**ANEXO “A”**

**CAPITULO 4: Resultados y discusión**

**Desarrollo Sprint 1**

1. **Objetivo del sprint**

En este Sprint se cubrirá el objetivo específico **OE5** “Aumentar o generar la visualización de los diferentes logs que circulan por una red, a través de un sistema de correlación de eventos”.

Al implementar las historias de usuario **HU-PA01** y **HU-PA06**. Donde se implementará un sistema de correlación de eventos, el cual permitirá la visualización y monitoreo de los diferentes logs que circulan por una red informática.

1. **Product Backlog**

A continuación, se presenta el Product Backlog completo para el Proyecto, este se encuentra priorizado con la técnica MoSCoW y la asignación de los puntos de historia con la estimación de serie Fibonacci.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | 10 | 5 |
|  | - |  |  |  |  |  |
| HU-PA03 | Como  operador | Quiero determinar a través de los paneles cual es un incidente informático. | Para poder discriminar entre un incidente y un falso positivo. | M | 8 | 4 |
|  | - |  |  |  |  |  |
| 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 | 10 | 3 |
|  | - |  |  |  |  |  |
| HU-PA05 | Como  administrador | Quiero poder customizar patrones de detección en base a requerimientos. | Para poder detectar lo desconocido en la red. | M | 11 | 2 |
|  | - |  |  |  |  |  |
| 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 | 10 | 1 |
|  | - |  |  |  |  |  |
| HU-PA07 | Como  administrador | Quiero implementar un sistema que logre detectar patrones anómalos de comportamiento. | Para entregar una mejor visualización a los encargados de Seguridad TI. | M | 18 | 7 |
|  | - |  |  |  |  |  |
| HU-PA08 | Como  administrador | Quiero crear reglas de detección de patrones anómalos de comportamiento. | Para poder detectar comportamientos anómalos en la red. | M | 16 | 6 |

**Tabla 4.1: Product Backlog**

1. **Sprint Backlog**

La siguiente tabla representa el Sprint Backlog planificado para el primer sprint, donde se asigna la estimación de horas de trabajo necesarias para completar cada tarea.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sprint #** | **1** | **Días Inicio Sprint** | **0** | **Inicio Puntos de Historia** | **45** |
| **Fecha de Inicio** | **09-12-2019** | **Días Termino Sprint** | **21** | **Término Puntos de Historia** | **0** |

|  |  |  |
| --- | --- | --- |
| **ID Tarea** | **Descripción** | **Estimación Inicial** |
| HU-PA01.T1 | Investigar que es una anomalía en la red. | 3 |
| HU-PA01.T2 | Setear el panel apropiado para esta visualización. | 3 |
| HU-PA01.T3 | Efectuar comprobación de anomalía en el equipo que la este reportando. | 2 |
| HU-PA06.T1 | Investigar como agregar nuevos dispositivos y funcionalidades a sistema. | 3 |
| HU-PA06.T2 | Implementar correlacionar de eventos y configurar la agregación de data source al sistema. | 8 |
| HU-PA06.T3 | Efectuar pruebas entre correlacionador y nuevo equipo ingresado. | 2 |
| HU-PA09.T1 | Coordinar Horario con profesor Guía Asistir a reunión y mostrar avances o realizar consultas Coordinar requerimientos de Product Owner Actualizar bitácora de reuniones | 2 |
| HU-PA10.T1 | Coordinar Horario con Cliente Asistir a reunión y mostrar avances o realizar consultas Coordinar requerimientos de Product Owner Actualizar bitácora de reuniones | 2 |
| HU-PA11.T1 | \_ Actualizar el Plan del Proyecto de Control de Cambios \_ Actualizar el Plan del Sprint \_ Integrar Plan del Sprint al Anexo de la Memoria | 2 |
| HU-PA12.T1 | \_ Actualizar el Plan del Proyecto de Control de la Configuración \_ Actualizar el Plan del Sprint \_ Integrar Plan del Sprint al Anexo de la Memoria | 2 |
| HU-PA13.T1 | \_ Actualizar el Plan del Proyecto Plan de Calidad \_ Actualizar el Plan del Sprint \_ Integrar Plan del Sprint al Anexo de la Memoria | 2 |
| HU-PA14.T1 | \_ Actualizar el Plan del Proyecto de Gestión de Riesgos \_ Actualizar el Plan del Sprint \_ Integrar Plan del Sprint al Anexo de la Memoria | 2 |
| HU-PA15.T1 | \_ Actualizar el Plan del Proyecto del Cronograma \_ Actualizar el Plan del Sprint \_ Integrar Plan del Sprint al Anexo de la Memoria | 2 |
| HU-PA16.T1 | Subir Códigos del entregable a GitHub, comentar los Commit o Branch y Documentar | 2 |
| HU-PA17.T1 | Realizar todas las pruebas necesarias para que el entregable quede sin errores y funcionando en producción, luego generar el Release en GitHub, asignar un TAG y documentar | 2 |
| HU-PA18.T1 | Entregar el documento al Cliente, para que tome conocimiento de todos los atributos o requisitos que se consideraron en el entregable, e indique si tiene observaciones | 2 |
| HU-PA19.T1 | Reunir todas las evidencias de avance del Sprint y redactar el Documento enfocándose en todos los puntos de la Pauta de corrección | 2 |
| HU-PA20.T1 | Reunir todas las evidencias de avance del Sprint y redactar el PowerPoint enfocándose en todos los puntos de la Pauta de corrección | 2 |

**Tabla 4.2: Sprint backlog**

1. **Duración del sprint**

Se establece que la duración para cada Sprint será de 3 semanas, el inicio de este será el día 09 de diciembre de 2019 y terminará el día 29 de diciembre de 2019.

1. **Criterios de aceptación**

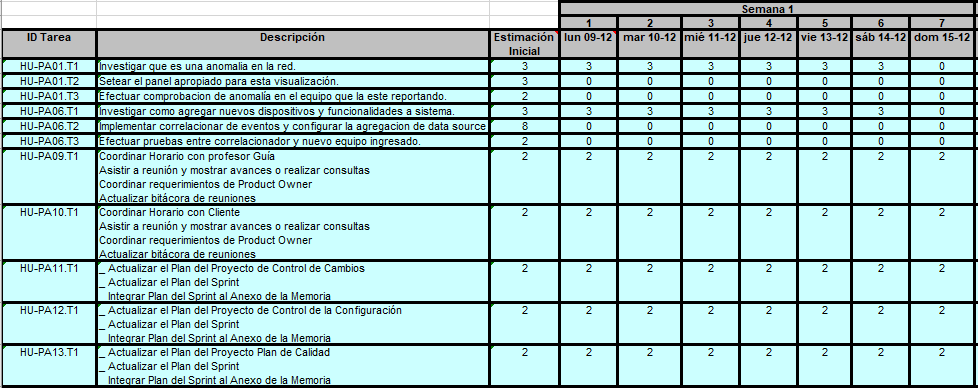
A continuación, se presentan los criterios de aceptación para las HU-PA01 y HU-PA06 que se desarrollaran en el Sprint 1.

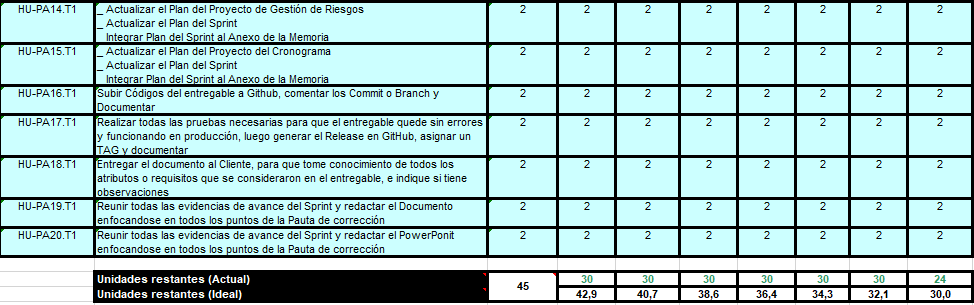
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CRITERIOS DE ACEPTACIÓN** | | | | | |
| **Número de**  **escenario** | **Criterio de aceptación (Título)** | **Contexto** | **Evento** | **Resultado / Comportamiento esperado** | **Estado** |
|  |  |  |  |  |  |
| E1 | HU-PA01.T3.E1 - Visualización 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-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 % |

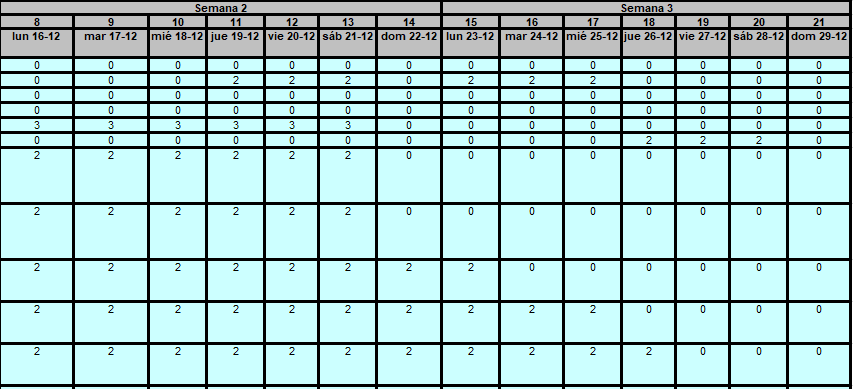
**Tabla 4.3: Criterios de aceptación**

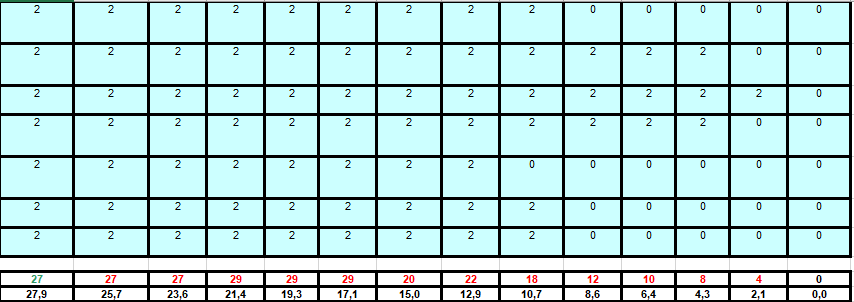
1. **Seguimiento para Sprint 1**

1. **Sprint Planning**









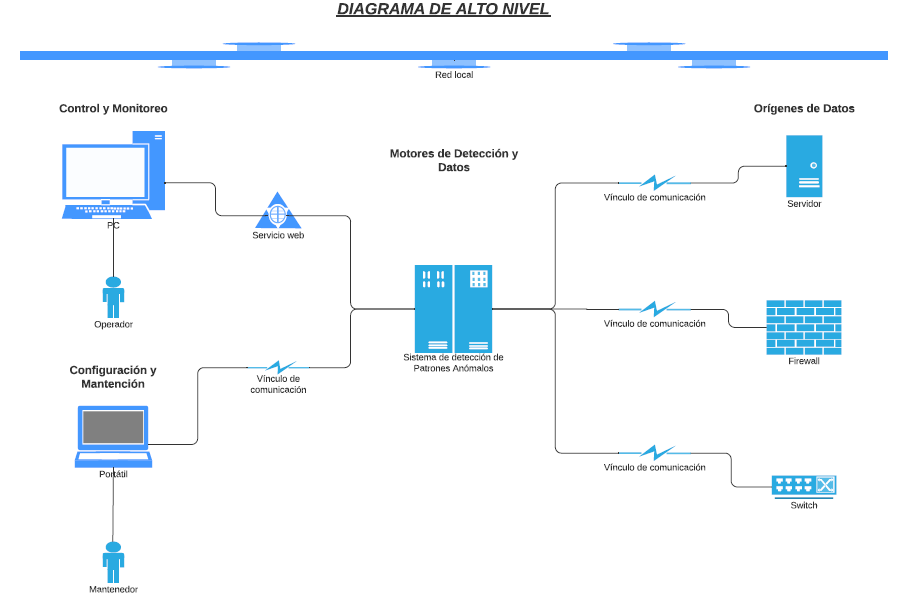
**Tabla 4.4: Seguimiento de sprint 1 backlog**

1. **Sprint 1 Burn Down Chart**

**Figura 4.5: Burn down chart**

1. **Arquitectura de la aplicación**

1. **Diagrama de Alto nivel**



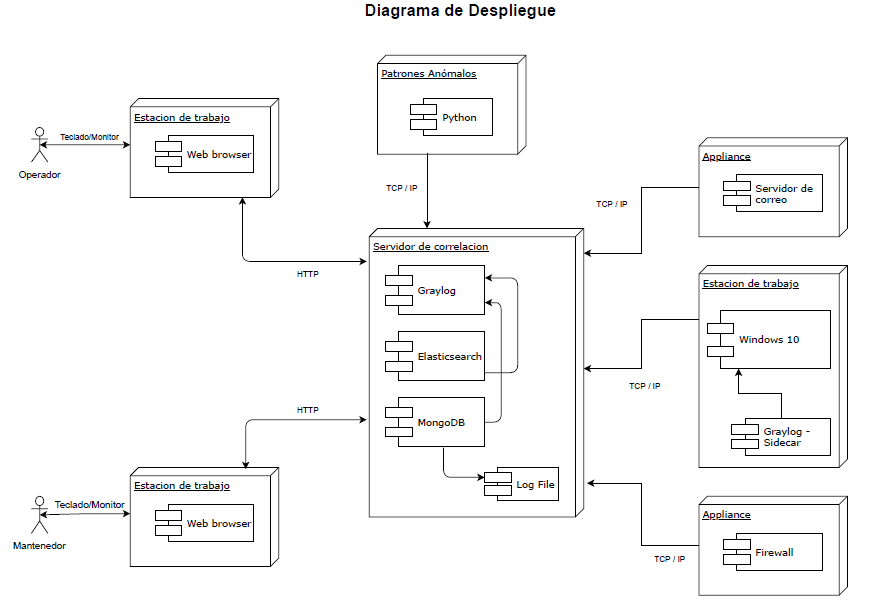
**Figura 4.6: Diagrama de Alto Nivel**

En la figura 4.6 se muestra el diagrama de Alto Nivel para la implementación del sistema, aquí podemos ver en forma macro 4 componentes o grupos de trabajo vistos desde bien arriba, los cuales son:

* **Control y monitoreo:**Este componente del diagrama esta destinado para el operador del sistema (Seguridad TI), será el encargado de monitorear, detectar y mitigar los posibles eventos informáticos que se originen.

* **Configuración y mantención:** Esta sección esta destinada al mantenedor, el cual tendrá la labor de dejar implementado y operando en forma optima todo el sistema.
* **Motores de detección y datos:** En este componente se encuentran los principales componentes del sistema, sus motores de correlación, bases de datos, motores de búsqueda, motores de parseo, etc. aquí es donde se realiza la ardua labor de parsear y customizar los diferentes ingresos de datos. Todo esto con el objetivo de entregar una mejor visualización al operador.
* **Orígenes de datos:** Estos son los componentes encargados de alimentar a este gran sistema y a su vez también son los interesados en que sus comportamientos sean monitoreados. Debemos tener en cuenta que gran parte de estos logs nunca son observados, entonces con este sistema podremos ver efectivamente que es lo que sucediendo en segundo plano.

1. **Diagrama de despliegue**



**Figura 4.7: Diagrama de Despliegue**

En la figura 4.7 se muestra el diagrama de Despliegue para la implementación del sistema, en donde podemos observar lo siguiente:

* **Estación de trabajo Operador:**Aquí la comunicación e interacción con el sistema se realiza a través del protocolo http y por el puerto 9000, puerto que utiliza el correlacionador para poder interactuar con su interfaz de visualización.

* **Estación de trabajo Mantenedor:** Aquí la comunicación e interacción entre los distintos módulos que componen el sistema se realiza a través de:

- ssh (puerto 22)

- Vmware Vsphere Client maquinas Ubuntu 16.04 virtuales.

- Teamviewer para servidor Ubuntu alojado en red UNAB.

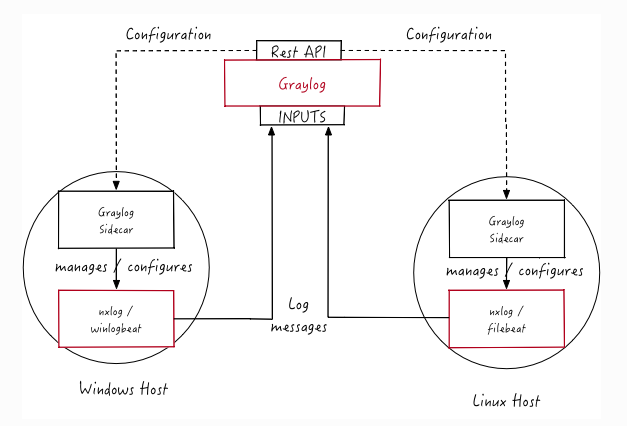
- Protocolo http, puerto 9000.

* **Servidor de correlación:** En este servidor Ubuntu 16.04 LTS, se encuentran alojados los siguientes módulos:
* Graylog, correlacionador de eventos (Orquestador).
* Elasticsearch, sistema de almacenamiento de trazas.
* MongoDB, base de datos de configuración.
* **Orígenes de datos:** Los diferentes orígenes de datos enviar sus logs directamente a este correlacionador de eventos o también a través de intermediarios que en algunos casos son llamados agentes.

Implementación en laboratorio 316 UNAB:

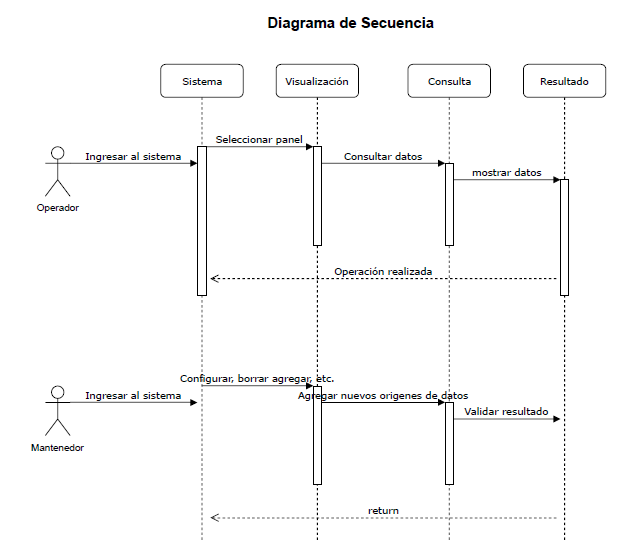
Aquí se utilizaron 5 equipos Windows 10 y se implemento Graylog-Sidecar en cada uno de ellos.

**Graylog Sidecar** es un sistema de administración de configuración para diferentes recolectores de registros, también llamado Backends . Los nodos Graylog actúan como un concentrador centralizado que contiene las configuraciones de los recolectores de registros. En los dispositivos / hosts compatibles, Sidecar puede ejecutarse como un servicio (host de Windows) o daemon (host de Linux).



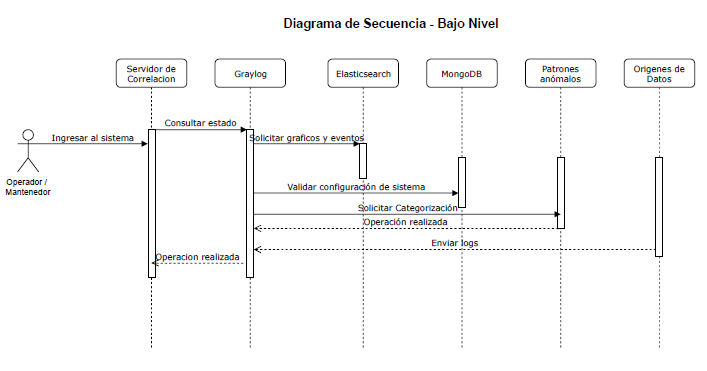
**Figura 4.8: Diagrama Graylog-Sidecar**

1. **Diagrama de secuencia**



**Figura 4.9: Diagrama de secuencia**

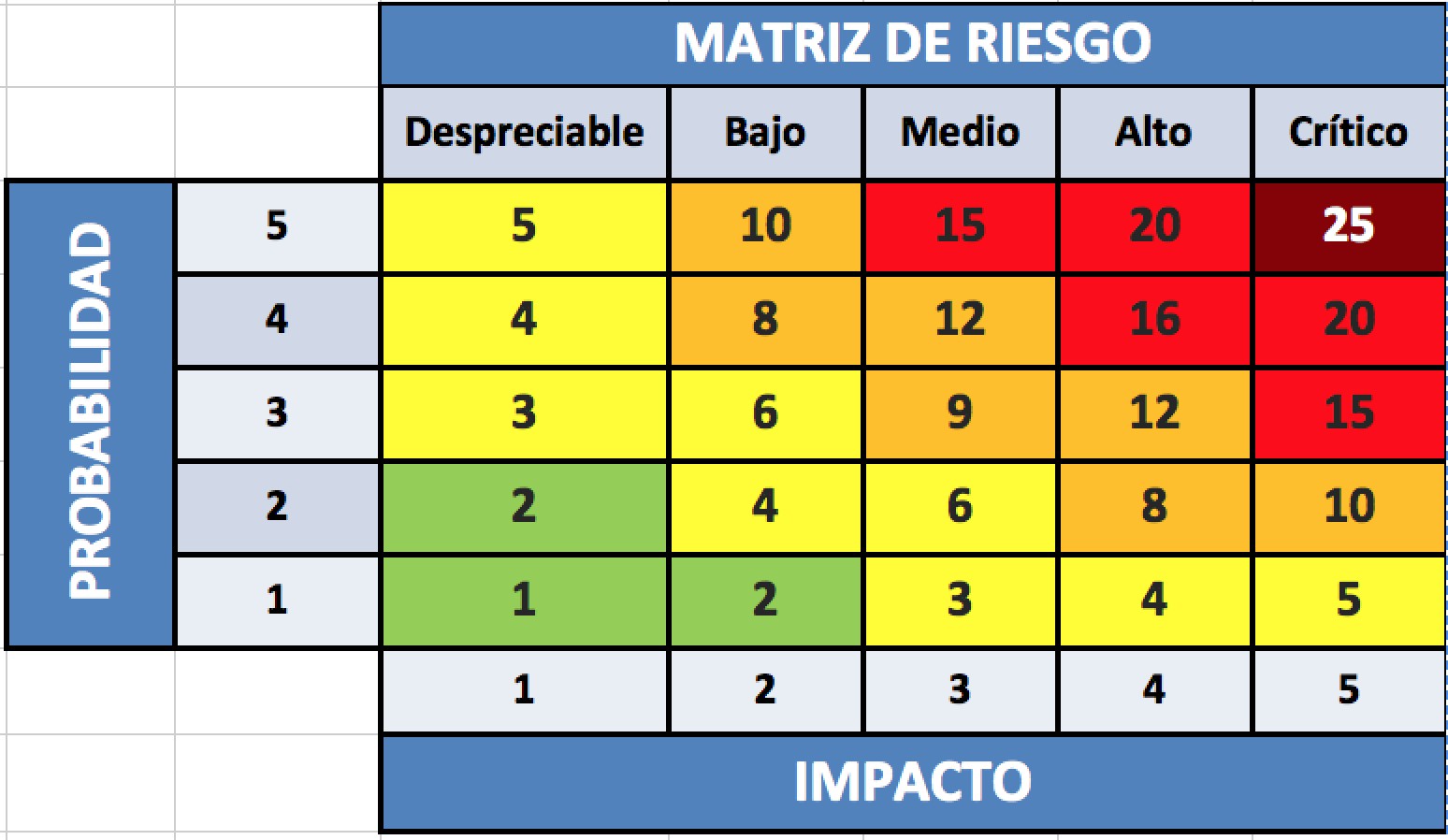
1. **Diagrama de secuencia – Bajo Nivel**



**Figura 4.10: Diagrama de secuencia – Bajo Nivel**

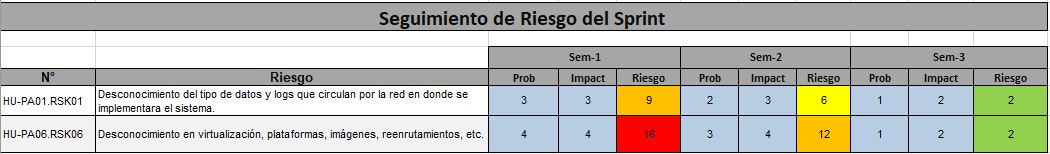
1. **Riesgo técnico del Sprint**

El análisis del riesgo técnico para este sprint se enumera como sigue, la estimación del riesgo se realizó teniendo en cuenta valores de impacto y probabilidad según tabla adjunta.



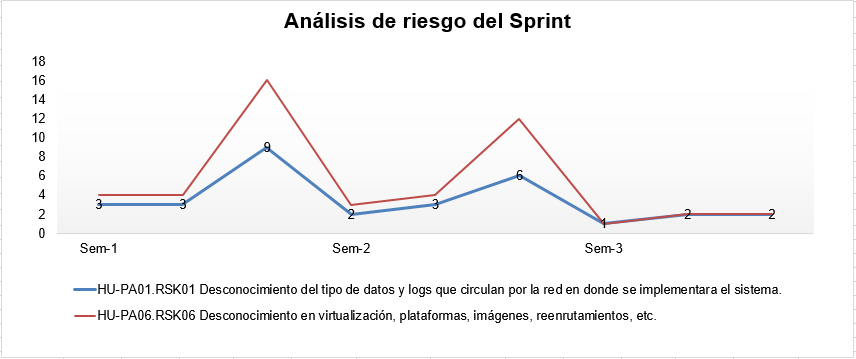
**Figura 4.11: Tablas de riesgo**

1. **Análisis de riesgo técnico Sprint 1**



**Tabla 4.12: análisis de riesgo técnico para Sprint 1**

1. **Análisis de riesgo del Sprint 1**



**Tabla 4.13: análisis de riesgo técnico para Sprint 1**

1. **Pruebas de Desarrollador**

|  |  |
| --- | --- |
| **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 |

1. **Pruebas de aceptación**

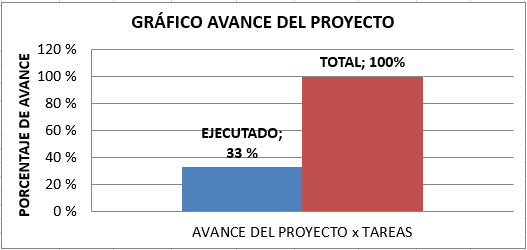
Evidencias en los criterios de Aceptación que están asociados con las HU, en el Sprint Backlog.

El sistema se encuentra alojado en la siguiente url: <http://10.40.5.25:9000/>, a la cual se puede acceder desde los equipos de la red del laboratorio 306 (las islas de al fondo de la sala), las credenciales para ingresar son:

User : **admin**

Password: **Unab2020\***

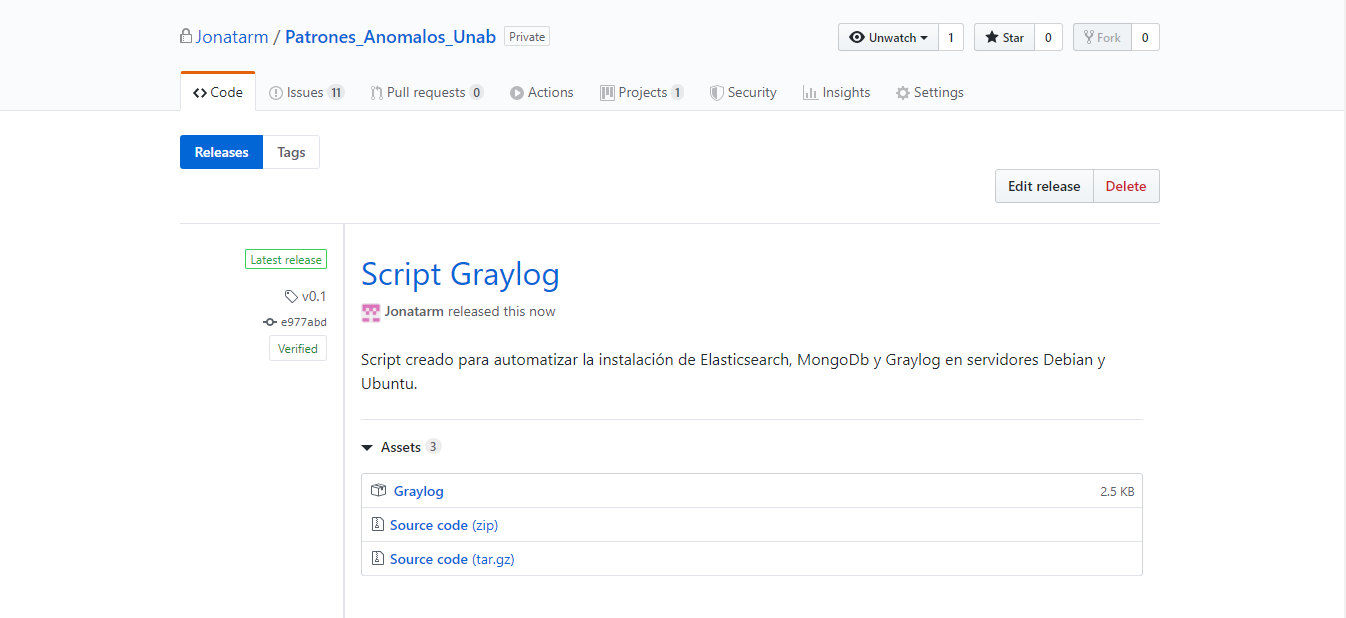
1. **Métricas Producto / Proyecto**



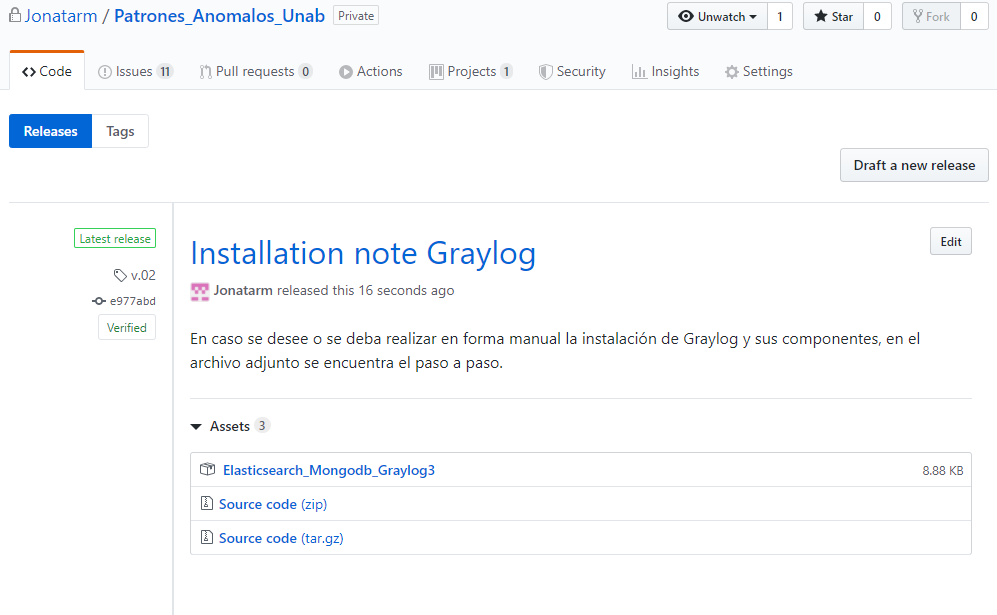
1. **Plan de control de versiones**

El control de versiones se mantiene según se menciona en el capítulo 3: Materiales y métodos. Este sprint se libera como la versión v.01 para la aplicación.

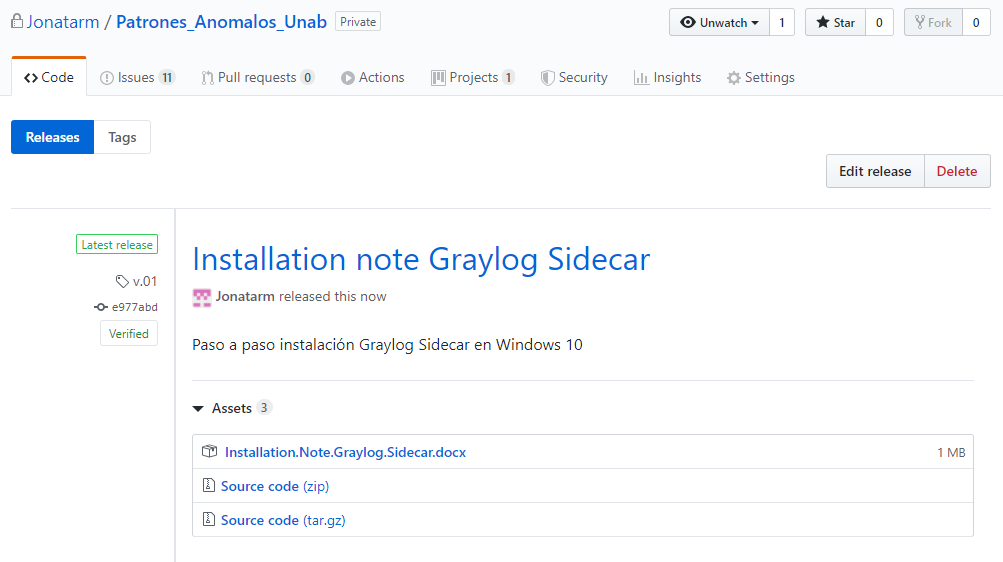
Github : <https://github.com/Jonatarm/Patrones_Anomalos_Unab/projects/1>



**Figura 4.14 Liberación aplicación web GitHub**



**Figura 4.15 Installation note Graylog**



**Figura 4.16 Installation note Graylog Sidecar**

**Capítulo 5: 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.

1. **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.

1. **Trabajo Futuro**

Como trabajo pendiente quedan la realización de las historias de usuario HU-PA02, 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.)

**Revisión del Sprint**

Al finalizar el sprint se realizó una reunión con el Product Owner, para presentar la liberación del incremento para este sprint al término del periodo acordado por él.

El objetivo programado para este sprint fue de completar las **HU-PA01** y **HU-PA06,** que se alinean con el objetivo específico **OE5**, establecidos al inicio de este documento, que básicamente tratan de construir un sistema el cual logre alimentarse de orígenes de datos (Firewall, Routers, Switches, Filtros, Equipos de escritorio, etc.), todo aquel que genere un log podría ser ingresado a este sistema de correlación, este sistema de correlación de eventos es capaz de procesar, sensar, parsear, graficar, correlacionar y permitir una visualización en detalle de lo que esta ocurriendo en segundo plano con una determinada red informática.

Se terminó el Sprint en el tiempo acordado y aceptado por el Product Owner.