

SISGRAN

GESTIÓN DE PROYECTO WEB

C.S.G.O

ROL	C.I	APELLIDO	NOMBRE	E-MAIL	TEL/CEL
Coordinador	52340981	Galeano	Nahuel	nahuelgaleano7778ng7@gmail.com	091791304
Subcoordinador	53176442	Soca	Camilo	Camilosoca0506@gmail.com	092466611
Integrante 1	45542358	Cardozo	Fabian	Fabcar20@hotmail.com	097337635
Integrante 2	53882619	Olivera	Julián	Julibe112003@gmail.com	095390025

Prof. Barboza Gabriel

Fecha de culminación: **9/9/2022**

SEGUNDA ENTREGA


ÍNDICE

Reuniones 2º Entrega	3
Planes de Contingencias	9
Diagrama de Planificacion	23
Diagrama de KanBan	24
Metricas	25
Repositorio de GitHub	26

Reuniones


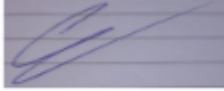
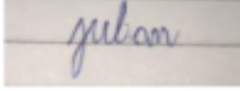

C.S.G.O



ACTA DE REUNIÓN			
ACTA N°: 10	FECHA: 16/8/2022	DURACION: 60 min	LUGAR: Discord
ASISTENTES			
Julián Olivera Camilo Soca Nahuel Galeano			
ORDEN DEL DIA			
Finalizar métricas Finalizar Scripts de Sistemas Operativos			
PUNTOS TRATADOS			
Culminamos con los scripts restantes para el Firewall de sistemas operativos Modificamos y finalizamos las métricas del proyecto			
TAREAS PENDIENTES			
Pendiente continuar con la programación de la aplicación web. Avanzar con tareas de ADA. Terminar los objetivos de las demás materias para la 2da entrega			
AGENDA TENTATIVA			
Continuar programación del proyecto.			
FIRMAS			
Coordinador 	Subcoordinador 	Integrante 1 	Integrante 2 
OBSERVACIONES			
Sin observaciones.			

C.S.G.O



ACTA DE REUNIÓN			
ACTA Nº: 12	FECHA: 28/8/2022	DURACION: 120 min	LUGAR: Discord
ASISTENTES			
Julián Olivera Camilo Soca Fabian Cardozo Nahuel Galeano			
ORDEN DEL DIA			
Comenzar planificación de las tareas de ADA y Proyecto			
PUNTOS TRATADOS			
Continuamos con la programación del proyecto, avanzando en distintas funcionalidades. Desarrollamos el nivel 1 del DFD de ADA.			
TAREAS PENDIENTES			
Continuar con la programación del sistema de SISGRAN Realizar tareas de Gestión de Proyecto			
AGENDA TENTATIVA			
Continuar programación del proyecto.			
FIRMAS			
Coordinador 	Subcoordinador 	Integrante 1 	Integrante 2 
OBSERVACIONES			
Sin observaciones.			

ITI-CETP

3ºBV

C.S.G.O




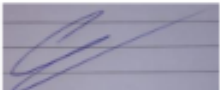
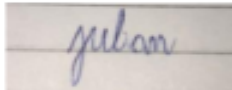

ACTA DE REUNIÓN			
ACTA N°: 12	FECHA: 04/9/2022	DURACION: 120 min	LUGAR: Discord
ASISTENTES			
Julián Olivera Camilo Soca Fabian Cardozo Nahuel Galeano			
ORDEN DEL DIA			
Realizar tareas de ADA			
PUNTOS TRATADOS			
Continuamos con la programación del proyecto, avanzando en distintas funcionalidades. Desarrollamos la maquina de estados para ADA			
TAREAS PENDIENTES			
Continuar con la programación del sistema de SISGRAN Realizar tareas de Gestión de Proyecto Terminar con las tareas de ADA			
AGENDA TENTATIVA			
Continuar programación del proyecto.			
FIRMAS			
Coordinador 	Subcoordinador 	Integrante 1 	Integrante 2 
OBSERVACIONES			
Sin observaciones.			

ITI-CETP

3°BV

C.S.G.O



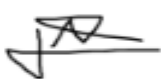

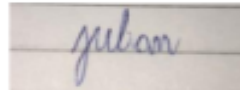

ACTA DE REUNIÓN			
ACTA N°: 13	FECHA: 06/9/2022	DURACION: 40 min	LUGAR: Discord
ASISTENTES			
Julián Olivera Camilo Soca			
ORDEN DEL DIA			
Realizar tareas de ADA Corrección de la 1ª entrega de Gestión de Proyecto			
PUNTOS TRATADOS			
Se organizo el trello de la empresa. Se corrigió los fallos en los planes de contingencias Se agrego un plan de contingencia para la sala de servidores.			
TAREAS PENDIENTES			
Continuar con la programación del sistema de SISGRAN Realizar tareas de Gestión de Proyecto Terminar con las tareas de ADA			
AGENDA TENTATIVA			
Continuar programación del proyecto.			
FIRMAS			
Coordinador 	Subcoordinador 	Integrante 1 	Integrante 2 
OBSERVACIONES			
Sin observaciones.			

ITI-CETP

3ºBV

C.S.G.O



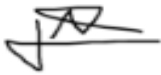

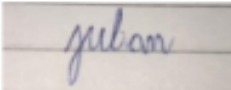

ACTA DE REUNIÓN			
ACTA N°: 14	FECHA: 07/9/2022	DURACION: 160 min	LUGAR: Discord
ASISTENTES			
Julián Olivera Camilo Soca Nahuel Galeano			
ORDEN DEL DIA			
Realizar tareas de ADA Corrección de la 1ª entrega de Gestión de Proyecto Realizar nivel 2 del DFD			
PUNTOS TRATADOS			
Se realizo el nivel 2 del DFD de ADA Se desarrollo aun mas los puntos en la primera entrega de Gestión de Proyecto. Se termino la Maquina de estados.			
TAREAS PENDIENTES			
Continuar con la programación del sistema de SISGRAN Subir las actas de reuniones para la 2ª entrega de Gestión de Proyecto. Terminar con las tareas de ADA			
AGENDA TENTATIVA			
Continuar programación del proyecto.			
FIRMAS			
Coordinador 	Subcoordinador 	Integrante 1 	Integrante 2 
OBSERVACIONES			
Sin observaciones.			

ITI-CETP

3ºBV

C.S.G.O



ACTA DE REUNIÓN			
ACTA Nº: 15	FECHA: 8/9/2022	DURACION: 120 min	LUGAR: Discord
ASISTENTES			
Julián Olivera Camilo Soca Nahuel Galeano			
ORDEN DEL DIA			
Finalizar tareas de ADA Corrección de WireFrame Verificación de archivos finales			
PUNTOS TRATADOS			
Desarrollamos el diagrama nassi-shneiderman. Corregimos el WireFrame de Diseño web			
TAREAS PENDIENTES			
Continuar con la programación del sistema de SISGRAN Terminar archivos finales			
AGENDA TENTATIVA			
Continuar programación del proyecto.			
FIRMAS			
Coordinador 	Subcoordinador 	Integrante 1 	Integrante 2 
OBSERVACIONES			
Sin observaciones.			

ITI-CETP

3ºBV

Planes de Contingencias

Plan de contingencia para acción de pandemia

Descripción del problema

A continuación se detallarán las medidas necesarias a tomar en caso de que ocurra una pandemia. Este plan de contingencia está pensado para que en caso de que ocurra una pandemia y así seguir trabajando mediante teletrabajo.

Planificación

Se deberán respetar las medidas de seguridad que se dictaminen por el bien de la salud de todos. Se otorgará acceso a plataformas de teletrabajo (en caso de cuarentena) a los trabajadores para así poder trabajar remotamente.

Recursos

- Se implementará el uso de software con licencia comercial ya sea TeamViewer o Anydesk.
- En caso de ser necesario se otorgará, un equipo portátil para que los funcionarios puedan trabajar remotamente.
- Las oficinas se sanitizan una vez al día y dentro de las mismas habrá alcohol en gel y tapabocas.

Ejecución

En caso de que ocurra una pandemia, se van a tener que tomar las siguientes medidas de seguridad:

1. Se respetarán las medidas de seguridad que se dictaminen en ese momento.
2. En caso de que las medidas sean hacer cuarentena, se llevará a cabo el teletrabajo.
3. En caso de que algún trabajador tenga que entrar a las oficinas de Sisgran, este se tendrá que realizar la prueba de antígeno para verificar que no haya dado positivo del virus y deberá de usar tapabocas dentro de las oficinas.
4. En caso de que un funcionario dé positivo, este debe realizar cuarentena estrictamente e informar que contrajo el virus. Los funcionarios que tuvieron contacto estrecho deberán de realizar el test de antígenos.

Plan de contingencia para acción de virus informáticos en sala de servidores Sisgran

Descripción del problema

A continuación se detallarán las medidas necesarias a tomar en caso de que la infraestructura informática de la cooperativa sufra de un virus informático. Este plan de contingencia está pensado para que en caso de que el servidor sufra algún percance se pueda recuperar la información lo más rápido posible y seguir trabajando.

Planificación

Se deberá de programar en el servidor rutinas cron para que se realicen respaldos diarios de manera incremental a las 22:00 horas de:

- Se respaldara la base de datos de manera incremental
- Los Logs de los distintos tipos de usuario
- Respalda los archivos de configuración de nuestro servidor

También se generan respaldos de manera semanal de:

- Del total de la base de datos
- Hacer un git push con su respectivo commit para identificar el trabajo que se realizó

Todos estos respaldos son enviados por la red al servidor secundario que se encuentra en las oficinas del directivo de sisgran utilizando rsync y crontab.

Recursos

- Crontab
- Rsync
- Cpio
- Kaspersky antivirus

Ejecución

En caso de acción de virus en la sala de servidores es importante ver en qué estado quedó el servidor, a continuación se detallan algunas verificaciones previas en caso de poder acceder a la sala

Comprobar el estado del servidor a nivel de software y los cortafuegos.

1. Se programará una revisión de los datos con el antivirus cada 24 horas antes de realizar el respaldo programado.
2. En caso de notar pérdidas o robo de información por culpa de los virus, intentar de poder solucionar las pérdidas e intentar que no se filtre la información.
3. Si no se noto vulnerabilidades en el software, se procederá a hacer un respaldo lo más pronto del mismo.
4. Si nada de esto se puede realizar, se va a tener que usar temporalmente el servidor de emergencia que está ubicado en las oficinas de Sisgran. Es necesario descargar el script que está subido al repositorio de github llamado "RestaurarServidor.sh", al correr este script se copiaran todos los respaldos al nuevo servidor y se restaurarán los datos.

Plan de contingencia para fallas en el Suministro Eléctrico en
sala de servidores Sisgran

Descripción del problema

A continuación se detallarán las medidas necesarias a tomar en caso de que la infraestructura de la cooperativa sufra una falla en su suministro eléctrico en la sala de servidores. Este plan de contingencia está pensado para que en caso de que el servidor sufra algún percance se pueda recuperar la información lo más rápido posible y seguir trabajando.

Planificación:

Se deberá de programar en el servidor rutinas cron para que se realicen respaldos diarios de manera incremental a las 22:00 horas de:

- Se respaldara la base de datos de manera incremental
- Los Logs de los distintos tipos de usuario
- Respalda los archivos de configuración de nuestro servidor

También se generan respaldos de manera semanal de:

- Del total de la base de datos
- Hacer un git push con su respectivo commit para identificar el trabajo que se realizó

Todos estos respaldos son enviados por la red al servidor secundario que se encuentra en las oficinas del directivo de sisgran utilizando rsync y crontab.

Recursos:

- Crontab
- Rsync
- Cpio

Ejecución:

En caso de una falla en el suministro eléctrico en la sala de servidores es importante ver en qué estado quedó el servidor, a continuación se detallan algunas verificaciones previas en caso de poder acceder a la sala:

1. Para los casos que se corte el suministro eléctrico se utilizará un generador de emergencia que se activará de forma automática (también se podrá activar de forma manual en caso de que se agote la reserva o el combustible) de ese modo dar tiempo de poder guardar los datos más recientes , respaldarlos y apagar los equipos de forma segura.
2. Comprobar el estado del suministro eléctrico que da al servidor
3. En caso de notar deterioro de suministro eléctrico, verificar en qué estado está el mismo.
4. Comprobar si algún elemento del hardware ha sufrido algún deterioro por causa del corte eléctrico, verificar el estado del mismo, arreglarlo o cambiarlo por uno nuevo lo antes posible.
5. Si nada de esto se puede realizar, se va a tener que usar temporalmente el servidor de emergencia que está ubicado en las oficinas de Sisgran. Es necesario descargar el script que está subido al repositorio de github llamado "RestaurarServidor.sh", al correr este script se copiaran todos los respaldos al nuevo servidor y se restaurarán los datos.

Plan de contingencia para catástrofe natural

Descripción del problema

A continuación se detallarán las medidas necesarias a tomar en caso de que haya una catástrofe natural. Este plan de contingencia está pensado para que en caso de que el edificio de Sisgran sufra algún percance se pueda recuperar la información del servidor, y reconstruir la infraestructura lo más rápido posible y seguir trabajando.

Planificación

Se deberá de programar en el servidor rutinas cron para que se realicen respaldos diarios de manera incremental a las 22:00 horas de:

- Se respaldara la base de datos de manera incremental
- Los Logs de los distintos tipos de usuario
- Respalda los archivos de configuración de nuestro servidor

También se generan respaldos de manera semanal de:

- Del total de la base de datos
- Hacer un git push con su respectivo commit para identificar el trabajo que se realizó

Todos estos respaldos son enviados por la red al servidor secundario que se encuentra en las oficinas del directivo de sisgran utilizando rsync y crontab.

Recursos

- Crontab
- Rsync
- Cpio

Ejecución

En caso de que ocurra alguna catástrofe natural en el edificio de Sisgran, a continuación se detallan algunas verificaciones previas en caso de poder ingresar al edificio:

1. En caso de derrumbe o roturas en el edificio se pondrá en contacto con los bomberos para verificar que se pueda acceder al edificio.
2. En caso de que esto sea posible, se pondrá en contacto con el arquitecto para saber los costes de refracción del edificio.
3. Si no hubo roturas en el servidor en cuanto a hardware, se recupera la información de los discos duros y se hará respaldo de los mismos.
4. En caso de que los discos duros se encuentren en estado crítico, descargar el script que está subido al repositorio de github llamado "RestaurarServidor.sh", al correr este script se copiarán todos los respaldos al nuevo servidor y se restaurarán los datos.
5. En caso de que el servidor presente fallas o ruptura a nivel de hardware se va a tener que usar temporalmente el servidor de emergencia que está ubicado en las oficinas de SISGRAN.

Plan de contingencia para Manipulación y Sabotaje en sala de servidores SISGRAN (Servidor Mysql)

Descripción del problema:

A continuación se detallarán las medidas necesarias a tomar en caso de que la infraestructura de la cooperativa sufra una manipulación no autorizada y/o sabotaje en la sala de servidores. Este plan de contingencia está pensado para que en caso de que el servidor sufra algún percance se pueda recuperar la información lo más rápido posible y seguir trabajando.

Planificación:

Se deberá de programar en el servidor rutinas cron para que se realicen respaldos diarios de manera incremental a las 22:00 horas de:

- Se respaldara la base de datos de manera incremental
- Los Logs de los distintos tipos de usuario
- Respalda los archivos de configuración de nuestro servidor

También se generan respaldos de manera semanal de:

- Del total de la base de datos
- Hacer un git push con su respectivo commit para identificar el trabajo que se realizó

Todos estos respaldos son enviados por la red al servidor secundario que se encuentra en las oficinas del directivo de SISGRAN utilizando rsync y crontab.

Recursos:

- Crontab
- Rsync
- Cpio

Ejecución:

En caso de una manipulación o sabotaje en la sala de servidores es importante ver en qué estado quedó el servidor, a continuación se detallan algunas verificaciones previas en caso de poder acceder a la sala:

1. Para evitar el ingreso de intrusos y para la seguridad de todos los trabajadores se colocarán cámaras de seguridad que estarán monitoreadas por uno o dos guardias, también se implementará una recepción en la cual se comprobará el ingreso y salida del personal.
2. Comprobar el estado del servidor a nivel de hardware y software.
3. En caso de notar deterioro o sabotaje a nivel de hardware o software, verificar en qué estado está el software o hardware, dejando constancia de los detalles por escrito.
4. Si existe manipulación o sabotaje en el software, verificar el estado del software y solventar el problema.
5. En caso de notar alguna manipulación o sabotaje en el hardware, ver el estado de estos y si es necesario cambiar el hardware por uno nuevo.
6. Si nada de esto se puede realizar, se va a tener que usar temporalmente el servidor de emergencia que está ubicado en las oficinas de SISGRAN. Es necesario descargar el script que está subido al repositorio de github llamado "RestaurarServidor.sh", al correr este script se copiarán todos los respaldos al nuevo servidor y se restaurarán los datos.

Plan de contingencia para incendio en sala de servidores SISGRAN (Servidor Mysql)

Descripción del problema:

A continuación se detallarán las medidas necesarias a tomar en caso de que la infraestructura de la cooperativa sufra un incendio en su sala de servidores. Este plan de contingencia está pensado para que en caso de que el servidor sufra algún percance se pueda recuperar la información lo más rápido posible y seguir trabajando.

Planificación:

Se deberá de programar en el servidor rutinas cron para que se realicen respaldos diarios de manera incremental a las 22:00 horas de:

- Se respaldara la base de datos de manera incremental
- Los Logs de los distintos tipos de usuario
- Respalda los archivos de configuración de nuestro servidor

También se generan respaldos de manera semanal de:

- Del total de la base de datos
- Hacer un git push con su respectivo commit para identificar el trabajo que se realizó

Todos estos respaldos son enviados por la red al servidor secundario que se encuentra en las oficinas del directivo de sisgran utilizando rsync y crontab.

Recursos:

- Crontab
- Rsync

- Cpio

Ejecución:

En caso de incendio en la sala de servidores es importante ver en qué estado quedó el servidor, a continuación se detallan algunas verificaciones previas en caso de poder acceder a la sala

1. Comprobar el estado del servidor a nivel de hardware, verificar con un multímetro el estado de los componentes.
2. Si existe algún deterioro a nivel de hardware, verificar en qué estado están los discos duros del sistema del servidor.
3. Si alguno de los discos duros está en buen estado, hacer un respaldo lo más pronto del mismo.
4. Si nada de esto se puede realizar, se va a tener que usar temporalmente el servidor de emergencia que está ubicado en las oficinas de SISGRAN. Es necesario descargar el script que está subido al repositorio de github llamado "RestaurarServidor.sh", al correr este script se copiarán todos los respaldos al nuevo servidor y se restaurarán los datos.

Plan de contingencia para Robo común de equipos y archivos en sala de servidores SISGRAN

Descripción del problema

A continuación se detallarán las medidas necesarias a tomar en caso de que la infraestructura de la cooperativa sufra de robo común de equipos o/y archivos. Este plan de contingencia está pensado para que en caso de que el servidor sufra algún percance se pueda recuperar la información lo más rápido posible y seguir trabajando.

Planificación:

Se deberá de programar en el servidor rutinas cron para que se realicen respaldos diarios de manera incremental a las 22:00 horas de:

- Se respaldara la base de datos de manera incremental
- Los Logs de los distintos tipos de usuario
- Respalda los archivos de configuración de nuestro servidor

También se generan respaldos de manera semanal de:

- Del total de la base de datos
- Hacer un git push con su respectivo commit para identificar el trabajo que se realizó

Todos estos respaldos son enviados por la red al servidor secundario que se encuentra en las oficinas del directivo de sisgran utilizando rsync y crontab.

Recursos

- Crontab
- Rsync
- Cpio

Ejecución

En caso de robo de equipos y archivos en la sala de servidores es importante saber cuales son los equipos y archivos que fueron robados, a continuación se detallan algunas verificaciones previas en caso de saber cuales son los equipos y archivos que faltan. En este caso se deberá tener presente el inventario de los equipos actuales de la cooperativa.

1. Comprobar el estado de los equipos o archivos que hay, y verificar cuales son los equipos o archivos que faltan.
2. En caso de que algún equipo esté en mal estado, intentar de poder cambiarlo por otro nuevo .
3. En caso de que algún equipo, si se dispone de equipos sin utilizar, cambiarlo por uno nuevo lo más antes posible.
4. En caso de que algún equipo sea hurtado, identificar el usuario que estaba haciendo uso de ese equipo y bloquear la cuenta que se estaba utilizando en ese mismo equipo, el administrador o el encargado de la administración de usuarios deberá asignarle una nueva contraseña y desbloquear la cuenta para que prosiga con sus labores.

Diagrama de Planificación

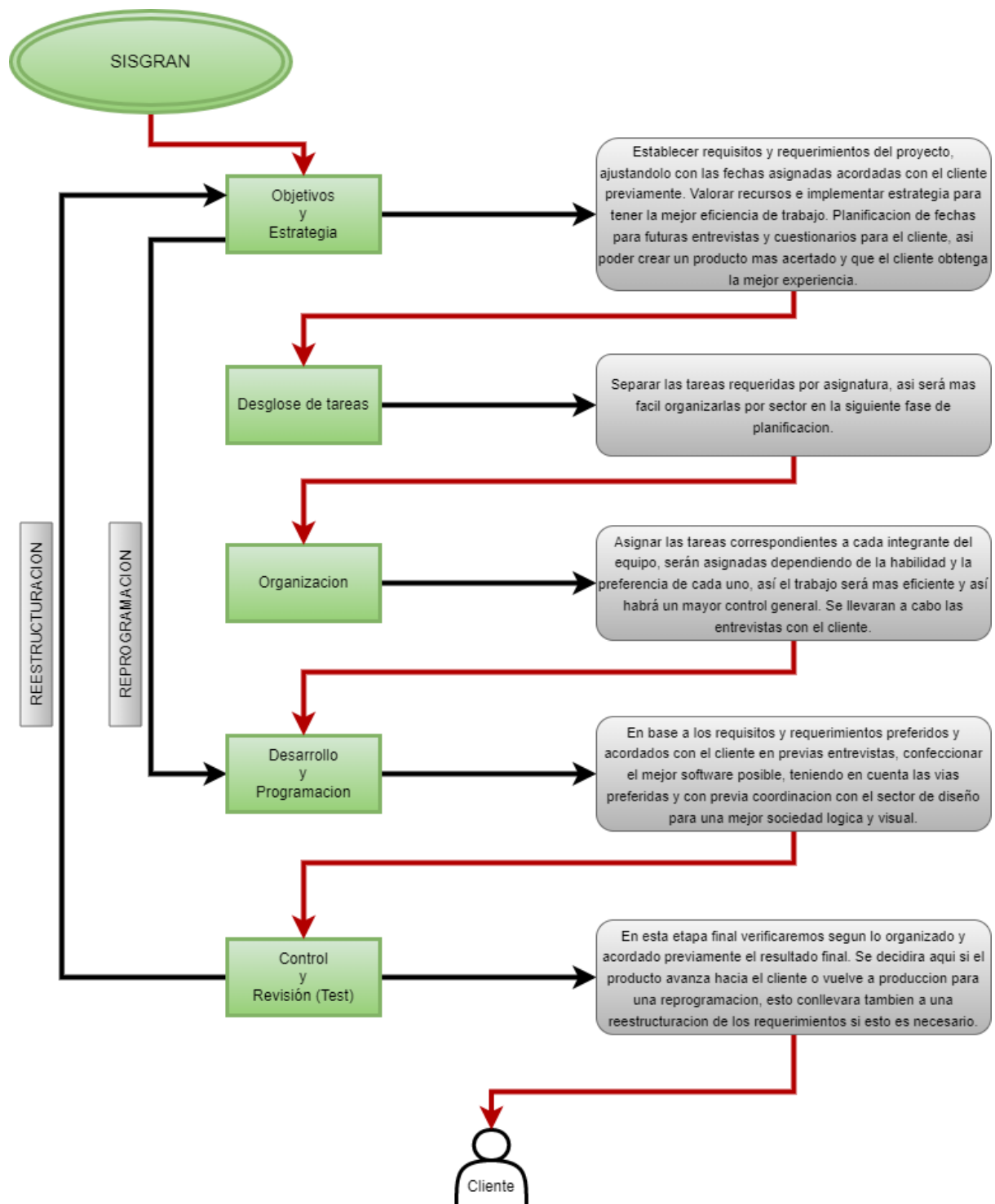
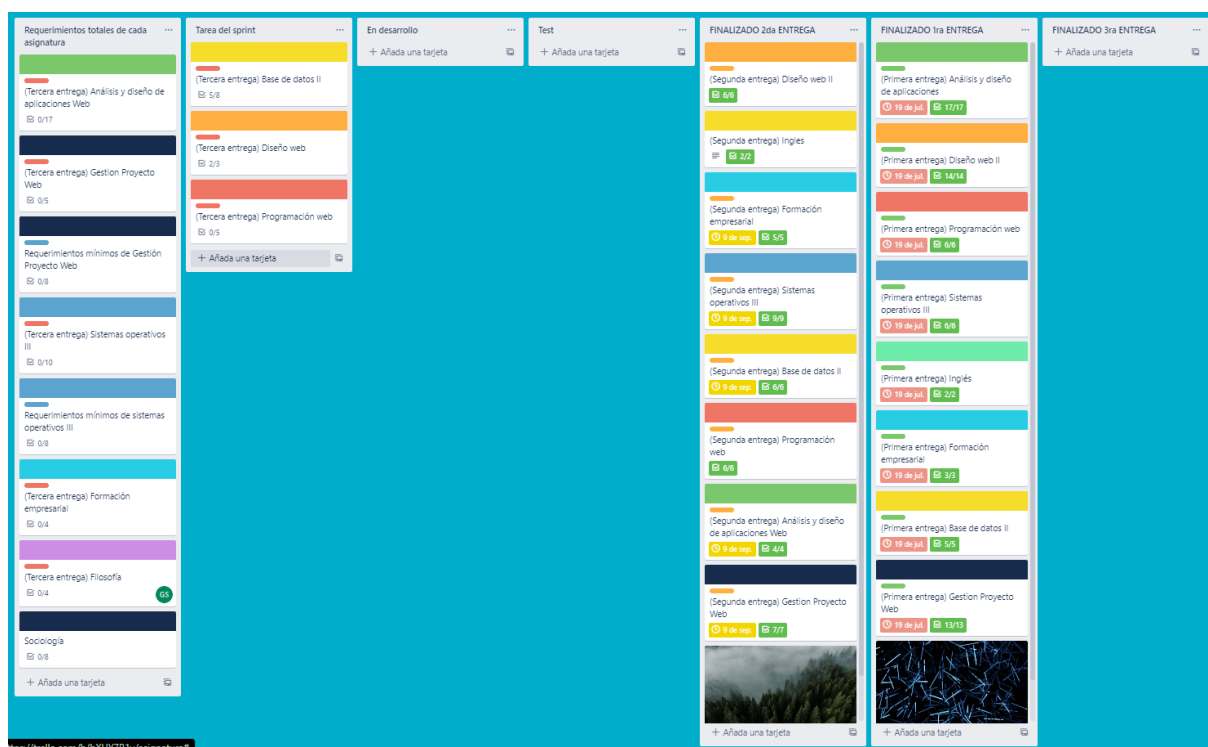


Diagrama de KanBan


(imágenes meramente ilustrativas, se adjuntan los archivos originales en el anexo del documento para una mejor visualización)




Métricas





(se adjuntan directamente los enlaces a las imágenes para una visión más limpia del documento)



Documento .xlsx:



 [Metricas de clase greensoft.xlsx](#)

Fotos:

 [admin-clientes.png](#)  [admin-empresa.png](#)  [admin-huertas.png](#)

 [buscador greensoft.PNG](#)  [directivo.png](#)  [footer.png](#)  [login greensoft.PNG](#)

 [main productos.png](#)  [registro-empresa greensoft.PNG](#)

 [registro-huerta greensoft.PNG](#)  [registro-web greensoft.PNG](#)



Repositorio GitHub

Enlace directo al repositorio de GreenSoft:

[https://github.com/GreensoftITI/Entregas-Proyecto-2022-GreenSoft.
git](https://github.com/GreensoftITI/Entregas-Proyecto-2022-GreenSoft.git)

ANEXO

Archivos originales:

(Click)

Actas de Reuniones:

- 📄 REUNION 10.pdf
- 📄 REUNION 11.pdf
- 📄 REUNION 12.pdf
- 📄 REUNION 13.pdf
- 📄 REUNION 14.pdf
- 📄 REUNION 15.pdf

KanBan:

- 📄 kanban.png

Repositorio GitHub:

<https://github.com/GreensoftITI/Entregas-Proyecto-2022-GreenSoft.git>