**ANEXO - SPRINT 4**

1. **Objetivo del sprint**

Este Sprint aportará a cubrir parte del objetivo específico **OE4** “Aumentar los tiempos de respuesta ante un incidente informático por parte del personal de Seguridad TI”.

Al implementar la historia de usuario **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”.

Se implementarán sitio web “Ciberdefensa Unab”, el cual estará compuesto por:

1. 01 Sitio web “Ciberdefensa Unab”.
2. 01 Formulario con preguntas en sitio web (Autoevaluación)**.**
3. 03 Blog con recomendaciones de acuerdo a nivel obtenido en autoevaluación.

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 | 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 customizar patrones de detección en base a requerimientos. | Para poder detectar lo desconocido en la red. | 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 sistema que logre detectar patrones anómalos de comportamiento. | Para entregar una mejor visualización a los encargados de Seguridad TI. | M | 20 | 7 |
|  | - |  |  |  |  |  |
| 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 |

**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 #** | **4** | **Días Inicio Sprint** | **0** | **Inicio Puntos de Historia** | **48** |
| **Fecha de Inicio** | **13-05-2020** | **Días Termino Sprint** | **21** | **Término Puntos de Historia** | **0** |

|  |  |  |
| --- | --- | --- |
| **ID TAREA** | **TAREA** | **PUNTOS HISTORIA** |
| HU-PA09.T1 | Investigar respecto a como crear paginas web con formularios de encuestas. | 3 |
| HU-PA09.T2 | Generar formulario de preguntas para autoevaluación. | 2 |
| HU-PA09.T3 | Crear sitio web Ciberdefensa Unab con formulario de "Autoevaluación". | 8 |
| HU-PA09.T4 | Efectuar pruebas objeto comprobar la correcta realización de encuesta. | 2 |
| HU-PA09.T5 | Configurar formulario de preguntas, objeto este asigne una puntuación y entregue recomendaciones. | 5 |
| 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 o archivos del entregable a Github o Drive, 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 este Sprint 4 será de 3 semanas, el inicio de este será el día 13 de mayo de 2020 y terminará el día 02 de junio de 2020.

1. **Criterios de aceptación**

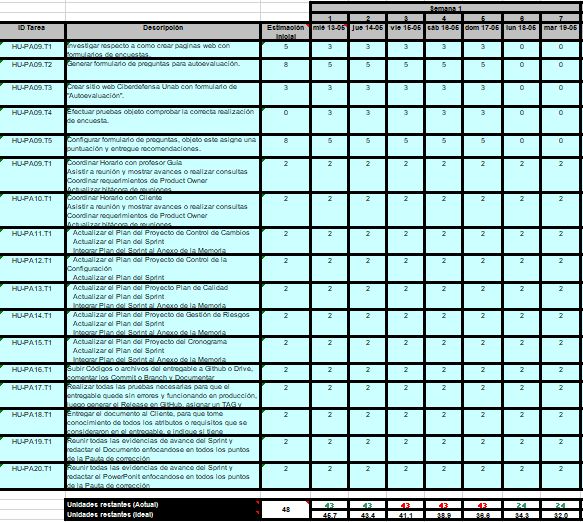
A continuación, se presentan los criterios de aceptación para la HU-PA09 que se desarrollará en el Sprint 4 (Hito-3) 2020.

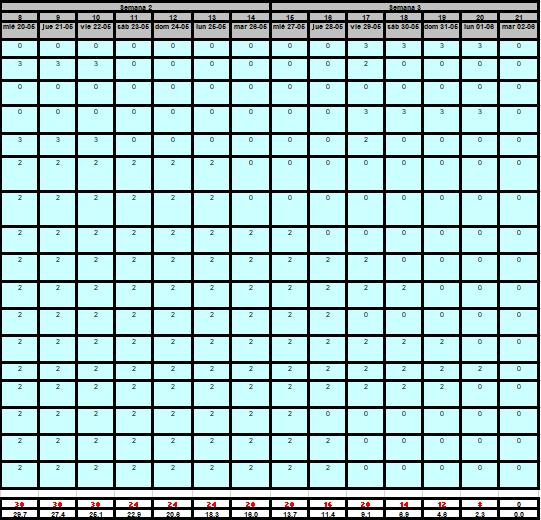
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CRITERIOS DE ACEPTACIÓN** | | | | | |
| **Número de**  **escenario** | **Criterio de aceptación (Título)** | **Contexto** | **Evento** | **Resultado / Comportamiento esperado** | **Estado** |
|  |  |  |  |  |  |
| E1 | HU-PA09.T5.E1 - Sitio 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 4.3: Criterios de aceptación**

1. **Seguimiento para Sprint 1**

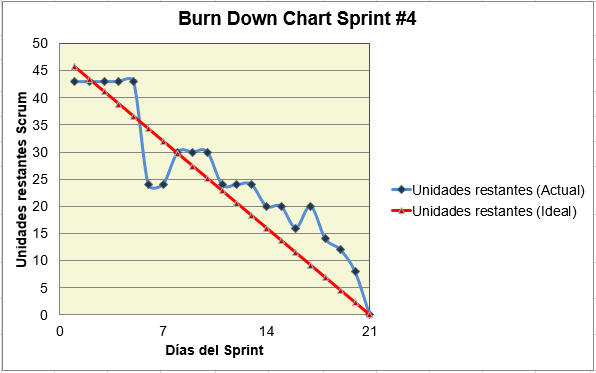
1. **Sprint Planning**





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

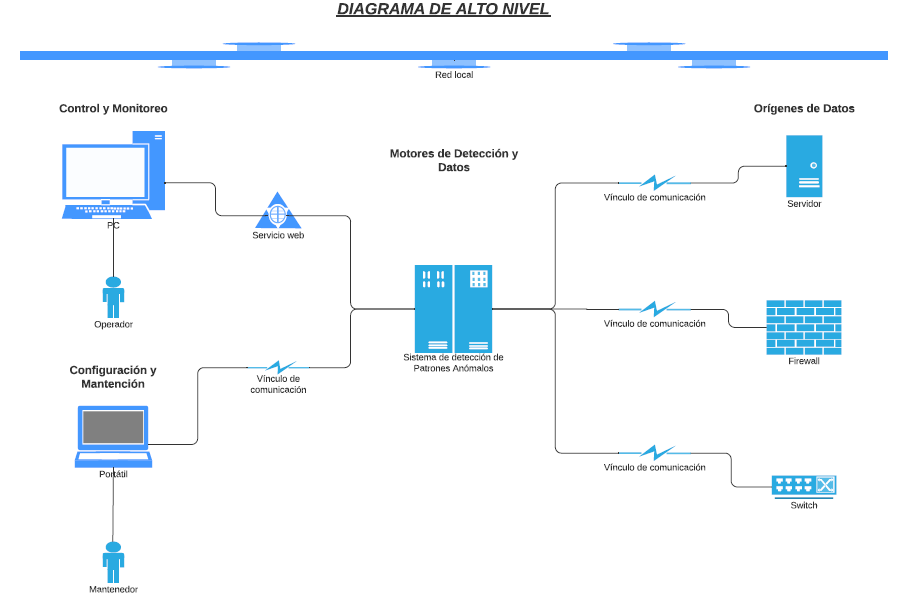
1. **Sprint 3 Burn Down Chart**



**Figura 4.5: Burn down chart**

1. **Arquitectura de la aplicación**

1. **Diagrama de Alto nivel**



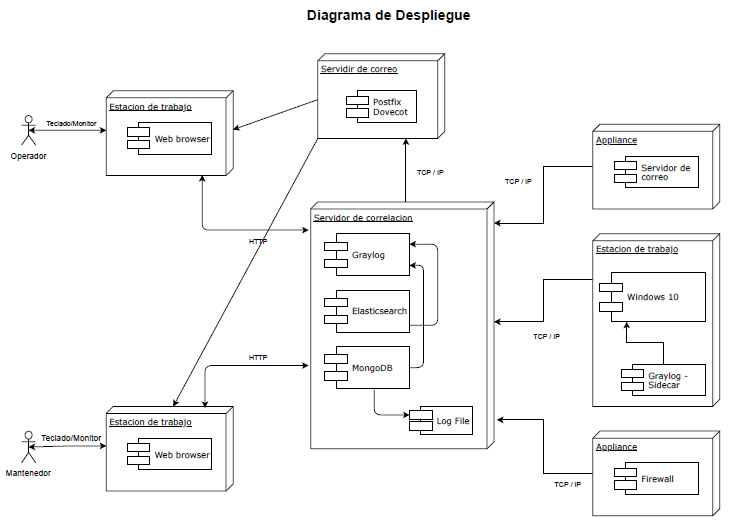
**Figura 4.6: Diagrama de Alto Nivel**

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.
* **Data source:** 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 Workstation con máquinas Ubuntu 16.04.

- AnyDesk para servidor Ubuntu alojado en red UNAB.

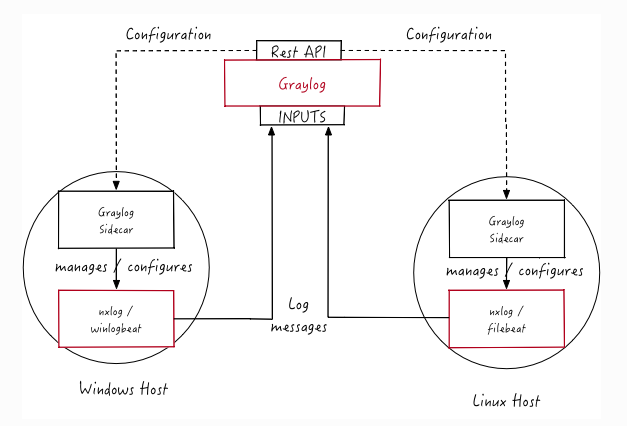
- Protocolo http, puerto 9000.

* **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).



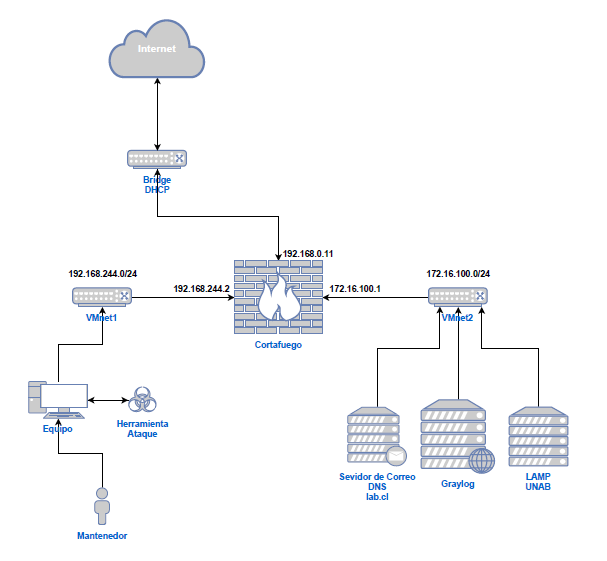
**Figura 4.8: Diagrama Graylog-Sidecar**

**fuente**

* **Servidor de correo:**

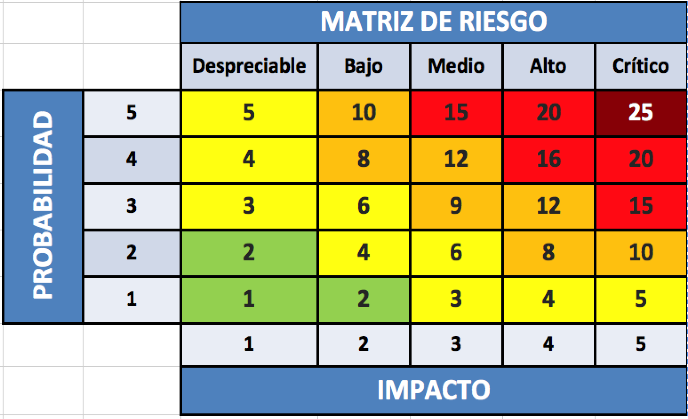
El cual esta compuesto por Postfix y Dovecot, Postfix es un mx (mail exchange) y Dovecot permite que se puedan conectar gestores de correo por imap o pop3, en este caso imap.

1. **Arquitectura actual**



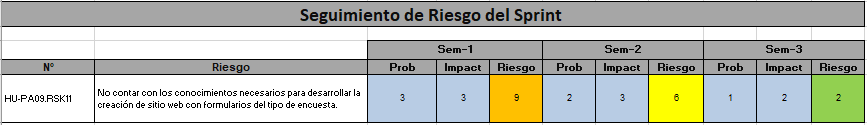
1. **Riesgo técnico del Sprint**

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.



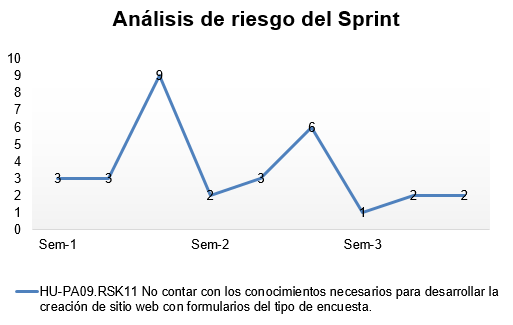
**Figura 4.11: Tabla de riesgo**

1. **Análisis de riesgo técnico Sprint 4**



**Tabla 4.12: análisis de riesgo técnico para Sprint 4**

1. **Análisis de riesgo del Sprint 3**



**Tabla 4.13: análisis de riesgo técnico para Sprint 4**

1. **Pruebas de aceptación / desarrollador**

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

1. **Escenario actual:**

A raíz de la contingencia que se nos presenta hoy en día, no es posible asistir en forma presencial a los laboratorios de la Universidad, es por esto que en este sprint 4 y con el objetivo de cumplir con lo planificado, se coordino con encargado de laboratorios de la Universidad la asignación de un “Subdominio en Wordpress” para crear e implementar sitio web correspondiente a este Sprint.

A continuación se detallan pruebas realizadas, objeto el cliente acepte el producto presentado.

|  |  |
| --- | --- |
| **Serie** | **P1 – 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** | **P2 – 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** | **P3 – 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. |

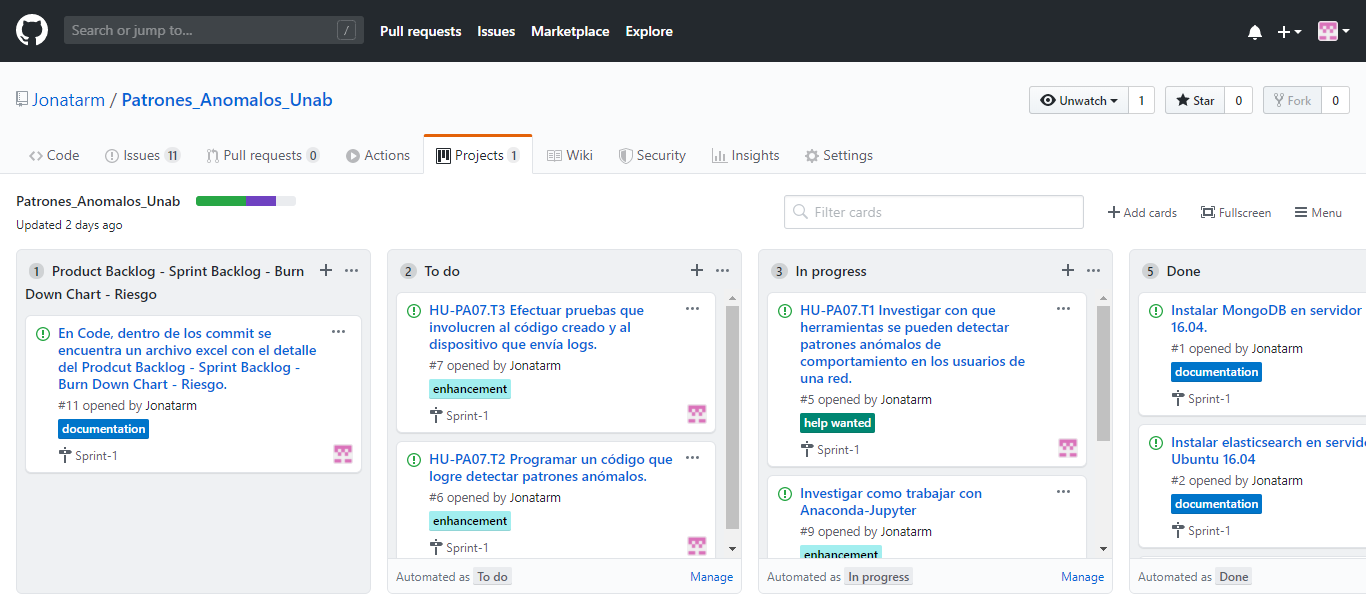
1. **Escenario anterior:**

Respecto al escenario anterior asociado a este Sprint, el cual en términos generales trata de crear un sitio web, se hace presente de que no existe ningún sitio web anterior a este que se implemento; por lo cual el escenario anterior es que no existía sitio web referente a este tema de Ciberdefensa

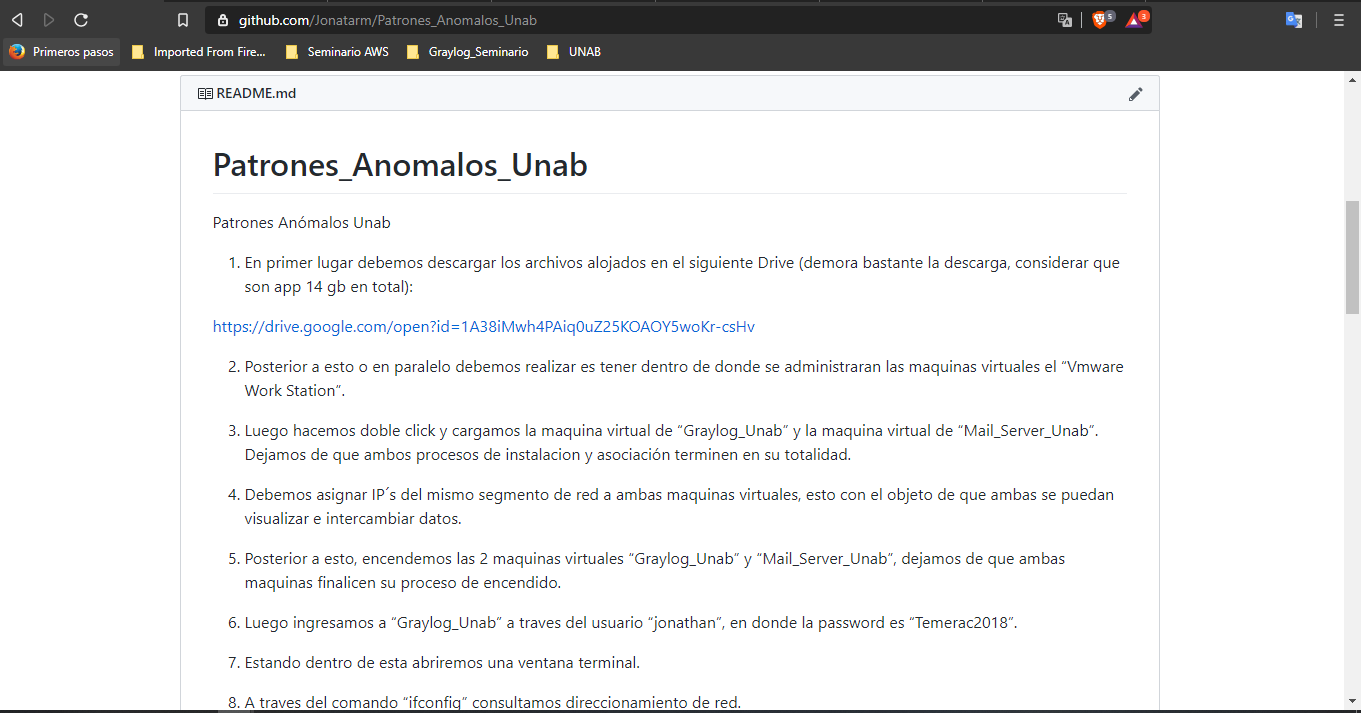
1. **Plan de control de versiones**

El control de versiones se mantiene según se menciona en el capítulo 3: Materiales y métodos. Este sprint se libera como la versión v.04 para la aplicación.

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

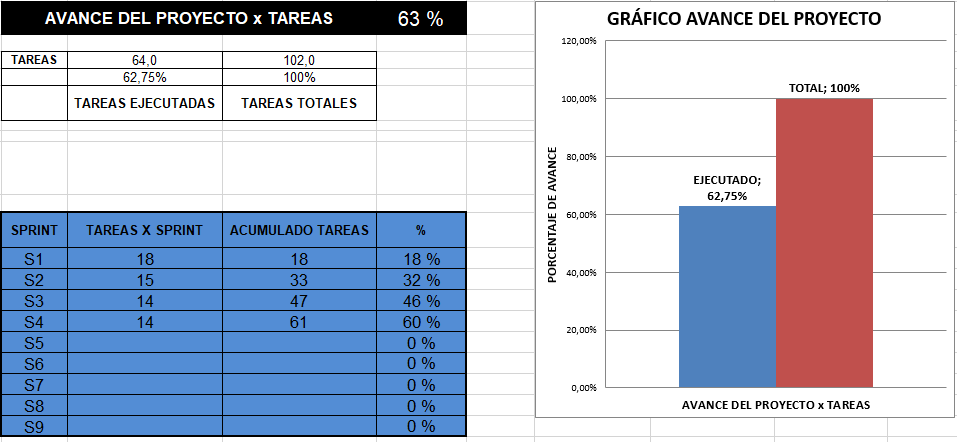


**Figura 4.14 Liberación aplicación web GitHub**

****

**Figura 4.17 readme.md**

1. **Métricas Producto / Proyecto**



**Capítulo 5**

1. **Post Morten**

El producto como tal (sitio web) quedo liberado dentro del subdominio Wordpress <http://ciberdefensa.informatica-unab-vm.cl> el cual fue aceptado por el cliente.

Respecto a las pruebas con el cliente y aceptación del producto fueron realizadas de forma remota a raíz de la contingencia que nos afecta actualmente.

El producto entregado cumple con lo planificado y solicitado por el cliente, sitio web esta desplegado y operando en forma normal, a través de este se puede realizar la “Autoevaluación”, posterior a esta se envía en forma automática una recomendación de seguridad basada en los resultados de la Autoevaluación.

1. **Problemas abiertos:**

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.

1. **Trabajo Futuro**

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. Implementar 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.