**Plan de cierre**

1. **Objetivo del Plan de cierre**

El objetivo de este Plan de cierre, es informar de todas las HU´s y actividades asociadas a estas que se realizaron durante la ejecución del proyecto titulado como “**Propuesta de Infraestructura TI de bajo costo para proteger una RED CORPORATIVA de micro y pequeñas empresas**”.

Con esto se pretende tener una visión global y asertiva de que HU’s podrían descartarse de este proyecto y cual o cuales pueden agregarse a este, enfocándose en la finalización del presente proyecto.

1. **HU´s completadas:**

A continuación, se presentan las HU´s completadas para el Proyecto, estas se encuentra priorizadas 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-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-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 1: HU´s completadas**

1. **HU´s Pendientes:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID HU** | **Rol ¿Quien?** | **Característica Funcionalidad Objetivo ¿Quiero?** | **Razón Resultado ¿Para qué?** | **Prioridad** | **Pts. Hist HU** | **# Sprint** |
| 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-PA08 | Como administrador | Quiero crear reglas de detección de patrones anómalos de comportamiento. | Para poder detectar comportamientos anómalos en la red. | M | 13 | 6 |

**Tabla 2: HU´s Pendientes**

Respecto a estas 02 HU´s pendientes, se propone que sean **descartadas** del proyecto, tomando en cuenta que:

La **HU-PA08** actualmente esta siendo ejecutada por las HU-PA05 y HU-PA07 en el Sprint-5 (Hito 1) recién pasado.

La **HU-PA04** no va por el camino de detectar posibles incidentes dentro de la red, sino mas bien como una forma de optimizar el sistema.

1. **HU´s Propuestas:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID HU** | **Rol ¿Quien?** | **Característica Funcionalidad Objetivo ¿Quiero?** | **Razón Resultado ¿Para qué?** | **Prioridad** | **Pts. Hist HU** | **# Sprint** |
| HU-PA04 | Como Mantenedor | Quiero poder extraer todos los Dataset de los ataques ejecutados sobre el sistema a prueba. | Para tener una visualización certera de que efectivamente es lo que se esta realizando sobre la red. | M | 13 | 6 |
| HU-PA08 | Como Mantenedor | Quiero poder categorizar de forma correcta los ataques ejecutados sobre la red a través del modulo de categorización en conjunto con el correlacionador de eventos. | Para no tener falsos positivos, ni errores de interpretación en gestión y ejecución de medidas de mitigación adoptadas. | M | 13 | 7 |

**Tabla 3: HU´s Propuestas**

1. **Tareas HU-PAX1**

La siguiente tabla representa el Sprint Backlog planificado para la **HU-PAX1** “Quiero poder extraer todos los Dataset de los ataques ejecutados sobre el sistema a prueba.” propuesta, donde se asigna la estimación de horas de trabajo necesarias para completar cada tarea.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID TAREA** | **TAREA** | **Estimación Hrs.** | **Sprint** |
| HU-PAX1.T1 | Investigar respecto a como ejecutar los diferentes tipos de ataques sobre la infraestructura ya implementada. | 15 | 6 |
| HU-PAX1.T2 | Generar de manera correcta los Dataset posterior al ataque ejecutado. | 12 | 6 |
| HU-PAX1.T3 | Extraer y disponibilizar de manera correcta los diferentes Dataset antes del análisis de estos en el modulo de Machine Learning. | 12 | 6 |

**Tabla 4: Tareas HU-PAX1**

1. **Tareas HU-PAX2**

La siguiente tabla representa el Sprint Backlog planificado para la **HU-PAX2** “Quiero poder categorizar de forma correcta los ataques ejecutados sobre la red a través del modulo de categorización en conjunto con el correlacionador de eventos” propuesta, donde se asigna la estimación de horas de trabajo necesarias para completar cada tarea.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID TAREA** | **TAREA** | **Estimación Hrs.** | **Sprint** |
| HU-PAX2.T1 | Investigar respecto a como integrar de manera correcta los logs que envía el Modulo de Machine Learning al correlacionador de eventos. | 12 | 7 |
| HU-PAX2.T2 | Mostrar una categorización correcta de los diferentes tipos de ataques dentro de la infraestructura propuesta. | 12 | 7 |
| HU-PAX2.T3 | Ejecutar las acciones de notificación del incidente detectado vía correo electrónico al encargado del área. | 9 | 7 |

**Tabla 5: Tareas HU-PAX2**

1. **Conclusión**

Con las 02 HU´s descartadas del proyecto y con estas nuevas 02 HU´s propuestas se pretende dar una enfoque mas enfocado en la génesis de este proyecto, tomando siempre como prioridad la detección de posibles incidentes de seguridad dentro de la red, para con esto lograr apoyar de manera correcta y asertiva la gestión y toma de decisiones ante un inminente evento de Ciberseguridad.