MARCO METODOLÓGICO

Juan Carlos Suela Martín

Sergio del Pino Gómez

Marcos Illán López

Iván del Pino García

RESECO

Desarrollo y Gestión de Sistemas de Información

RESECO

RESECO

Definición del Marco Metodológico:

En nuestro proyecto, el equipo adoptará roles claramente definidos dentro del marco de Scrum:

Roles:

Product Owner (PO): Este rol será asumido por uno de los integrantes del equipo, preferiblemente alguien que tenga una comprensión profunda de las necesidades del negocio y pueda representar efectivamente al cliente. El Product Owner será responsable de gestionar el backlog del producto, priorizar las funcionalidades y tomar decisiones sobre el producto en nombre del cliente y del equipo. Este rol se le ha asignado a Marcos Illán.

Scrum Master (SM): Otro integrante del equipo asumirá el rol de Scrum Master. Este rol implica liderar y facilitar el proceso Scrum, asegurándose de que se sigan las prácticas y los principios de Scrum. El Scrum Master también será responsable de eliminar los obstáculos que puedan surgir durante el desarrollo del proyecto y de fomentar un ambiente colaborativo y productivo. Este rol se le ha asignado a Juan Carlos Suela.

Equipo de Desarrollo: Los dos miembros restantes del equipo formarán parte del equipo de desarrollo. Serán responsables de implementar las funcionalidades del Sistema de Información Automatizado de acuerdo con las prioridades establecidas por el Product Owner. Trabajarán de manera autónoma durante los sprints para completar las tareas asignadas, colaborando estrechamente entre ellos y con el Product Owner para asegurar la entrega de un producto de alta calidad. Este rol se les ha asignado a los miembros Sergio del Pino e Iván del Pino.

Con esta distribución de roles, cada integrante del equipo tendrá responsabilidades claras y contribuirá al éxito del proyecto utilizando sus habilidades y conocimientos específicos.

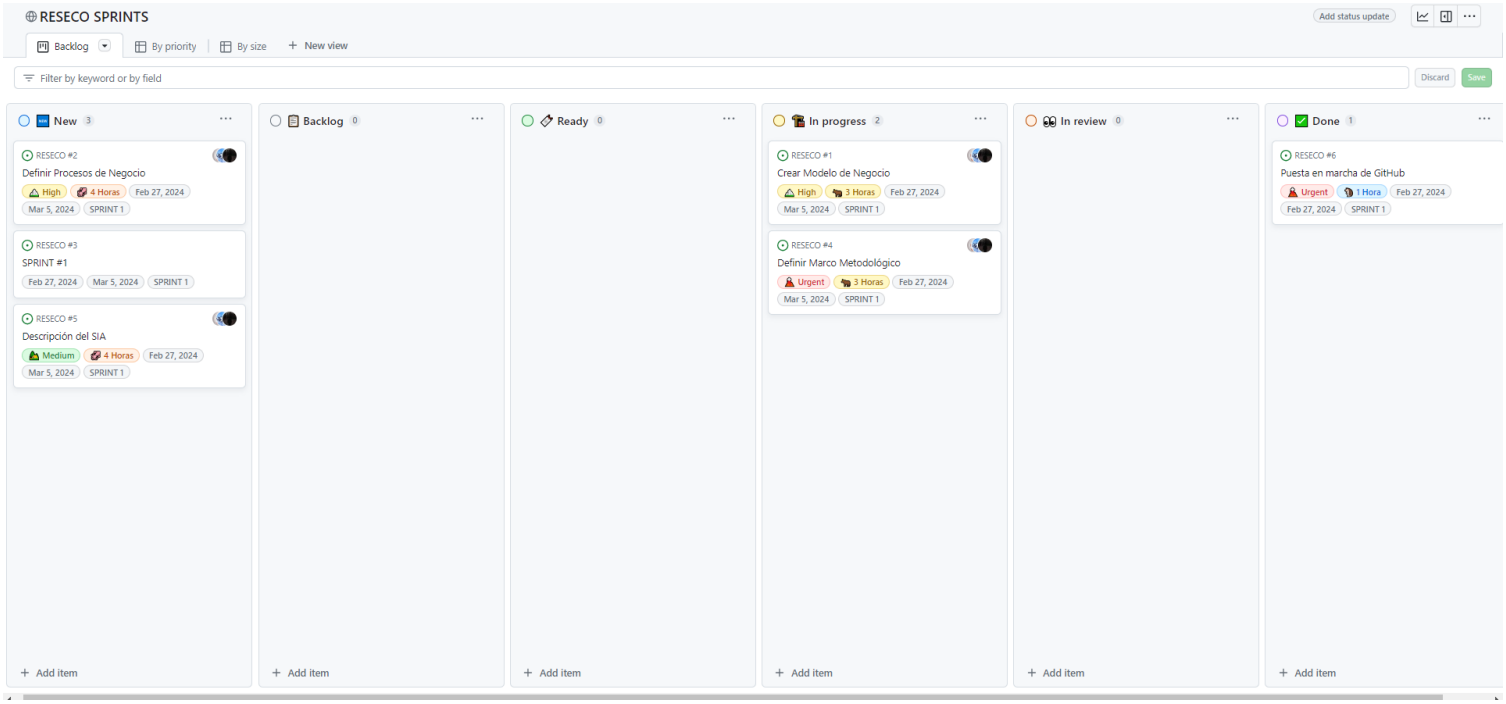
Puesta en marcha en GitHub:

Para la gestión del proyecto, se utilizará GitHub como plataforma principal. Se ha creado una organización denominada "dgsi-lab-gl5-2324", donde se han agregado los miembros del equipo y el profesor de prácticas.

Dentro de esta organización, se ha creado un proyecto específico para el desarrollo del SIA, con el nombre RESECO (Redes y Seguridad Corporativas). Este proyecto utilizará un tablero en GitHub para la planificación y seguimiento de las tareas.

RESECO

El tablero en GitHub se ha configurado de acuerdo con las necesidades del proyecto. Se han añadido vistas y columnas pertinentes para el seguimiento del trabajo, y se han creado campos personalizados como "status", "weight", "sprint" y "date" para facilitar la organización y la planificación de los requisitos. Las columnas creadas representan los diferentes estados por los que pasan las tareas en un sprint, desde que se añaden nuevas al tablero en su reunión semanal (*New*), pasando por *Backlog* (rincón para situar las tareas que quedan libres), *Ready* (las tareas de Backlog pasan a esta columna cuando están listas para que un miembro pueda trabajar con ellas, sin ninguna clase de dependencia entre tareas), *In Progress* (cuando la tarea se está llevando a cabo o desarrollando), *In review* (cuando la tarea acabó de desarrollarse y está lista para revisarse o se está revisando), y acabando en *Done* (cuando la tarea se ha revisado correctamente y es aprobada).



Además, se han configurado workflows para asegurar que los requisitos avancen adecuadamente durante cada sprint, según los eventos definidos en el proceso de desarrollo.

Sistema de Información

Descripción del Sistema de Información Automatizado (SIA) para una Empresa de Redes y Seguridad

El Sistema de Información Automatizado (SIA) diseñado para la empresa es una plataforma integral que combina tecnologías de vanguardia para ofrecer soluciones avanzadas en el ámbito de la seguridad de la información y la gestión de redes. Este sistema se fundamenta en un enfoque holístico que abarca tanto el software como el hardware necesario para garantizar la protección, el monitoreo y la administración eficiente de los recursos de red y la seguridad cibernética.

Infraestructura Tecnológica:

1. Hardware:

El SIA se basa en una infraestructura de hardware robusta y escalable que proporciona el soporte necesario para ejecutar las diversas funcionalidades y procesos del sistema. Esto incluye servidores de alto rendimiento, sistemas de almacenamiento de datos redundantes y equipos de red de última generación, como firewalls, switches y routers, capaces de gestionar el tráfico de red de manera eficiente y segura.

2. Software:

El corazón del SIA reside en su conjunto de software especializado, que ofrece una amplia gama de funcionalidades diseñadas para abordar los desafíos específicos de la seguridad de la información y la gestión de redes. Entre las principales características del software se incluyen:

Sistema de Gestión de Eventos e Información de Seguridad (SIEM): Este componente central del SIA permite la recopilación, correlación y análisis de datos de seguridad procedentes de múltiples fuentes, como registros de eventos, sistemas de detección de intrusiones, y dispositivos de seguridad de red. Utilizando algoritmos avanzados y técnicas de inteligencia artificial, el SIEM identifica patrones y anomalías que podrían indicar actividades maliciosas o riesgos de seguridad.

Sistema de Detección y Prevención de Intrusiones (IDS/IPS): El SIA integra sistemas de detección y prevención de intrusos que monitorean el tráfico de red en busca de comportamientos sospechosos o intentos de violación de seguridad. Estos sistemas utilizan firmas, reglas y algoritmos de detección avanzados para identificar y mitigar amenazas en tiempo real, protegiendo así la integridad y confidencialidad de los datos.

Gestión Unificada de Amenazas (UTM): El SIA incorpora una plataforma de UTM que combina múltiples funciones de seguridad, como firewall, antivirus, filtrado de contenido, y control de aplicaciones, en una sola solución integrada. Esto proporciona una defensa perimetral completa y simplifica la administración de la seguridad en toda la infraestructura de red.

Herramientas de Gestión y Monitorización de Redes: Además de las capacidades de seguridad, el SIA incluye herramientas de gestión y monitorización de redes que permiten supervisar el rendimiento, la disponibilidad y la utilización de los recursos de red en tiempo real. Estas herramientas ofrecen visibilidad completa sobre la topología de red, el tráfico de datos y el estado de los dispositivos, facilitando la detección temprana de problemas y la optimización del rendimiento de la red.

Sistema de Gestión de Identidades y Accesos (IAM): Este componente es esencial para controlar y administrar los accesos a los recursos de la red y los sistemas de información. El IAM gestiona la autenticación, autorización y auditoría de usuarios y dispositivos, asegurando que solo las personas autorizadas tengan acceso a la información y los servicios correspondientes a sus roles y privilegios.

Gestión de Vulnerabilidades: El SIA incluye herramientas de escaneo y evaluación de vulnerabilidades que identifican y clasifican las posibles debilidades y fallos de seguridad en la infraestructura de red y los sistemas informáticos. Estas herramientas permiten realizar análisis de riesgos y priorizar la aplicación de medidas correctivas para mitigar las vulnerabilidades y fortalecer la postura de seguridad de la organización.

Sistema de Gestión de Configuración (CMS): El CMS facilita la configuración y administración centralizada de los dispositivos de red y los sistemas informáticos, garantizando la coherencia y consistencia en la implementación de políticas de seguridad y las configuraciones de los equipos. Esto reduce el riesgo de errores de configuración y facilita la detección y corrección de desviaciones no autorizadas en la configuración.

Plataforma de Análisis de Seguridad: El SIA puede integrar una plataforma de análisis de seguridad que utiliza técnicas avanzadas de aprendizaje automático y análisis de comportamiento para identificar amenazas y anomalías en el tráfico de red y los datos de seguridad. Esta plataforma proporciona una capa adicional de defensa contra amenazas sofisticadas y ataques dirigidos, permitiendo una respuesta más rápida y efectiva a las emergencias de seguridad.

Gestión de Incidentes de Seguridad: Para gestionar eficazmente los incidentes de seguridad, el SIA incluye un sistema de gestión de incidentes que facilita la notificación, respuesta y resolución de eventos de seguridad en tiempo real. Este sistema permite coordinar las acciones

de los equipos de seguridad, recopilar información forense y mantener registros detallados de los incidentes para análisis posterior y mejora continua.