MODELO DE NEGOCIO

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

Contexto

RESECO es una empresa especializada en servicios de redes, con un enfoque distintivo en la seguridad de las redes. Con la creciente dependencia de las redes en la vida cotidiana y empresarial, la seguridad se ha convertido en una preocupación fundamental.

RESECO busca satisfacer esta necesidad, ofreciendo soluciones que recojan desde la implementación y mantenimiento de redes hasta la fabricación y reparación de dispositivos relacionados con la seguridad y conectividad.

Objetivos

- Ofrecer servicios de consultoría en seguridad de redes para evaluar riesgos, elaborar planes de implementación y recomendar medidas de seguridad adecuadas para satisfacer las necesidades del cliente.
- Montar firewalls físicos o virtuales en redes empresariales, asegurando su correcta configuración y funcionamiento para proteger la infraestructura de posibles amenazas.
- Instalar firewalls de acuerdo con los requisitos de seguridad del cliente, garantizando que las configuraciones sean aplicadas de manera efectiva y adaptadas a las necesidades específicas de cada red.
- Gestionar incidentes de seguridad, investigando y resolviendo eventos de seguridad, además de ofrecer recomendaciones para prevenir futuros incidentes.
- Configurar redes privadas virtuales (VPN) para permitir el acceso remoto de manera segura, proporcionando documentación detallada sobre la configuración y las políticas de acceso.
- Monitorear amenazas en tiempo real para identificar y responder rápidamente a posibles riesgos de seguridad, emitiendo alertas y generando informes de incidentes de red.
- Brindar soporte técnico especializado para resolver problemas de seguridad y garantizar el funcionamiento adecuado de los sistemas implementados.
- Ofrecer formación en seguridad para capacitar al personal de las empresas en las mejores prácticas y procedimientos de seguridad cibernética.
- Desarrollar software seguro para complementar las soluciones de seguridad ofrecidas, asegurando la integridad y confidencialidad de los datos de los clientes.

Stakeholders

- **Clientes:** Son la parte más importante de RESECO, ya que son quienes utilizan y se benefician de los servicios y soluciones de seguridad de redes ofrecidos. Los clientes pueden ser empresas de diversos tamaños y sectores que buscan proteger sus activos digitales y garantizar la continuidad de sus operaciones.

- **Equipo de Gestión y Empleados**: Incluye a los fundadores, directivos, gerentes y personal de RESECO. Estos individuos son responsables de la dirección estratégica de la

empresa, la toma de decisiones operativas y la prestación de servicios de alta calidad. Su compromiso y competencia son fundamentales para el éxito y la reputación de la empresa.

- **Proveedores y Socios Tecnológicos:** Compañías que suministran hardware, software y otros recursos tecnológicos utilizados por RESECO en la prestación de sus servicios. Estos proveedores y socios tecnológicos son vitales para garantizar que RESECO cuente con las herramientas y la tecnología más avanzadas y confiables para satisfacer las necesidades de seguridad de sus clientes.

- **Reguladores y Organismos de Control:** Incluye entidades gubernamentales, reguladores de la industria y organismos de estándares que establecen directrices y normativas relacionadas con la seguridad cibernética y la protección de datos. Cumplir con estas regulaciones es esencial para la operación legal y ética de RESECO, y mantener una buena relación con estos stakeholders puede ayudar a la empresa a mantenerse actualizada y competitiva en un entorno en constante cambio.

- **Inversores y Accionistas:** Personas o entidades que han invertido capital en RESECO y tienen un interés financiero en su éxito y rentabilidad. Estos stakeholders están interesados en el crecimiento y la rentabilidad de la empresa a largo plazo, por lo que es importante para RESECO mantener una gestión financiera sólida y transparente para mantener su confianza y apoyo.

- **Comunidad y Sociedad:** La comunidad local y la sociedad en general también pueden considerarse stakeholders de RESECO, ya que la empresa puede tener un impacto en ellos a través de sus actividades comerciales, empleo y responsabilidad social corporativa. Mantener buenas relaciones con la comunidad y contribuir al desarrollo sostenible puede mejorar la reputación y la imagen pública de la empresa.

- **Competidores:** Otras empresas que ofrecen servicios similares en el mercado también son stakeholders importantes para RESECO. La competencia puede influir en la estrategia empresarial, la innovación y los estándares de calidad de RESECO, y mantenerse al tanto de las acciones y los movimientos de los competidores es crucial para mantener una posición sólida en el mercado.

- **Medios de Comunicación y Opinión Pública**: Los medios de comunicación y la opinión pública pueden influir en la percepción y la reputación de RESECO a través de la cobertura mediática, las redes sociales y otras plataformas de comunicación. Mantener una comunicación abierta y transparente con estos stakeholders y gestionar

eficazmente la imagen de la empresa es fundamental para construir y proteger su reputación.

Procesos de negocio

1.Consultoría de Seguridad de Redes:

- Entradas: Requisitos del cliente, información sobre la infraestructura de la red, historial de incidencias de seguridad
- Salidas: Informe de evaluación de riesgos, plan de implementación y recomendaciones de seguridad
- Recursos: Expertos en seguridad informática, herramientas de evaluación de riesgos, documentación sobre mejores prácticas de seguridad.

2.Montaje de Firewalls

- Entradas: Firewalls físicos o virtuales, especificaciones técnicas, especificaciones de hardware y diseño de la red
- Salidas: Firewalls montados y configurados físicamente en la red y pruebas de
- Recursos: Personal técnico preparado para el montaje, herramientas para realizar pruebas, manuales de instalación

3.Instalación de Firewalls

- Entradas: Firewalls configurados, diseño de red, requisitos de seguridad.
- Salidas: Firewalls instalados, configuraciones de firewall aplicadas según los requisitos de clientes
- Recursos: Personal técnico, acceso a la red del cliente, herramientas para realizar pruebas.

4. Gestión de incidentes de Seguridad

- Entradas: Informes de incidentes de seguridad, registros de actividad de red, alertas de amenazas
- Salidas: Incidentes investigados y resueltos, recomendaciones de prevención de futuros incidentes
- Recursos: Equipo encargado a la seguridad, herramientas de análisis de seguridad

5. Configuración de VPNs

- Entradas: Requisitos de acceso remoto, topología de la red
- Salidas: VPN ya configurada y disponible, documentación sobre la configuración, políticas de acceso remoto
- Recursos: Equipo encargado a la seguridad, herramientas de análisis de seguridad

6.Monitoreo de Amenazas en Tiempo Real

- Entradas: Fuentes de información de amenazas, eventos de la red en tiempo real
- Salidas: Alertas de seguridad en tiempo real, informes de incidentes de la red.
- Recursos: sistemas de monitoreo de seguridad, trabajadores encargados de analizar eventos

7.Soporte Técnico

- Entradas: Solicitudes de soporte, informes de problemas
- Salidas: Problemas de seguridad resueltos,
- Recursos:

8.Formación en Seguridad

- Entradas: Material de aprendizaje, actualizaciones e información sobre las últimas amenazas.
- Salidas: Personal formado y capacitado en seguridad, material actualizado
- Recursos: Instructores con el aprendizaje necesario, simulaciones de ataque

9.Desarrollo de Software Seguro

- Entradas: Requisitos de seguridad del software, especificaciones funcionales.
- Salidas: Aplicaciones y software seguros, pruebas realizadas, documentación de seguridad.
- Recursos: Desarrolladores software, herramientas de análisis

10.Implementación de Autenticación Multifactor (MFA)

- Entradas: Requisitos y requerimientos de autenticación, infraestructura de red existente, políticas de acceso
- Salidas: Implementaciones MFA ya configuradas, políticas de autenticación definidas
- Recursos: Expertos desarrolladores en MFA, soluciones MFA (tokens, aplicaciones móviles) y herramientas de gestión de identidad

Marco metodológico

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.

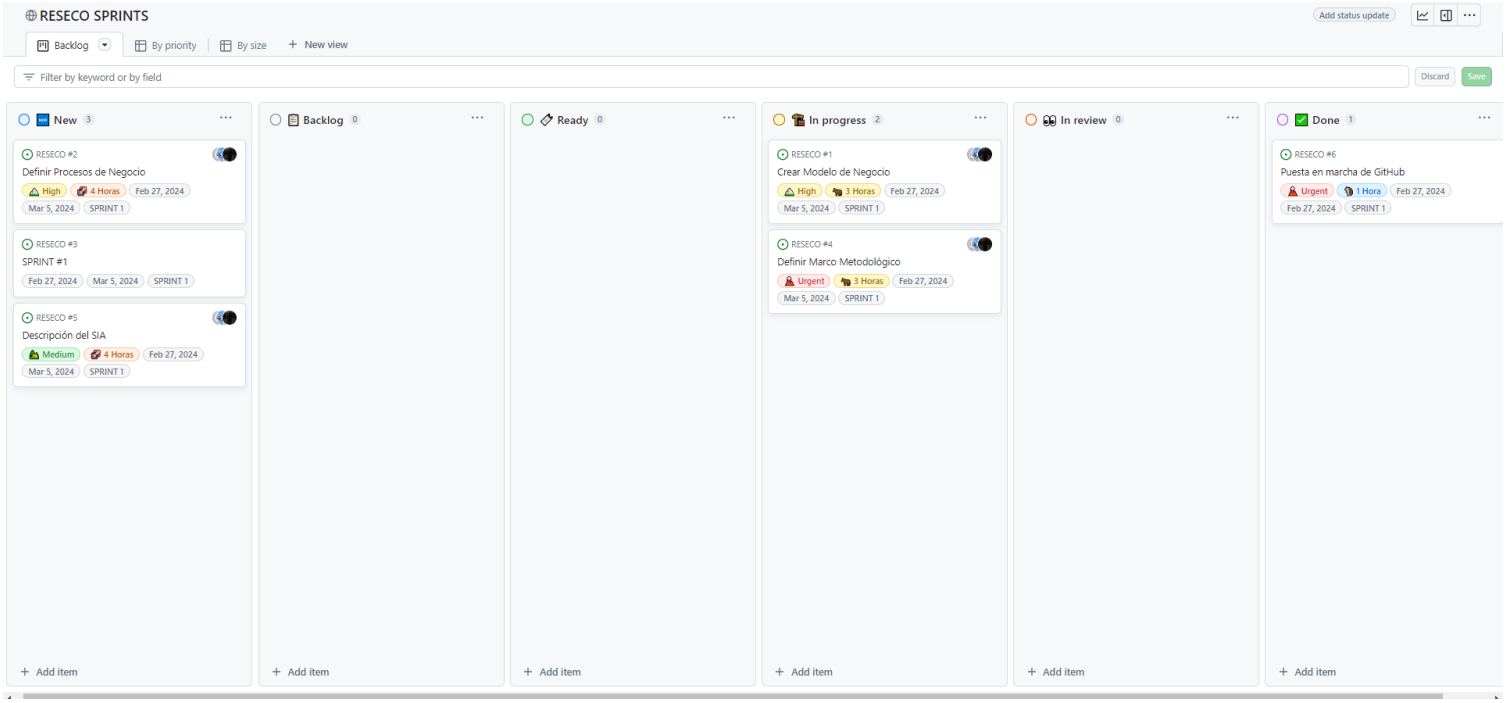
Puesta en marcha en GitHub:

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.

RESECO

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.

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.