas y POC, objeto detectar y corroborar formato de logs de dispositivos. | Documento entregado por encargado de red. | En proceso de resolución e investigación |
| 7 | Desconocimiento en virtualización, plataformas, imágenes, reenrutamientos, etc. | Retraso en la puesta en marcha del proyecto. | Efectuar búsqueda de tutoriales y documentación al respecto. | Efectuar cursos de capacitación y/o Contratar especialista externo. | Certificado del curso realizado y/o  Patrones creados en equipamiento. | En proceso de resolución e investigación. |
| 8 | La customización de patrones pensada es más difíciles de implementar de lo que se esperaba. | Perder mucho tiempo resolviendo el problema. Atraso en el proyecto. | Solicitar ayuda a un profesor o entendido que conoce el ambiente de desarrollo o Lenguaje de programación. | Cambiar el enfoque de la solución, por algo con lo que se obtenga el mismo resultado. | En GitHub se van almacenando los patrones de prueba en los que se ha trabajado durante el desarrollo del proyecto. | En proceso de resolución e investigación. |
| 9 | No contar con un buen Dataset de eventos o logs con valor agregado. | Retraso en la puesta en marcha del proyecto. | Descargar Logs de Internet, solicitar Dataset de logs a encargados de red de la Universidad. | Pedir apoyo a encargados de red de la Universidad. | Correos electrónicos solicitando apoyo y Dataset. | En proceso de resolución e investigación. |
| 10 | No contar con los conocimientos necesarios para desarrollar la creación de reglas o código en lenguaje Python. | Atraso en los periodos estipulados de entrega. Pérdida de tiempo. Desconocimiento de errores que aparecen en el proceso de programación y pruebas. | Tomar clases de programación en Python Online. Buscar tutoriales y explicaciones en Internet. | Pedir apoyo al profesor guía, compañeros de clase u otra persona que tenga conocimiento en el tema. | Matrícula de curso de programación online. Correos y WhatsApp de apoyo con profesor guía. | En proceso de resolución e investigación. |

## Plan de Gestión de la Configuración y Cambios

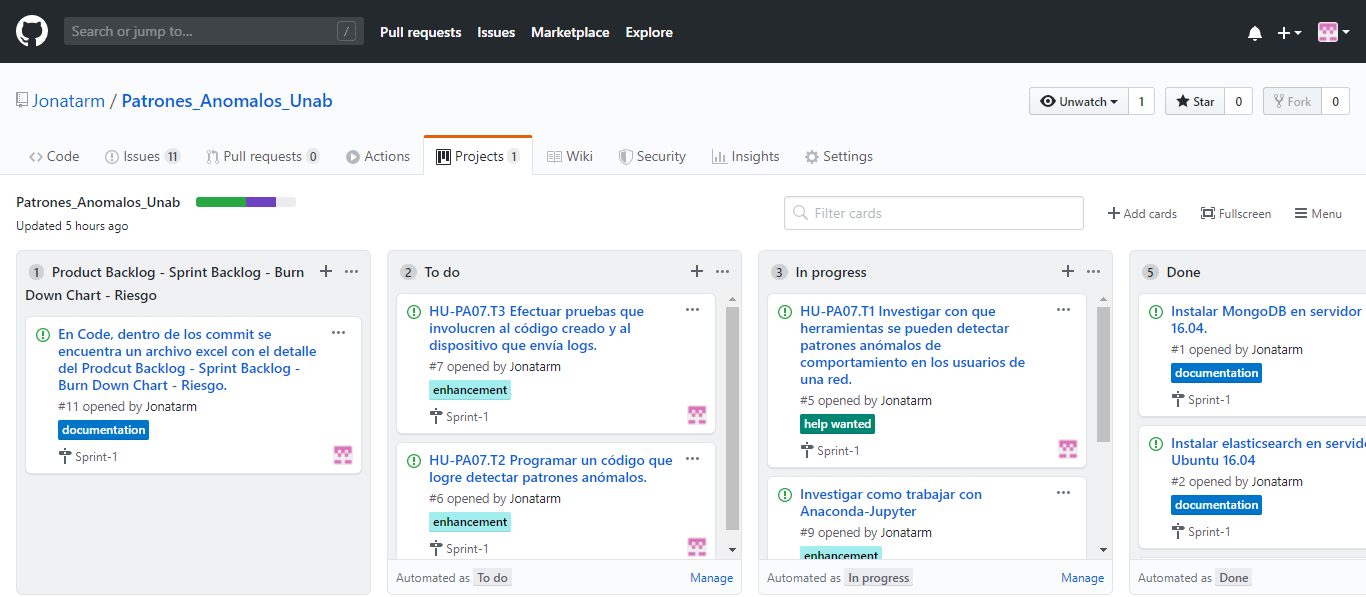
Se debe tener presente que desde los inicios del alcance del proyecto, es imprescindible que se especifiquen de modo claro, conciso y sin ambigüedades las metas a cumplir, durante la ejecución del mismo, junto con todas aquellas limitaciones que deben ser tenidas en cuenta para su óptimo desarrollo.

No obstante, es común que, durante su realización empírica, se presente la necesidad de efectuar algún tipo de cambio. Por ello, es importante conocer las características de este tipo de gestión, junto con la descripción de los pasos a tener en cuenta y que integran, a la vez, el procedimiento para llevar a cabo este conjunto de modificaciones.

A continuación se muestra esto a través de un Workflow (Flujo de Trabajo) “Gestión de Cambios”.



**Ilustración 7: Workflow Gestión de cambios**



**Ilustración 8: Github del proyecto**

## Plan de Aseguramiento de la Calidad (pruebas)

Un plan de aseguramiento de la calidad es un documento que asegura a través del autocontrol cada uno de los procesos, tareas y acciones a realizar, este se apoya en forma principal por un plan de procedimientos, el cual es asignado a cada una de las tareas. Los Procedimientos, son documentos complementarios en los que se describe, con el nivel de detalle preciso en cada caso, cómo, cuándo, dónde, para qué y con qué, debe realizarse una determinada actividad ya programada, siguiendo las directrices establecidas. Su objeto es normalizar los procedimientos y evitar las indefiniciones e improvisaciones que pudieran dar lugar posteriormente a problemas o deficiencias en la realización de cada actividad.

|  |  |
| --- | --- |
| Serie | SP1 – HU-PA01 / HUPA06 – P01 |
| Nombre de la prueba | Parsear logs de prueba en sistema |
| Tipo de prueba | Prueba unitaria |
| Resumen objetivo | Al ingresar un log no categorizado al sistema, este debe ser capaz de parsearlo, identificando como esta compuesto. |
| Historia de usuario | HU-PA01 / HU-PA06 |
| Pre-condición | * Haber ingresado en forma correcta al sistema. * Seleccionar un log valido del sistema y verificar que este haya sido parseado. |
| Pasos | * Seleccionar el log deseado. * Hacer clic sobre este y desplazarse hacia abajo verificando la deconstrucción del log. * En caso sea requerido se puede realizar búsqueda por otros logs que estén cumpliendo misma categoría. |
| Resultado esperado | Que el log recibido pueda parsearse en al menos:   * beats\_type * Message * Source * Timestamp * winlogbeat\_beat\_hostname * winlogbeat\_event\_data\_PrivilegeList * winlogbeat\_log\_name |

## Entornos de desarrollo, pruebas y producción

**Entornos de desarrollo.**

1. **Servidor de desarrollo:**

Servidor Centos virtualizado, aquí se efectuaron pruebas del despliegue del correlacionador, el cual funcionaba bien, pero no de forma optima. Herramienta Anaconda – Jupyter, aquí es donde se realizan las pruebas al código Python, objeto verificar certeza de este.

1. **Servidor de integración:**

Maquina virtual Ubuntu 16.04, montada en equipo personal.

Máquinas virtuales montadas en AWS, estas pruebas no fueron satisfactorias, ya que capacidades de maquinas AWS asignadas a Universidad son muy limitadas.

1. **Servidor de producción:**

Maquina virtual Ubuntu montada en plataforma oVirt (Open virtualization Manager), posterior a esto se procede con la instalación de las herramientas Elasticsearch, MongoDB, actualmente sistema se encuentra instalado, operando y sensando datos en Laboratorio 316.

El sistema se encuentra alojado en servidores de la Universidad Andrés Bello, al cual se puede acceder desde los equipos de la red del laboratorio 306 (las islas de al fondo de la sala.

# **Resultados y Discusión**

## Análisis

**Historias de usuario (HU)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID HU** | **Rol ¿Quien?** | **Característica Funcionalidad Objetivo ¿Quiero?** | **Razón Resultado ¿Para qué?** | **Prioridad** | **Pts. Hist HU** | **# Sprint** |
| HU-PA01 | Como operador | Quiero visualizar alertas en caso de que ocurra una anomalía en la red. | Para tener una visualización rápida de las anomalías. | M | 8 | 1 |
| HU-PA02 | Como operador | Quiero recibir un correo electrónico en el cual se indique el incidente informático. | Para en caso de no estar en las dependencias, saber que incidente esta ocurriendo. | S | 13 | 2 |
| HU-PA03 | Como administrador | Quiero generar y visualizar ataques en la sistema de correlación de eventos. | Para poder discriminar entre un incidente y un falso positivo. | M | 13 | 3 |
| HU-PA04 | Como operador | Quiero poder visualizar el estado de los dispositivos conectados a la red. | Para poder determinar que dispositivo se encuentra con problemas. | M | 13 | 9 |
| HU-PA05 | Como administrador | Quiero poder integrar de forma correcta el modulo de detección de patrones de comportamiento con el actual sistema de correlación de eventos. | Para poder detectar y mostrar lo desconocido en la red a los encargados. | M | 13 | 5 |
| HU-PA06 | Como administrador | Quiero poder implementar dicho sistema y que sea escalable, en el sentido de que se puedan agregar mas dispositivos. | Para poder tener una mejor visualización del estado de la red. | M | 13 | 1 |
| HU-PA07 | Como administrador | Quiero implementar un modulo que logre detectar patrones anómalos de comportamiento dentro de una red corporativa. | Para entregar una mejor visualización a los encargados de Seguridad TI. | M | 26 | 5 |
| HU-PA08 | Como administrador | Quiero crear reglas de detección de patrones anómalos de comportamiento. | Para poder detectar comportamientos anómalos en la red. | M | 13 | 6 |
| HU-PA09 | Como administrador | Quiero implementar un sitio web en donde se de a conocer el trabajo en Ciberdefensa y tenga la capacidad de generar una autoevaluación a las Pymes. | Para poder detectar el estado actual de la red de una Pyme. | M | 20 | 4 |

**Criterios de Aceptación**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Número de escenario** | **Criterio de aceptación (Título)** | **Contexto** | **Evento** | **Resultado / Comportamiento esperado** | **Estado** |
| E1 | HU-PA01.T3.E1 - Visualización correcta. | Estando dentro del sistema debo poder visualizar distintos eventos. | Al seleccionar el menú "Search". | Visualizar diferentes eventos de red. | 100 % |
| E2 | HU-PA01.T3.E2 - Evento parseado correctamente. | Al seleccionar un evento, se debe corroborar que ese log sea del origen de datos que dice ser. | Al desplegarse un evento, luego de hacer clic sobre este. | Que el log parseado efectivamente sea del origen de datos que dice ser. | 100 % |
| E3 | HU-PA01.T3.E3 - Evento erróneo. | Al seleccionar un evento, este no muestre nada, solo basura. | Al intentar desplegar un evento, este no muestre nada. | Que efectivamente no se despliegue el menú hacia abajo. | 100 % |
| E1 | HU-PA02.T3.E1 - Evento gatillado correctamente en el panel de alertas. | Dentro del sistema debo poder visualizar el evento gatillado. | Al seleccionar y hacer clic en "Test" dentro de alarmas. | Visualizar alerta gatillada en pantalla. | 100 % |
| E2 | HU-PA02.T3.E2 - Plantilla de correo creada correctamente (JMTE). | Al seleccionar en "Notification" debo visualizar la plantilla JMTE y las configuraciones de envío. | Al seleccionar y hacer clic en "More actions / Edit" dentro de Notifications. | Visualizar configuración de envío y plantilla JMTE. | 100 % |
| E3 | HU-PA02.T3.E3 - Alerta enviada por correo electrónico. | Al seleccionar en el menú superior "Alerts" / "Notifications". | Al seleccionar y hacer clic en "Test" dentro del menú "Alerts" / "Notifications". | Visualizar correo electrónico con alerta enviada desde correlacionador de eventos. | 100 % |
| E1 | HU-PA03.T2.E1 - Parseo generado correctamente desde FW pfSense. | Dentro del sistema debo poder visualizar el evento detectado por Snort. | Al seleccionar y hacer clic en Event, dentro de pfSense. | Visualizar evento gatillado en pantalla. | 100 % |
| E2 | HU-PA03.T2.E2 - Ataque generado desde plataforma Mutillidae. | Al seleccionar ingresar a plataforma Mutillidae y seleccionar tipo de ataque. | Al seleccionar y hacer clic en Menú izquierdo Owasp 2017. | Visualizar el envío del ataque. | 100 % |
| E3 | HU-PA03.T2.E3 - Dashboard con detalle de anomalías en la red. | Al seleccionar en el menú superior "Search", filtrar por message o clasificación. | Al seleccionar y hacer clic en message y luego Quick value. | Visualizar Dashboard tipo torta y tabla con detalle de incidente. | 100 % |
| E1 | HU-PA06.T3.N/A - Ingreso exitoso. | Cuando usuario y contraseña coincidan con las registradas en sistema. | Posterior al ingresar usuario y contraseña y dar enter. | El usuario hará ingreso al sistema. | 100 % |
| E2 | HU-PA06.T3.N/A - Origen de datos ingresado correctamente. | Cuando el mantenedor ingrese un origen da datos nuevo al sistema. | Al hacer clic en guardar los cambios. | El origen de datos debiera mostrar el estado en "running". | 100 % |
| E3 | HU-PA06.T3.E3 - Origen de datos erróneamente ingresado. | Cuando el mantenedor ingrese un origen da datos nuevo al sistema. | Al hacer clic en guardar los cambios. | El sistema debe mostrar un ventana con la alerta y motivo, del porque no se ingreso el origen de datos. | 100 % |
| E1 | HU-PA07.T3.E1 - Detección exitosa | Cuando el log y el código coincidan con los parámetros programados. | Al ejecutar o hacer correr el modulo. | El modulo debe mostrar detección de comportamiento anómalo. | 100 % |
| E2 | HU-PA07.T3.E2 - Log no soportado | Cuando el log y el código no coincidan con los parámetros programados. | Al ejecutar o hacer correr el modulo. | El log no será parseado o detectado. | 100 % |
| E3 | HU-PA07.T3.E3 - Erróneamente detectado | Cuando el log y el código coincidan con los parámetros programados, pero esta detección no sea la correcta. | Al ejecutar o hacer correr el modulo. | El log quedara erróneamente parseado. | 100 % |
| E1 | HU-PA09.T5.E1 - Sitio web generado correctamente en servidores de Universidad. | Dentro del sitio web, debo poder visualizar los distintos módulos que componen este sitio. | Al ingresar a url http://ciberdefensa.informatica-unab-vm.cl. | Visualizar sitio web. | 100 % |
| E2 | HU-PA09.T5.E2 - Formulario de preguntas generado en forma correcta. | Dentro del sitio web en "Autoevaluación" debo visualizar la plantilla en donde se realicen las distintas preguntas. | Al seleccionar y hacer clic en "Autoevaluación" dentro del menú superior del sitio web. | Visualizar configuración de envío y plantilla JMTE. | 100 % |
| E3 | HU-PA09.T5.E3 - Resultados de autoevaluación deben ser enviados vía correo electrónico. | Terminando de responder todas las preguntas del formulario. | Al seleccionar y hacer clic en "Submit". | Visualizar correo electrónico con detalles de preguntas y respuestas en direcciones de email especificadas. | 100 % |

**Tabla: Criterios de aceptación**

**Pruebas de Desarrollador.**

|  |  |
| --- | --- |
| **Serie** | **SP1 – HU-PA01 / HU-PA06– P01** |
| Nombre de la prueba | Parsear logs de prueba en sistema |
| Tipo de prueba | Prueba unitaria |
| Resumen objetivo | Al ingresar un log no categorizado al sistema, este debe ser capaz de parsearlo, identificando como esta compuesto. |
| Historia de usuario | HU-PA01 / HU-PA06 |
| Pre-condición | * Haber ingresado en forma correcta al sistema. * Seleccionar un log valido del sistema y verificar que este haya sido parseado. |
| Pasos | * Seleccionar el log deseado. * Hacer clic sobre este y desplazarse hacia abajo verificando la deconstrucción del log. * En caso sea requerido se puede realizar búsqueda por otros logs que estén cumpliendo misma categoría. |
| Resultado esperado | Que el log recibido pueda parsearse en al menos:   * beats\_type * Message * Source * Timestamp * winlogbeat\_beat\_hostname * winlogbeat\_event\_data\_PrivilegeList * winlogbeat\_log\_name |

Posterior a esta prueba unitaria y a la visualización que se tiene actualmente de la plataforma, se tiene que el sistema se encuentra operando en forma normal y con sus módulos habilitados, ya que a través de él se visualiza que los logs de los orígenes de datos enviados hacia este correlacionador, están siendo parseados de manera correcta.

A su vez también se aprecia que al seleccionar un evento y deslazarse por su menú hacia abajo se aprecia que el log enviado en forma bruta (Ro), ahora se ve parseado y cada una de sus partes se encuentra catalogada, de acuerdo a lo seteado.

|  |  |
| --- | --- |
| **Serie** | **SP2 – HU-PA02** |
| Nombre de la prueba | Alerta gatillada sea enviada vía correo electrónico a cuenta dominio @lab.cl |
| Tipo de prueba | Prueba unitaria |
| Resumen objetivo | Al generarse un evento de warning o seguridad dentro del correlacionador, este se parsee como alerta y se envíe por correo electrónico. |
| Historia de usuario | HU-PA02 |
| Pre-condición | * Haber ingresado en forma correcta al sistema. * Posicionarse dentro del correlacionador de eventos. |
| Pasos | * Seleccionar el panel de alertas. * Hacer clic sobre “All Alerts” y visualizar alerta gatillada. * Dirigirse a gestor de correo “Thunderbird” y visualizar correo recibido. |
| Resultado esperado | Que el correo recibido muestre al menos:   * Alert description * Stream Title * Stream ID * Stream URL |

|  |  |
| --- | --- |
| **Serie** | **SP3 – HU-PA02** |
| Nombre de la prueba | Redireccionamiento a correlacionador de eventos desde URL inserta en cuerpo del correo |
| Tipo de prueba | Prueba unitaria |
| Resumen objetivo | Al recibir un correo electrónico desde Graylog y al hacer click en URL asociada este redirigirá a sistema Graylog |
| Historia de usuario | HU-PA02 |
| Pre-condición | * Haber ingresado en forma correcta al gestor de correo (Thunderbird) * Posicionarse en los inbox de cuenta [jonathan@lab.cl](mailto:jonathan@lab.cl) |
| Pasos | * Seleccionar correo desde inbox de cuenta jonathan@lab.cl * Hacer doble clic sobre correo * Dirigirse a Stream URL y hacer clic el link |
| Resultado esperado | Que el Stream Url inserto en el cuerpo del correo redirija hacia correlacionador de eventos |

|  |  |
| --- | --- |
| **Serie** | **SP4 – HU-PA02** |
| Nombre de la prueba | Ataque Web Stress visualizado en el panel de alertas |
| Tipo de prueba | Prueba unitaria |
| Resumen objetivo | Al generar un ataque desde la herramienta “Web Stress” el sistema en base a sus reglas cargadas es capaz de detectar y enviar logs al correlacionador de eventos. |
| Historia de usuario | HU-PA03 |
| Pre-condición | * Haber generado un ataque desde “Web Stress”. * Ingresar parámetros para generar ataque, desde “Web Stress” |
| Pasos | * Seleccionar “Run” desde “Web Stress”. * Hacer clic sobre “Search” en Graylog y seleccionar alerta de ataque. * En caso sea requerido se puede realizar búsqueda por otras alertas que estén cumpliendo misma categoría. |
| Resultado esperado | Que la alerta muestre al menos:   * Timestamp * Source * Message |

|  |  |
| --- | --- |
| **Serie** | **SP5 – HU-PA02** |
| Nombre de la prueba | Alerta gatillada detectada por motores en Firewall “pfSense” |
| Tipo de prueba | Prueba unitaria |
| Resumen objetivo | Al generarse un ataque desde “Web Stress” (DDos- Attack) los motores de detección de ataque de pfSense deben detectar ataque y generar un log. |
| Historia de usuario | HU-PA03 |
| Pre-condición | * Haber ingresado en forma correcta al Firewall pfSense. * Ingresar con las credenciales correctas a Firewall. * Levantar herramienta “Web Stress” (DDos-Attack). |
| Pasos | * Seleccionar el menú principal de Firewall pfSense. * Ejecutar herramienta “Web Stress”: * Ingresar IP de la victima y cantidad de Thread. * Hacer clic en el botón “Run” * Visualizar widget de logs y verificar la cantidad de logs que se gatillan. |
| Resultado esperado | Que el widget de log genere una alta cantidad de detecciones del ataque que se esta realizando, debieran aparecer logs del tipo:   * Snort * Barnyard2 * nginx |

|  |  |
| --- | --- |
| **Serie** | **SP6 – HU-PA09** |
| Nombre de la prueba | Despliegue de sitio web “Ciberdefensa UNAB” |
| Tipo de prueba | Prueba unitaria |
| Resumen objetivo | Al generar cargar sitio web, este debe desplegar una estructura referente a Ciberdefensa. |
| Historia de usuario | HU-PA09 |
| Pre-condición | * Haber creado un sitio web en el Subdominio Wordpress de la Universidad. |
| Pasos | * Seleccionar http://ciberdefensa.informatica-unab-vm.cl/ * Hacer clic sobre “Quienes somos” y que pagina redirija. * Hacer clic sobre “Contacto” y que redirija a los datos de contacto. * Deslizarse hacia abajo del sitio y visualizar “Características / Servicios” y “Nuestro equipo”. |
| Resultado esperado | Que el sitio muestre o despliegue:   * Sitio “Ciberdefensa Unab” * Que muestre “Quienes somos” y “Contacto” * Visualizar “Características/Servicios” y “Nuestro Equipo” |

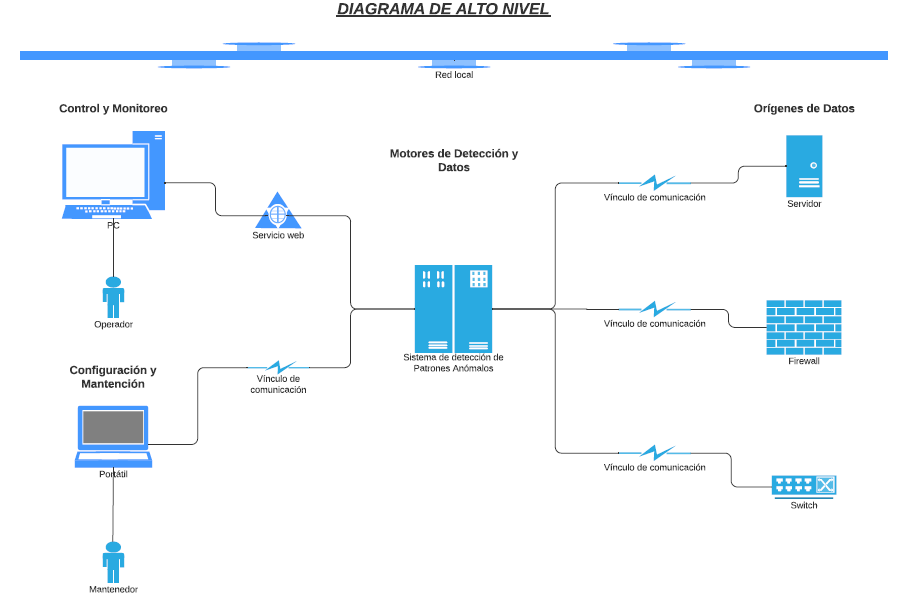
|  |  |
| --- | --- |
| **Serie** | **SP7 – HU-PA09** |
| Nombre de la prueba | Autoevaluación de Seguridad TI, genera desde sitio web “Ciberdefensa UNAB”. |
| Tipo de prueba | Prueba unitaria |
| Resumen objetivo | Al seleccionar la opción de “Autoevaluación” esta debe comenzar con la Autoevaluación de la Pyme. |
| Historia de usuario | HU-PA09 |
| Pre-condición | * Estar dentro del sitio web “Ciberdefensa Unab”. * Ingresar con las credenciales correctas sitio web. |
| Pasos | * Seleccionar el menú superior la opción “Autoevaluación”. * Completar los datos solicitados (Nombre y Correo electrónico) * Completar el total de la encuesta y enviar datos. * Hacer clic en el botón “Submit” |
| Resultado esperado | Que las preguntas se vayan presentando una a una, de acuerdo al avance y respuesta a cada una de estas. |

|  |  |
| --- | --- |
| **Serie** | **SP8 – HU-PA09** |
| Nombre de la prueba | Entrega de recomendación de acuerdo al nivel de seguridad de la Pyme |
| Tipo de prueba | Prueba unitaria |
| Resumen objetivo | Al seleccionar el envío de la “Autoevaluación”, se despliegue una recomendación de Seguridad. |
| Historia de usuario | HU-PA09 |
| Pre-condición | * Estar dentro del sitio web “Ciberdefensa Unab”. * Ingresar con las credenciales correctas sitio web. * Haber realizado en forma correcta la “Autoevaluación” |
| Pasos | * Hacer clic en el botón “Submit” * Posterior a esto verificar y leer recomendaciones de seguridad. |
| Resultado esperado | Que posterior al envío de la “Autoevaluación”, se despliegue en forma automática una ventana con una recomendación de seguridad, esto de acuerdo al nivel obtenido en la encuesta realizada. |

|  |  |
| --- | --- |
| **Serie** | **SP9 – HU-PA09** |
| Nombre de la prueba | Detección de ataques a través de modulo de Machine Learning |
| Tipo de prueba | Prueba unitaria |
| Resumen objetivo | Modulo de Machine Learning debe ser capaz de detectar ataques generados en sistema. |
| Historia de usuario | HU-PA07 / HU-PA05 |
| Pre-condición | * Haber creado modulo de machine Learning. * Tener integrado el modulo de Machine Learning con Graylog. |
| Pasos | * Se debe abrir herramienta “Web Stress” y generar ataques sobre objetivo. * Se debe ejecutar modulo de Machine Learning en equipo víctima. * Visualizar Histograma en Graylog. |
| Resultado esperado | Categorización de amenazas a través de modulo de Machine Learning con Graylog. |

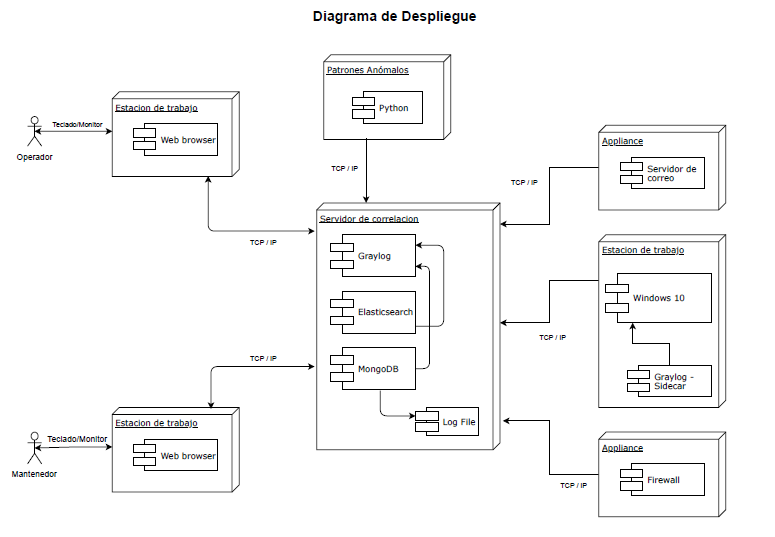
## Arquitectura

1. **Diseño de Alto Nivel**

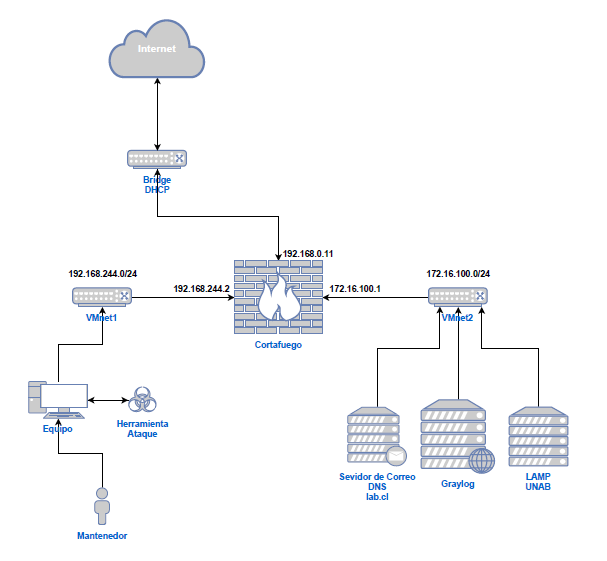


**Ilustración 8: Diagrama de Alto Nivel**

1. **Diagrama de Despliegue**



**Ilustración 9: Diagrama de Despliegue**



**Ilustración 10: Arquitectura del Laboratorio proyecto**

## Resultados

Con el objeto de implementar este laboratorio, tomaremos como caso de prueba una clínica particular, la cual tiene una red interna establecida; pero no tiene sistemas de seguridad en sus computadores y no cuenta con equipos perimetrales de contención (Por ej. cortafuegos).

A continuación se le indicara al encargado de redes como desplegar este sistema.

1. En primer lugar debemos descargar los archivos alojados en el siguiente Drive (demora bastante la descarga, considerar que son app 14 kb en total):

https://drive.google.com/open?id=1A38iMwh4PAiq0uZ25KOAOY5woKr-csHv

2. Posterior a esto o en paralelo debemos realizar es tener dentro de donde se administraran las maquinas virtuales el “Vmware Work Station”.

3. Luego hacemos doble click y cargamos la maquina virtual de “Graylog\_Unab” y la maquina virtual de “Mail\_Server\_Unab”. Dejamos de que ambos procesos de instalación y asociación terminen en su totalidad.

4. Debemos asignar IP´s del mismo segmento de red a ambas maquinas virtuales, esto con el objeto de que ambas se puedan visualizar e intercambiar datos.

5. Posterior a esto, encendemos las 2 maquinas virtuales “Graylog\_Unab” y “Mail\_Server\_Unab”, dejamos de que ambas maquinas finalicen su proceso de encendido.

6. Luego ingresamos a “Graylog\_Unab” a través del usuario “jonathan”, en donde la password es “Temerac2018”.

7. Estando dentro de esta abriremos una ventana terminal.

8. A través del comando “ifconfig” consultamos direccionamiento de red.

9. Tomamos nota de la ip que aparece en ens33 “inet addr: 192.168.203.137” (en este caso), ya que esta debemos reemplazarla en el archivo que detallaremos mas adelante.

10. Posterior a esto nos dirigimos al archivo de configuración de Graylog, con el siguiente comando # sudo nano /etc./Graylog/server/server.conf. Ingresaremos nuevamente la pass “Temerac2018”.

11. Visualizaremos siguiente archivo, en donde nos debemos dirigir a “http\_”, esto lo podemos hacer mas rápido a través de “ctrl + w” y tipeamos “http\_bind\_address”, aquí debemos reemplazar el valor con la ip que habíamos copiado anteriormente (xxx.xxx.xxx.xxx:9000). Posterior a este cambio “ctrl + o” y enter para guardar.

12. Dentro del mismo archivo y con las teclas “ctrl + w” tipeamos “email transport” y enter, llegando a esta sección del archivo, debemos configurar la misma ip anterior, tal como se ve en la siguiente figura.

13. En la sección recién vista del archivo (#Email transport), también se efectúa la configuración del servidor de correo (dominio @lab.cl), con el cual se establecerá la comunicación, en este caso la configuración ya esta realizada y solo se debe cambiar la ip de la Uri, de acuerdo a lo solicitado en el pto. 11. Posterior a esto presionamos “ctrl + o” y enter para guardar, luego “ctrl + x” para salir.

14. Posterior a esto reiniciamos el correlacionador, con el comando

#sudo systemctl restart graylog-server

15. Ahora instalaremos y configuraremos Graylog-Sidecar (agente) en un equipo(s) Windows, lo primero que haremos en equipo Windows será ejecutar el archivo graylog\_sidecar\_installer\_1.0.2-1, el cual estará junto a las maquinas virtuales, dejamos que el proceso de instalación termine.

16. Posterior a esto buscamos CMD y lo ejecutamos como “administrador”.

17. Estando dentro de CMD vamos al archivo de configuración de Graylog-Sidecar, con el siguiente comando notepad.exe C:\Program Files\Graylog\sidecar\sidecar.yml. Aquí seteamos la dirección ip de Graylog\_Unab en la línea server\_url: http://xxx.xxx.xxx.xxx:9000/api, como aprece en la figura de abajo. Luego “ctrl + g” para guardar y cerramos el archivo.

18. Creamos un API Token para este input desde System/Autenthication aquí seleccionamos provider setting del panel izquierdo y le damos un nombre al nuevo Token, posterior a esto lo copiamos y reemplazamos en este archivo ya editado de configuración de Graylog\_Sidecar.

Nota: Ya hay creado un Api Token “Windows\_Token\_Sidecar\_Unab”, también se puede copiar este y reemplazar en el archivo ya editado.

server\_api\_token: "d52sfsoiridmrk8ju25q2s1u2p93flm9qmv1okm2qt802nn1noj" (Token ejemplo).

19. Luego dentro de CMD ejecutamos siguientes comandos:

"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service install

"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service start

En el caso de que el proceso estuviera corriendo, ejecutamos:

"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service stop y luego:

"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service start

20. Luego ingresamos a Graylog http://ipa.ddr.ess.ss:9000/ y nos dirigimos a System/Sidecard/Configuration y en el archivo de configuración en host seteamos la ip de Graylog\_Unab, como muestra la figura de abajo (hosts: ["ipa.ddr.ess.sss:5044"]) (en este caso es esa ip).

21. Luego abajo le damos “Update”.

22. Posterior a estos nos dirigimos a “Alertas”, menú que se encuentra en el panel superior y vamos a “Notifications”, luego en “Alerta de seguridad” le damos click a “More actions” y le damos a “edit”.

23. Debemos dejar siguiente configuración, en E-mails receivers dejaremos la cuenta jonathan@lab.cl que es el receptor y una de las cuentas configuradas en el servidor de correo “Mail\_Server\_Unab”, le damos “Save” con la cual guardaremos dicha configuración.

24. Ahora instalaremos en otros equipo (Que seria el equipo donde efectuare el monitoreo y donde recibiré los correos) un gestor de correo, las pruebas e implementación se realizaron con Thunderbird, posterior a la instalación configuraremos 2 cuentas de correos en este gestor, de acuerdo a siguiente detalle:

**Cuenta 1.**

Nombre: jonathan@lab.cl

**Cuenta 2.**

Nombre: graylog@lab.cl

Ambas cuentas deben que configuradas de acuerdo a las figuras (figura 1 – figura 2) de mas abajo.

Se debe tener presente para ambas cuentas:

a) Your name: El que desee.

b) Email address: jonathan@lab.cl (cuenta 1) y graylog@lab.cl (cuenta 2).

c) Password: test2020

d) Server hostname: Es la dirección ip del servidor de correo “Mail\_Server\_Unab”.

e) Puerto IMAP: 143

f) Puerto SMTP: 25

25. Posterior a esto nos vamos a la maquina “Graylog\_Unab” y seteamos como DNS de esta la direccion ip del servidor de correo “Mail\_Server\_Unab”, también como se muestra en las figuras siguientes se recomienda dejar direccionamiento IP en “Manual” y setera mismos datos ya asignados (#ifconfig).

26. Objeto ver si configuración esta correcta y las alertas (correos) quedaron bien seteados, nos dirigimos a “Alert”, dentro de este nos vamos a “Notifications” y buscamos la alerta configurada que lleva por nombre “Alerta de Seguridad”, aquí hacemos click en el boton “Test”, si esta todo bien nos debiera llegar un correo a la cuenta jonathan@lab.cl.

27. Mientras usted se encuentra trabajando en otras actividades frente al computador, las notificaciones deben aparecer como pop-up.

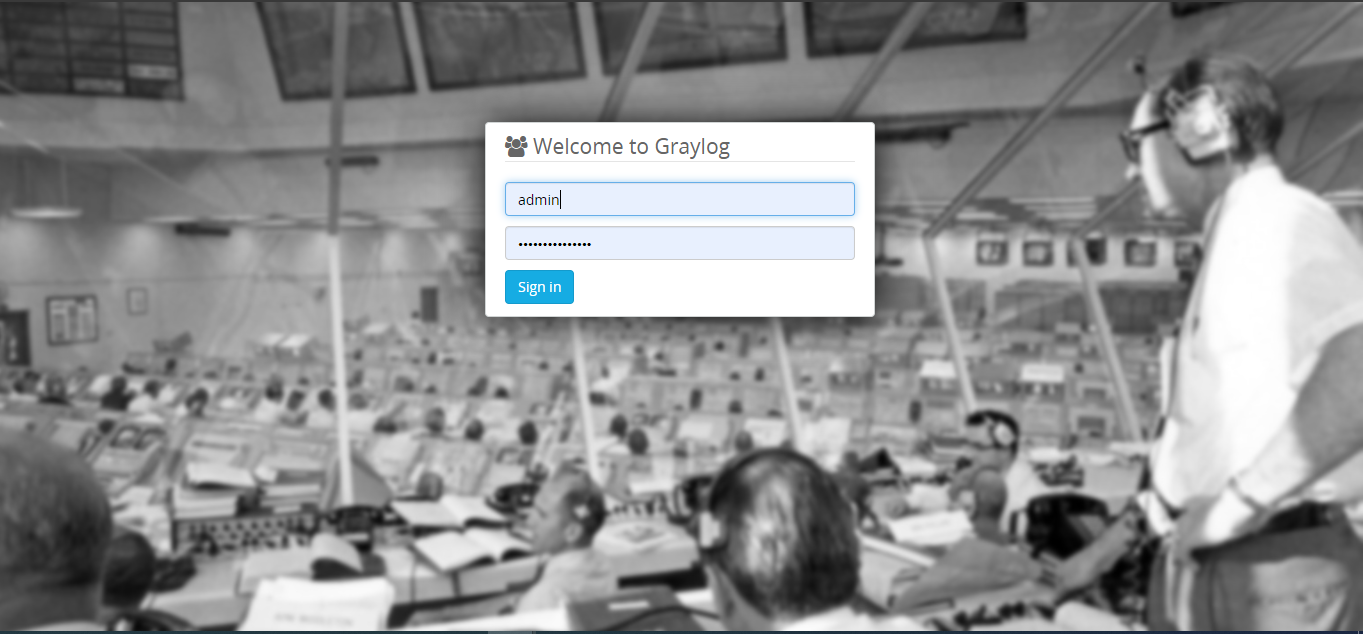
28. Respecto al servidor de correo “Mail\_Server\_Unab”, las credenciales para ingresar son las siguientes:

User: root / Pass: test

User:test / Pass:test

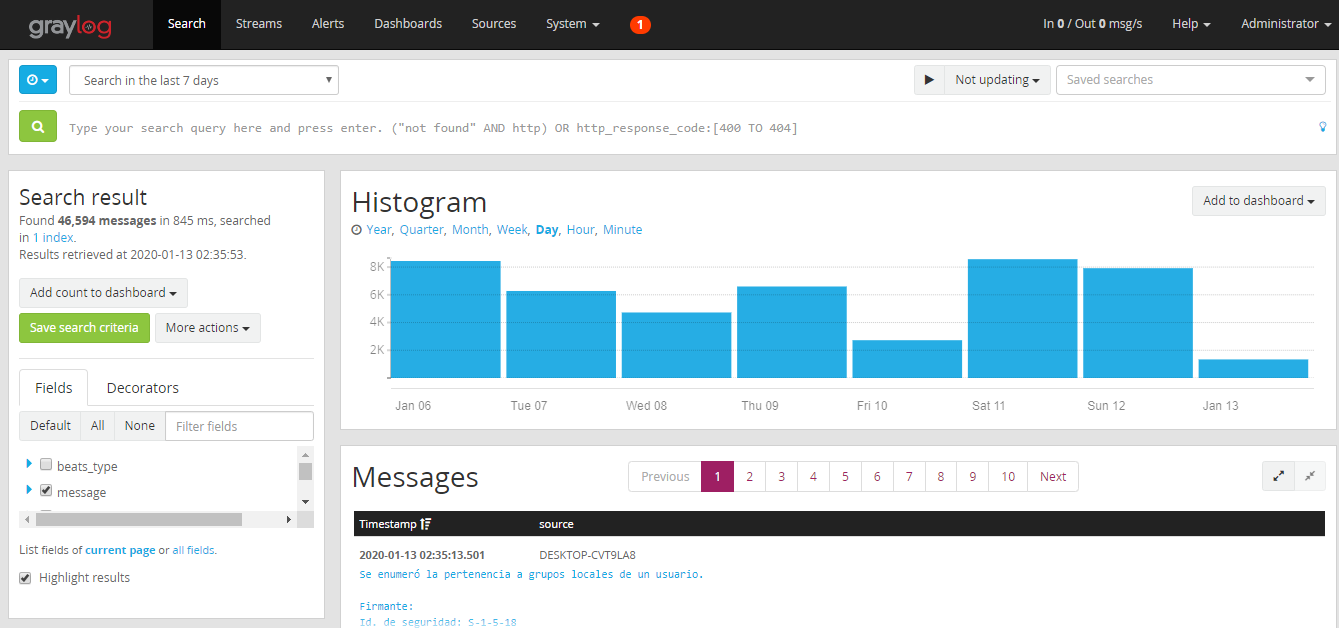
29. En el caso de que servidor de correo presente problemas, se debe verificar a través del comando #nano etc/bind/db.lab.cl que las ip´s que tiene configuradas son las asignadas (misma ip del servidor de correo).

A continuación se despliega la visualización del sistema de correlación.



**Ilustración 11: Ingreso a Graylog**

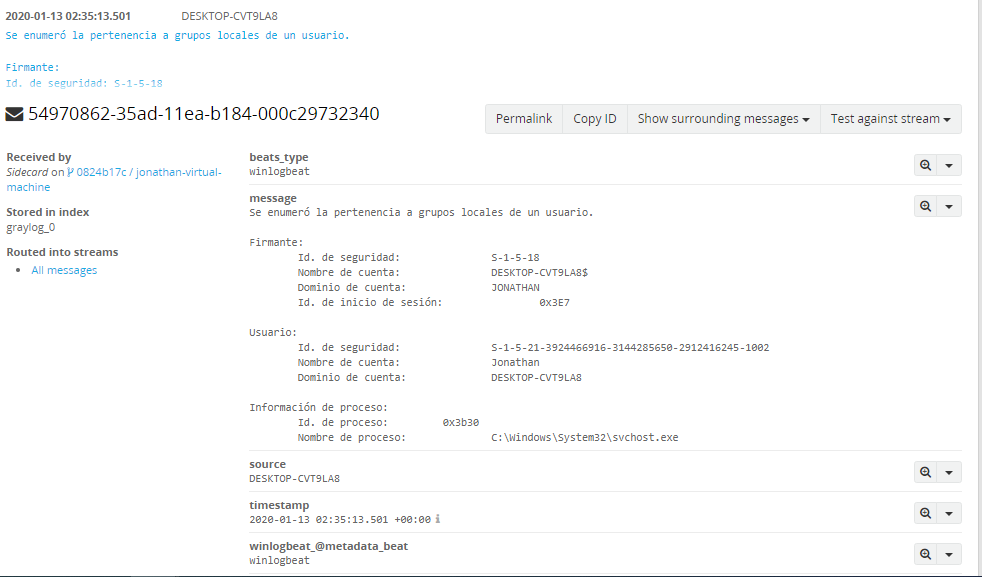
Esta es la visualización que debemos ver para hacer ingreso al correlacionador de eventos Graylog, con las credenciales entregadas.



**Ilustración 12: Histograma**

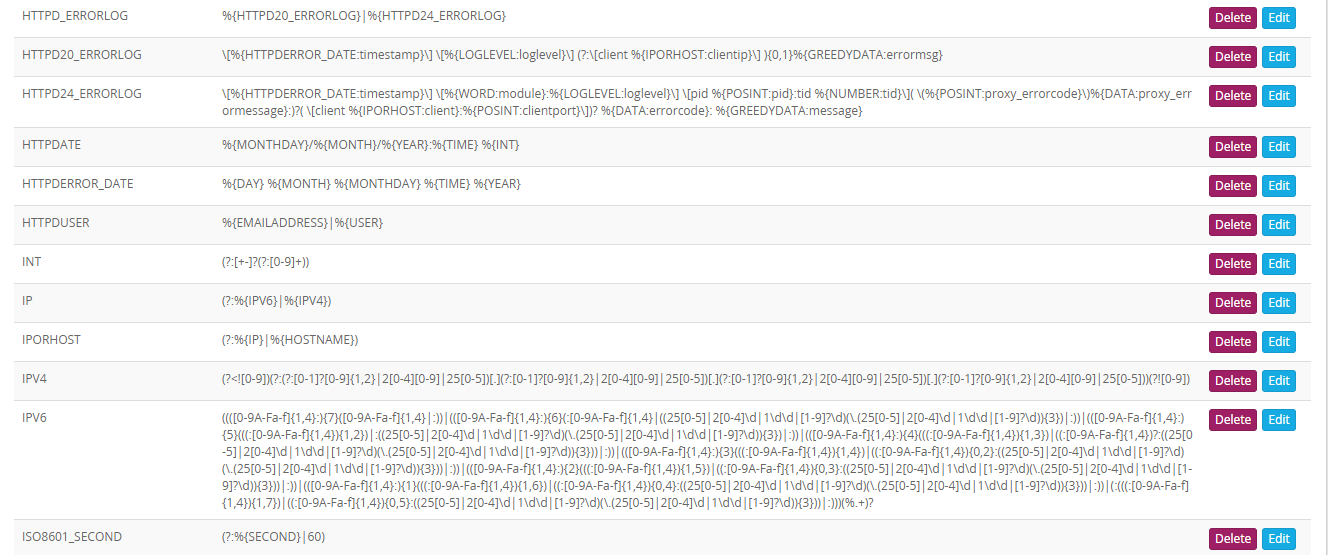
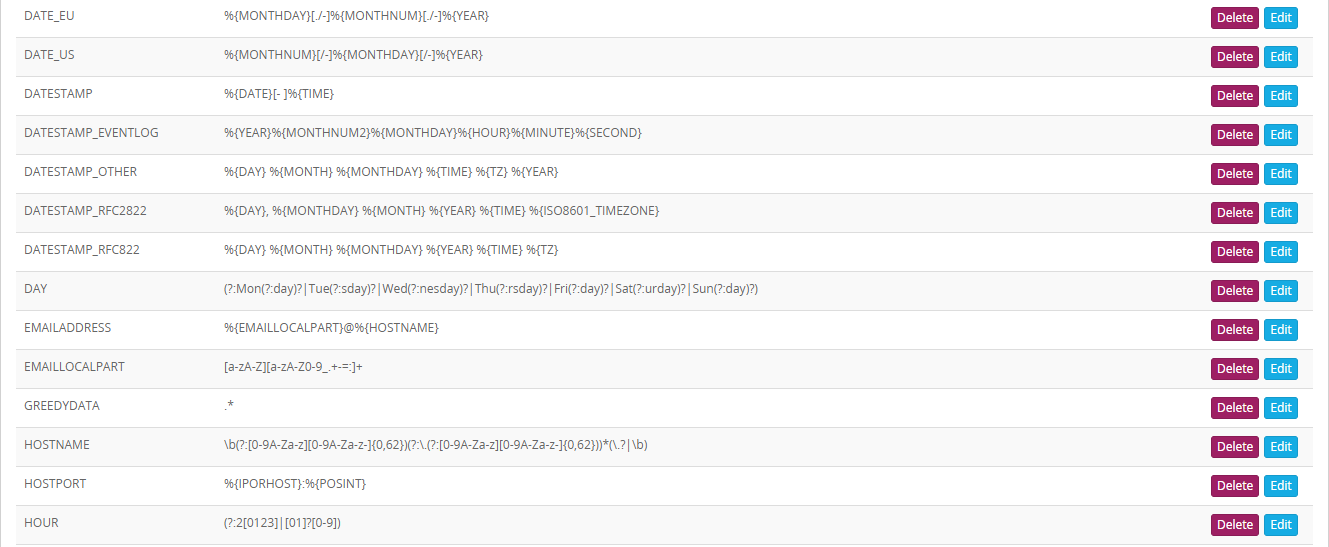
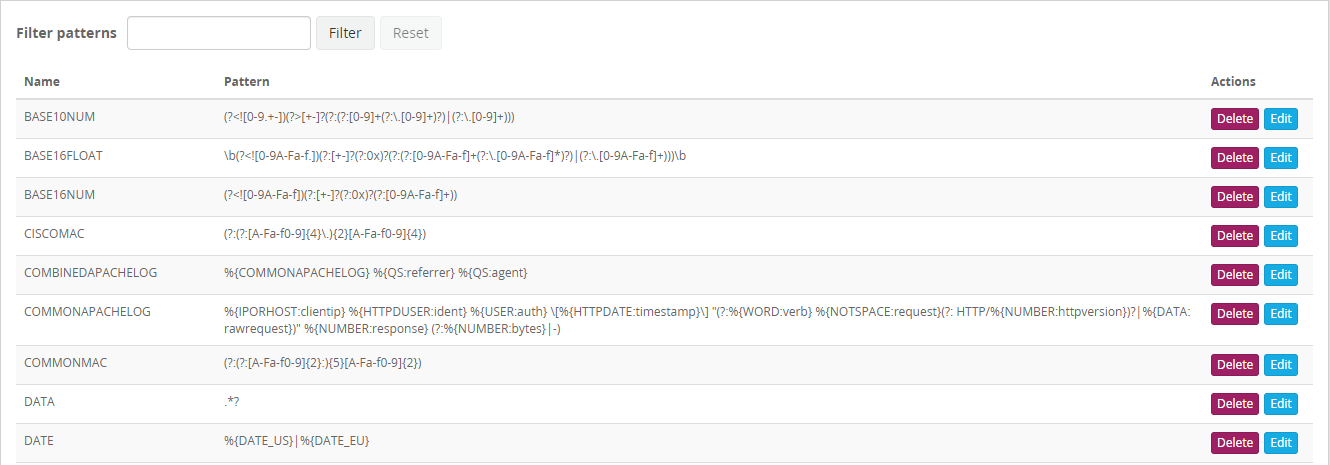
Una de las primeras visualizaciones que tendremos es esta en donde podemos ver el Histograma, en donde se pueden apreciar los eventos que están ingresando al sistema.

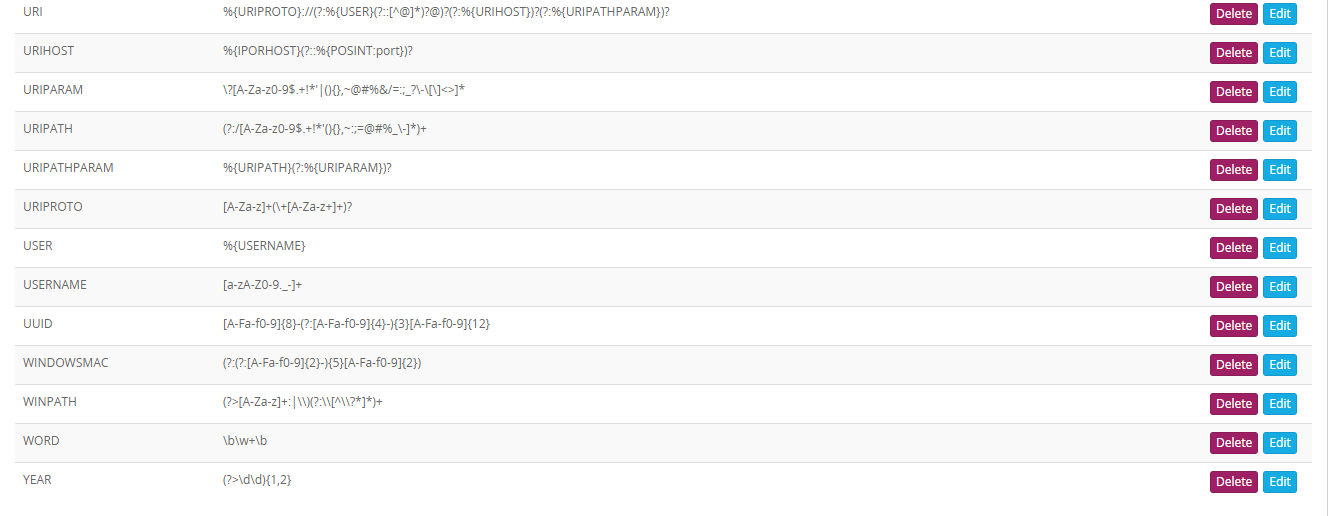
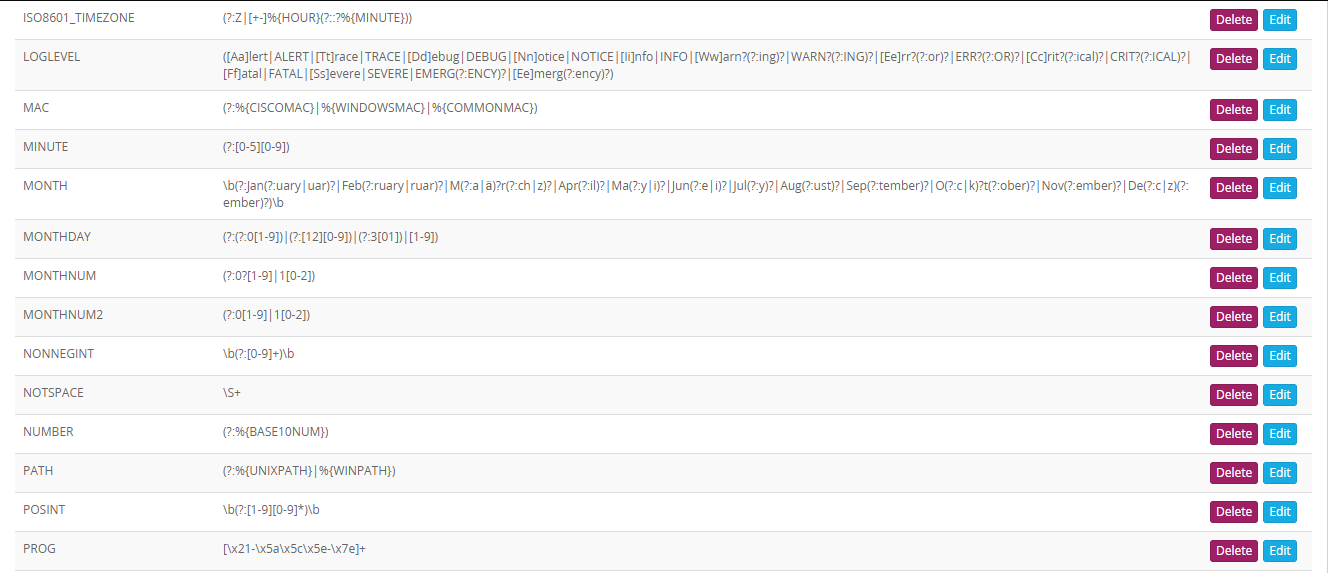
En el costado derecho podemos visualizar la cantidad de eventos recolectada y la cantidad de tiempo empleada en esta, lo cual nos hace ver que efectivamente el flujo de datos es considerable.



**Ilustración 12: Desglose del Log**

Si hacemos clic sobre uno de los eventos que se encuentran bajo el Histograma, notaremos que se despliega este evento y se pueden visualizar todos los componentes que forman parte de ese determinado log. Esto quita una gran carga de trabajo a los encargados de Seguridad TI, ya que podemos apreciar de forma rápida y certera quien es el origen del evento, su dominio, dependencia, hora de ocurrencia y otros datos que son de vital importancia para en caso lo requiera mitigar un incidente informático.





**Ilustraciones: Correspondientes a detalle de patrones Grok configurados**

En las imágenes anteriores podemos apreciar un listado de patrones Grok, los cuales nos ayudan a que los extractores de datos Graylog realicen su trabajo de mejor forma.

Graylog también admite la extracción de datos utilizando el popular lenguaje Grok para permitirle utilizar sus patrones existentes.

Grok es un conjunto de expresiones regulares que se pueden combinar con patrones más complejos, lo que permite nombrar diferentes partes de los grupos coincidentes.

Al usar patrones Grok, puede extraer múltiples campos de un campo de mensaje en un solo extractor, lo que a menudo simplifica la especificación de extractores.

Las expresiones regulares simples a menudo son suficientes para extraer una sola palabra o número de una línea de registro, pero si conoce de antemano la estructura completa de una línea, por ejemplo, para un registro de acceso o el formato de un registro de firewall, es ventajoso usar Grok.

## Aseguramiento de calidad

Se mostrará a continuación los casos de estudio que permitieron validar los requisitos funcionales, estas pruebas funcionales fueron realizadas con la versión actual del sistema.

**Versión 1**

|  |  |
| --- | --- |
| **Id/ Caso de prueba** | **Test – Inicio Sesión** |
| **Aspecto/función a probar** | Validar ingreso al sistema. |
| **Datos de entrada** | User = admin  Password = Unab2020\* |
| **Procedimiento** | 1. Se debe abrir navegador y dirigirse a la dirección del sistema. 2. Se debe iniciar sesión con usuario valido. |
| **Prerrequisito** | tener datos almacenados |
| **Resultado esperado** | Ingreso al sistema y visualización de eventos y logs |
| **Resultado actual** | Ingreso al sistema y visualización de eventos y logs |
| **Requisitos validados** | RF1 |

**Versión 1**

|  |  |
| --- | --- |
| **Id/ Caso de prueba** | **Test – Parseo de logs** |
| **Aspecto/función a probar** | Validar el parseo de los logs en sistema. |
| **Datos de entrada** | User = admin  Password = Unab2020\* |
| **Procedimiento** | 1. Se debe abrir navegador y dirigirse a la dirección del sistema. 2. Posterior se debe hacer clic en un logs del sistema y verificar que haya sido parseado (Hora, usuario, nombre, dominio, etc.). 3. Recorrer el log y verificar sus distintos campos. |
| **Prerrequisito** | Tener logs almacenados |
| **Resultado esperado** | Ingreso al sistema y visualización de eventos y logs parseados. |
| **Resultado actual** | Ingreso al sistema y visualización de eventos y logs parseados. |
| **Requisitos validados** | RF2 |

**Versión 2**

|  |  |
| --- | --- |
| **Id/ Caso de prueba** | **Evento gatillado correctamente en el panel de alertas** |
| **Aspecto/función a probar** | Validar el gatillado de los logs en sistema. |
| **Datos de entrada** | User = **Jupiter**  Password = **Sistema1919** |
| **Procedimiento** | 1. Se debe abrir navegador, dirigirse a la dirección del sistema e iniciar sesión. 2. Posterior se debe hacer clic en los logs de inicio de sesión. 3. Debe mostrar inicio de sesión fallido.. |
| **Prerrequisito** | Haber ingresado en forma correcta al sistema.  Tener logs almacenados en el sistema. |
| **Resultado esperado** | Ingreso al sistema y visualización de eventos y logs de falla de ingreso. |
| **Resultado actual** | Ingreso al sistema y visualización de eventos y logs de falla de ingreso. |
| **Requisitos validados** | RF4 |

**Versión 2**

|  |  |
| --- | --- |
| **Id/ Caso de prueba** | **Alerta gatillada sea enviada vía correo electrónico a cuenta dominio @lab.cl** |
| **Aspecto/función a probar** | Validar el envió de alerta vía correo electrónico. |
| **Datos de entrada** | Alerta gatillada por sistema. |
| **Procedimiento** | 1. Se debe abrir navegador y dirigirse a la dirección de Graylog. 2. Posterior a esto se debe iniciar sesión en cuenta [jonathan@lab.cl](mailto:jonathan@lab.cl), credenciales: test / test2020 3. Recorrer el log y verificar sus distintos campos. |
| **Prerrequisito** | Logs gatillados con alerta en Graylog. |
| **Resultado esperado** | Envío y recepción de correo electrónico en cuenta jonathan@lab.cl |
| **Resultado actual** | Envío y recepción de correo electrónico en cuenta jonathan@lab.cl |
| **Requisitos validados** | RF3 |

**Versión 2**

|  |  |
| --- | --- |
| **Id/ Caso de prueba** | **Redireccionamiento a correlacionador de eventos desde URL inserta en cuerpo del correo** |
| **Aspecto/función a probar** | Redireccionamiento hacia correlacionador de eventos. |
| **Datos de entrada** | Link de redireccionamiento en correo electrónico. |
| **Procedimiento** | 1. Se debe abrir gestor de correo y dirigirse a correos recibidos. 2. Posterior esto se debe hacer clic en link inserto en correo electrónico. 3. Visualizar detalles de alerta enviada a través de Graylog. |
| **Prerrequisito** | Tener recibidos correos electrónicos desde Graylog. |
| **Resultado esperado** | Al hacer click en link inserto en correo, este debe redireccionar hacia visualización en Graylog. |
| **Resultado actual** | Al hacer click en link inserto en correo, este debe re direccionar hacia visualización en Graylog. |
| **Requisitos validados** | RF3 |

**Versión 3**

|  |  |
| --- | --- |
| **Id/ Caso de prueba** | **Ataque Web Stress visualizado en el panel de alertas** |
| **Aspecto/función a probar** | Al generar un ataque desde la herramienta “Web Stress” el sistema en base a sus reglas cargadas es capaz de detectar y enviar logs al correlacionador de eventos. |
| **Datos de entrada** | Ataques generados desde herramienta “Web Stress”. |
| **Procedimiento** | 1. Se debe abrir herramienta “Web Stress”, setear el objetivo y lanzar ataque. 2. Posterior a esto se debe abrir el correlacionador de eventos y seleccionar el Histograma. 3. Visualizar detalles de logs de ataque enviados a Graylog. |
| **Prerrequisito** | Generar ataques desde “Web Stress” hacia objetivo de ataque. |
| **Resultado esperado** | Visualizar logs de ataque en el Histograma de Graylog. |
| **Resultado actual** | Visualizar logs de ataque en el Histograma de Graylog. |
| **Requisitos validados** | RF4 |

**Versión 3**

|  |  |
| --- | --- |
| **Id/ Caso de prueba** | Alerta gatillada detectada por motores en Firewall “pfSense” |
| **Aspecto/función a probar** | Al generarse un ataque desde “Web Stress” (DDos- Attack) los motores de detección de ataque de pfSense deben detectar ataque y generar un log. |
| **Datos de entrada** | Ataques generados desde herramienta “Web Stress” |
| **Procedimiento** | 1. Se debe abrir visualización de pfSense y verificar eventos detectados. 2. Posterior a esto verificar que motores snort detecten ataques. 3. Verificar que el log del ataque se encuentre en sistema. |
| **Prerrequisito** | Tener reglas snort configuradas en pfSense. |
| **Resultado esperado** | Visualizar y guardar logs de ataques en pfSense. |
| **Resultado actual** | Visualizar y guardar logs de ataques en pfSense. |
| **Requisitos validados** | RF2 |

**Versión 4**

|  |  |
| --- | --- |
| **Id/ Caso de prueba** | Despliegue de sitio web “Ciberdefensa UNAB” |
| **Aspecto/función a probar** | Al generar cargar sitio web, este debe desplegar una estructura referente a Ciberdefensa. |
| **Datos de entrada** | https://cibermadurez.cl |
| **Procedimiento** | 1. Se debe cargar en el navegador la dirección https://cibermadurez.cl. 2. Posterior a esto verificar sitio se despliegue en navegador. 3. Verificar los diferentes botones redirijan hacia donde indican. |
| **Prerrequisito** | Tener creado y montado el sitio cibermadurez. |
| **Resultado esperado** | Visualizar sitio https://cibermadurez.cl |
| **Resultado actual** | Visualización de sitio https://cibermadurez.cl |
| **Requisitos validados** | RF4 |

**Versión 4**

|  |  |
| --- | --- |
| **Id/ Caso de prueba** | Autoevaluación de Seguridad TI, generada desde sitio web “Ciberdefensa UNAB”. |
| **Aspecto/función a probar** | Al seleccionar la opción de “Autoevaluación” esta debe comenzar con la Autoevaluación de la Pyme. |
| **Datos de entrada** | Click en link de “Autoevaluación TI”. |
| **Procedimiento** | 1. Se debe abrir sitio https://cibermadurez.cl. 2. Posterior a esto hacer click en “Autoevaluación TI”. 3. Comenzar a responder preguntas de Autoevaluación. |
| **Prerrequisito** | Tener creado un cuestionario de “Autoevaluación TI”. |
| **Resultado esperado** | Poder realizar la “Autoevaluación TI” montada en sitio https://cibermadurez.cl |
| **Resultado actual** | Se puede realizar la “Autoevaluación TI” |
| **Requisitos validados** | RF4 |

**Versión 5**

|  |  |
| --- | --- |
| **Id/ Caso de prueba** | Detección de ataques a través de modulo de Machine Learning |
| **Aspecto/función a probar** | Modulo de Machine Learning debe ser capaz de detectar ataques generados en sistema. |
| **Datos de entrada** | Ataque generado desde herramienta “Web Stress”.  Ejecución de modulo de Machine Learning. |
| **Procedimiento** | 1. Se debe abrir herramienta “Web Stress” y generar ataques sobre objetivo. 2. Se debe ejecutar modulo de Machine Learning en equipo victima. 3. Visualizar Histograma en Graylog. |
| **Prerrequisito** | Haber creado modulo de machine Learning.  Tener integrado el modulo de Machine Learning con Graylog. |
| **Resultado esperado** | Categorización de amenazas a través de modulo de Machine Learning con Graylog. |
| **Resultado actual** | Categorización de amenazas a través de modulo de Machine Learning con Graylog. |
| **Requisitos validados** | RF1 |

# Todos los requisitos funcionales probados anteriormente, pasaron en su totalidad; por lo tanto estos cumplieron con lo establecido.

# **Conclusiones**

A continuación, se detalla la lección aprendida en estas primeras semanas del proyecto:

La comunicación con el profesor guía es de vital importancia, ya que el nos guía y nos da las directrices para no desviarnos del objetivo del proyecto, a su vez también se debe tener una comunicación constante con el cliente, ya que es él quien el que nos da la primera visión de qué es lo que se necesita desarrollar como solución a una necesidad. Cuando no se realizan las reuniones surgen los problemas de no tener los objetivos bien definidos dificultando todo el proyecto en adelante.

A continuación, se detallan las lecciones aprendidas.

El tema del “Estallido Social” a finales de año y actualmente la pandemia “COVID-19” que nos afecta a nivel mundial, ha provocado que todas las coordinaciones, reuniones, acuerdos, etc. se realicen en forma mas lenta y no con la regularidad esperada.

Sin perjuicio de lo anterior, se estima que se ha logrado el sacar adelante este Sprint en su totalidad.

Coincidiendo con lecciones del sprint 2, se comenta que a raíz de la Pandemia “COVID-19” que nos afecta a nivel mundial, todas las coordinaciones, reuniones, acuerdos, etc. se han realizado en forma no presencial y no con la regularidad esperada.

También se ha aprendido que el mundo de la “Virtualización” es algo que nos puede entregar herramientas robustas para la realización de laboratorios y de PoC (Pruebas de concepto).

Como resumen y en general se estima que se cumplió con todo lo planificado para este Sprint 3.

## Problemas Abiertos

Durante el desarrollo del proyecto me he encontrado con un principal problema, el cual se detalla a continuación

Investigación en el desarrollo de código en Python: Con el objetivo de detectar patrones anómalos en los usuarios de una red, en el transcurso de este proyecto se me ha hecho difícil el confeccionar líneas de código, las cuales lleguen a detectar patrones anómalos desde cero, con esto me refiero a tener un dataset de datos y desde ahí comenzar la detección de comportamientos anómalos. En esto ha sido de vital importancia mi profesora guía, ya que gracias a su labor he podido sortear estos inconvenientes.

Durante el desarrollo del proyecto se han encontrado problemas, los que se detallan a continuación.

Respecto principalmente al tiempo que se debe dedicar a la investigación de como trabajan, configuran, operan y customizan los sistemas Open Source en el área de seguridad. En esto ha sido de vital importancia la profesora guía, ya que gracias a su labor he podido sortear estos inconvenientes.

**Sprint 3:**

Se ha detectado en este Sprint que es de vital importancia para la correcta visualización y parsing de los datos, el dominar la creación y comprensión de expresiones regulares, Patrones Grok y JSON.

Respecto principalmente al tiempo que se debe dedicar a la investigación de como trabajan, configuran, operan y customizan los sistemas Open Source en el área de seguridad.

En esto ha sido de vital importancia la profesora guía, ya que gracias a su labor he podido sortear estos inconvenientes.

**Sprint 4:**

Durante el desarrollo del proyecto se han encontrado problemas, los que se detallan a continuación.

Es muy importante al crear estos sitios web y al incluir en ellos encuestas del tipo Autoevaluación, en las cuales de forma residual quedan datos clasificados o que podrían ser usados para otros fines no estadísticos y que no forman parte de este proyecto (ej.: algún uso malicioso con estos datos); tener bien definidos los “Términos de uso”, objeto toda la información que se entregue sea usada solo para los fines definidos con anterioridad.

En el presente Sprint y como en los anteriores se empleo tiempo en el Autoaprendizaje, esto a raíz de que no se dominaba la creación de paginas web en Wordpress.

El apoyo constante de la profesora guía a sido de vital importancia en la aclaración de dudas y en las directrices correspondientes al Sprint.

## Trabajo Futuro

Como trabajo pendiente quedan la realización de las historias de usuario HU-PA03, HU-PA04, HU-PA05, HU-PA07, HU-PA08; las cuales están consideradas para los siguientes Sprint.

También como trabajo a corto plazo y que debiera entregar una mejor visualización de los eventos cargados en el correlacionador, esta el envío de logs desde distintos dispositivos de red (Firewall, router, switch, Active Directory, etc.).

**Sprint 3:**

Como trabajo pendiente quedan la realización de las historias de usuario HU-PA04, HU-PA05, HU-PA07, HU-PA08, HU-PA09; las cuales están consideradas para los siguientes Sprint.

También como trabajo a corto plazo y con el objeto de entregar una mejor visualización y enriquecimiento de datos (logs) enviados al correlacionador, se debe considerar el crear otros tipos de ataques, con el objetivo de tener una mayor espectro de detecciones.

También se debe considerar el crear parsing detallado de los logs que actualmente se están procesando en el correlacionador de eventos.

**Sprint 4:**

Como trabajo pendiente quedan la realización de las historias de usuario HU-PA04, HU-PA05, HU-PA07, HU-PA08; las cuales están consideradas para los siguientes Sprint.

Se mantiene también como trabajo a corto plazo y con el objeto de entregar una mejor visualización y enriquecimiento de datos (logs) enviados al correlacionador, se debe considerar el crear otros tipos de ataques, con el objetivo de tener una mayor espectro de detecciones.

De igual forma se debe considerar el crear parsing detallado de los logs que actualmente se están procesando en el correlacionador de eventos.

1. **Revisión del Sprint 4**

Al finalizar el sprint 4 se realizó una reunión con el Product Owner, para presentar la liberación de los avances para este sprint.

El objetivo programado para este sprint fue de completar la **HU-PA09** “Quiero implementar un sitio web en donde se de a conocer el trabajo en Ciberdefensa y tenga la capacidad de generar una autoevaluación a las Pymes”**,** la cual se alineo con el objetivo específico **OE4** “Aumentar los tiempos de respuesta ante un incidente informático por parte del personal de Seguridad TI”.

En resumen en este Sprint se logro:

1. Implentar sitio web “Ciberdefensa UNAB”.
2. Confección de Autoevaluación enfocada en Pymes.
3. Generación de recomendación en base a resultados de Autoevaluación.
4. **Análisis Sprint 4**

La creación de este sitio web nos entrego una visión mas clara de como es el ciclo completo de creación de estos sitios web soportados en Wordpress.

Se obtuvieron experiencias asociadas al trabajo con Wordpress y formularios compatibles con este, en este caso el formulario que presento un mejor resultado fue “Quizzes/Surveys”, siempre teniendo en mente que esto es enfocados en las Pymes de la región.

Se mantiene la observación respecto a la pandemia “COVID-19” que nos afecta a nivel mundial, la cual ha provocado que todas las coordinaciones, reuniones, acuerdos, etc. se realicen en forma mas lenta y no con la regularidad esperada.

En resumen, se estima que se ha logrado sacar adelante este Sprint en su totalidad.

**Glosario**

1. TI = Tecnologías de la Información.
2. IA = Inteligencia Artificial.
3. ML = Machine Learning.
4. DOS = Denial of Service.
5. DDOS = Distributed Denial of Service.
6. APT = Advanced Persistant Threath.
7. C&C = Command and Control.
8. DNS = Domain Name Server.
9. PYME = Pequeña y Mediana Empresa.