



S.I.G.D.

GESTIÓN DE PROYECTOS WEB

GFORZE

ROL	APELLIDO	NOMBRE	C.I	CORREO	TELÉFONO
Coordinador	Farías	Facundo	5.332.076-0	j.facuwebmaster@gmail.com	093448935
Subcoordinador	Vallejos	Diego	5.493.546-5	mizezedie@gmail.com	097302419
Integrante 1	González	Sheila	6.392.488-5	sheilagn2003@gmail.com	096247975

Docente: Barboza, Gabriel

Fecha de culminación
05/09/2022

SEGUNDA ENTREGA

Índice

Índice	2
SOLUCIÓN PROPUESTA Y PLAN DE CONTINGENCIAS	3
De acuerdo al análisis de riesgos que realizamos y a la revisión de seguridad , presentamos algunas de las sugerencias de los casos para combatir cada uno de los riesgos potenciales a los que se enfrenta nuestra empresa GFORZE.	3
RECOMENDACIONES PARA PREVENIR FALLAS EN LOS EQUIPOS	3
RECOMENDACIONES CONTRA ACCESOS NO AUTORIZADOS	4
RECOMENDACIONES A NIVEL FÍSICO	4
RECOMENDACIONES A NIVEL LÓGICO	4
RECOMENDACIONES CONTRA EL ROBO DE DATOS Y FRAUDE MEDIDAS PREVENTIVAS CONTRA EL ROBO DE DATOS	5
PROTECCIÓN PARA CORREO CORPORATIVO	5
NO DESCARGUES DOCUMENTOS SIN COMPROBAR	6
EVITA HACER CLIC EN LOS ENLACES	6
NO DAR INFORMACIÓN CONFIDENCIAL POR CORREO	6
INSTALAR HERRAMIENTAS DE PROTECCIÓN	6
Plan de contingencias	7
ACTIVIDADES PREVIAS AL DESASTRE	7
Actas de Reunión	13
CORRECCIÓN - ANEXO	15
Especificar qué versión de Fedora server.	29
Ley de protección de datos (ley número 18371)-- factibilidad legal	29
Usar comentarios propios del sistema en el drive	29
Sprint backlog (semanas y no meses, promedio de 4 semanas) -- corresponde poner el nombre del libro de quién realiza la tarea o crea dicha tarea en Trello	30
Especificar el nombre de las materias (en sistemas operativos -> sistemas operativos III).	31
Usar app: camscanner	31

Personalización de las actas de reunión(se debe de poner el logo en dicha presentación)	32
Documentación	33
Formulario de Sanción	33

SOLUCIÓN PROPUESTA Y PLAN DE CONTINGENCIAS

De acuerdo al análisis de riesgos que realizamos y a la revisión de seguridad , presentamos algunas de las sugerencias de los casos para combatir cada uno de los riesgos potenciales a los que se enfrenta nuestra empresa GFORZE.

RECOMENDACIONES PARA PREVENIR FALLAS EN LOS EQUIPOS

Principalmente optamos por designar a uno o más empleados para que dediquen un tiempo para el aprendizaje y formación, mediante la toma de cursos o aprendizaje online, para que ellos mismos sean los encargados de brindar mantenimiento necesario, preventivo y correctivo a los equipos que posee la empresa.

Además como otra opción sugerimos si es necesario contratar los servicios de una empresa que de forma periódica realice un mantenimiento preventivo a los equipos y correctivo si lo amerita la situación.

Sea cual sea la decisión que escoja, sugerimos que como mínimo se realice al menos una vez al año y llevar un control del mismo, dando así un control en la vida útil de los diferentes equipos.

Llevaremos un control de los sistemas instalados mediante la utilización de las listas de software, recomendamos que todo nuevo software que se piense instalar sea probado en un computador que previamente poseía el software estándar para las

I.S.B.O.

GFORZE

3°BA

actividades de la empresa, con la finalidad de confirmar que este nuevo software no afectará a los otros anteriormente instalados y se obtenga un buen rendimiento sin afectar al computador de forma incorrecta

RECOMENDACIONES CONTRA ACCESOS NO AUTORIZADOS

Frente a este riesgo potencial, es necesario implementar lo siguiente:

RECOMENDACIONES A NIVEL FÍSICO

El software no debe ser accesible físicamente a cualquier persona que no esté autorizado para ingresar al sistema.

Es necesario que tengamos un espacio físico donde se ubique el sistema y los equipos, con acceso restringido al personal autorizado, y que cumpla con los requisitos necesarios para su funcionamiento, como temperatura ambiental adecuada, con los equipos aislados de polvo y plagas dañinas.

RECOMENDACIONES A NIVEL LÓGICO

Deberemos de desarrollar un firewall que evite ingresos desde redes externas hacia la Red de la Empresa, para la implementación del mismo presentamos las siguientes opciones:

La primera opción consta de configurar adecuadamente el firewall que viene incluido con el sistema operativo Fedora Server. En dicho proceso deberemos de deshabilitar los servicios innecesarios para luego de esto verificar los posibles puertos que se encuentren abiertos innecesariamente para proceder a cerrarlos.

Además deberemos de informar a los usuarios del sistema sobre la política mínima de seguridad, por ejemplo, evitar claves fácilmente descifrables.

Por último debemos agregar que solo estará permitido instalar el sistema tanto en las computadoras de la empresa para el desarrollo de las actividades del mismo como en los equipos de los clientes VERIFICADOS por nuestro personal, para esto se contará con un listado sobre la entrega del sistema, el cual deberá ser seleccionado por la administrativa de la empresa, teniendo presente que la mayoría de los ataques informático no viene de fuera, sino de dentro, según lo indica las estadísticas de penetración de redes corporativas, dando así a mayor seguridad para nuestra empresa como para el sistema desarrollado.

RECOMENDACIONES CONTRA EL ROBO DE DATOS Y FRAUDE

MEDIDAS PREVENTIVAS CONTRA EL ROBO DE DATOS

El conocimiento sobre las señales y métodos de robo ayudará a los jefes a estar más conscientes de posibles problemas y así mismo promover una solución a dichos problemas de forma eficiente y lo más rápido posible sin que afecte al sistema de forma directa, las empresas pueden defenderse implementando medidas preventivas como:

- Publicar la Política de Seguridad de la empresa.
- Promover el concepto de responsabilidad del empleado.
- Exigir certificado de antecedentes.
- Capacitar bien a los empleados nuevos en los procedimientos.
- Dar énfasis a las políticas de seguridad de la empresa.
- Mantener un ambiente de trabajo limpio y ordenado.
- Desarrollar buenos canales de comunicación con los empleados para resolver quejas.
- Capacitar a los empleados para que tengan una carrera profesional dentro de la empresa.
- El liderazgo, el jefe debe poner el ejemplo en seguir las normas.

PROTECCIÓN PARA CORREO CORPORATIVO

Es recomendado el uso de una herramienta que permita implementar una infraestructura de clave pública para proteger la comunicación por correo electrónico que implique el envío de información confidencial.

Unas de las herramientas recomendadas para este propósito es el uso de [Alinto](#).

NO DESCARGUES DOCUMENTOS SIN COMPROBAR

Deberemos antes de descargar cualquier documento adjunto como fotografías, archivos, PDFs o audios, comprobar su procedencia, porque puede contener algún virus o malware que infecte el equipo. Aunque nos llegue al correo corporativo hay que fijarse bien su procedencia, nombre y el tipo de archivo que es.

EVITA HACER CLIC EN LOS ENLACES

Al estar acostumbrados a recibir en nuestro correo corporativo mensajes, y muchos de ellos con enlaces que pasan nuestros compañeros para compartir información o documentos. Por este motivo, debemos estar atentos. Los ciberdelincuentes aprovechan esto para mandar enlaces maliciosos así que tendremos que tener cuidado con todo tipo de correos que lleven links.

NO DAR INFORMACIÓN CONFIDENCIAL POR CORREO

Si bien el correo corporativo es la vía de comunicación entre trabajadores y jefes de la empresa, es importante no mandar información confidencial de la empresa o información privada por correo. Hay que recordar que ni bancos ni entidades suelen pedir información confidencial por correo electrónico y si debemos de mandar datos importantes a compañeros y jefes, es importante cifrar los archivos para que en caso de que la información se vea comprometida, no puedan acceder a ella.

INSTALAR HERRAMIENTAS DE PROTECCIÓN

Tener los equipos protegidos es una garantía de seguridad.

[Alinto](#) permite detener ataques, impide la salida de información confidencial y facilita el cifrado de documentación. Un antivirus que garantizará una protección completamente segura del correo corporativo de la empresa.

Plan de contingencias

El Plan de Contingencias, es el instrumento principal para dar una respuesta oportuna, adecuada y coordinada a una situación de emergencia causada por fenómenos destructivos de origen natural o humano.

Sin embargo, es fundamental contar con la suma de los esfuerzos de todos, cuya composición permite fortalecer y cumplir en tiempo las acciones pertinentes para prevenir y mitigar desastres en tiempo según las circunstancias señaladas y dar respuesta oportuna a las contingencias que se presenten.

Es por eso que presentaremos el siguiente plan de contingencias, son las actitudes a tener en cuenta por cada uno de los colaboradores dentro de la empresa.

ACTIVIDADES PREVIAS AL DESASTRE

Estas son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo sobre la información, las cuales nos asegurará un proceso de recuperación de nuestra empresa con el menor costo posible en tiempo y forma. A continuación detallaremos las siguiente a realizar:

I.S.B.O.

GFORZE

3°BA

Establecimiento de plan de acción

En esta fase de planeamiento estableceremos los procedimientos y normas a seguir relativos a:

Instalaciones físicas de la empresa

En caso de que se pueda producir un robo, sismo o incendio se deberán de tomar las siguientes medidas preventivas:

Robos:

- Al entrar y salir de las instalaciones se deberá observar previamente que no exista ningún individuo sospechoso.
- Queda prohibido dar información personal de los empleados o información confidencial de la organización.
- Contar con personal para resguardo de las instalaciones de la empresa.
- Instalación de alarma.

Sismos:

- Ubicar y revisar periódicamente, que se encuentren en buen estado las instalaciones de AGUA, y SISTEMA ELÉCTRICO.
- Fijar a la pared repisas, cuadros armarios, estantes, espejos y libreros. Evitar colocar objetos pesados en la parte superior de éstos, además asegurar al techo las lámparas.
- Debe de existir y ubicarse en un lugar de fácil acceso y visible los números telefónicos de emergencia y un botiquín, de ser posible un radio portátil y una linterna con pilas.
- Todo el personal debería portar siempre una identificación.
- Realizar simulacros de manera periódica.

I.S.B.O.

GFORZE

3°BA

Incendios:

- Estar siempre alerta. La mejor manera de evitar los incendios, es la prevención.
- Procurar no almacenar productos inflamables.
- Cuidar que los cables de los aparatos eléctricos se encuentren en perfectas condiciones.
- No se deben realizar demasiadas conexiones en contactos múltiples, para evitar la sobrecarga de los circuitos eléctricos.
- Por ningún motivo mojar las instalaciones eléctricas. Hay que recordar que el agua es un buen conductor de la electricidad.
- Todo contacto o interruptor debe tener siempre su tapa debidamente aislada.
- Antes de salir de la empresa, la última persona en hacerlo, deberá revisar que los aparatos eléctricos estén apagados o perfectamente desconectados.
- Queda rotundamente prohibido fumar en las instalaciones de la empresa debido a que este hábito contaminante, no deja una buena impresión en los clientes y puede causar desagrado ante los no fumadores o puede causar un incendio.
- Bajo ningún motivo se debe sustituir los fusibles por alambre o monedas, ni usar cordones eléctricos dañados o parchados.
- Contar con una alarma de incendios.
- Tener en un lugar visible y accesible un extintor contra incendios.
- Realizar simulacros de manera periódica.
- Debe de existir y ubicarse en un lugar de fácil acceso y visible los números telefónicos de emergencia y un botiquín.

Procedimiento sobre la información crítica de la empresa

Obtención y almacenamiento de los respaldos de información (BACKUPS)

Se harán copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución del Sistema.

Para lo cual se debe contar con:

- Backups del Sistema Operativo.
- Backups de Paquetes y/o Lenguajes de Programación.
- Backups de Productos Desarrollados (Considerando tanto los programas fuentes, como los programas objetos correspondientes)
 - Backups de los Datos (Bases de Datos, Índices, y todo archivo necesario para la correcta ejecución del producto desarrollado)

Para realizar los respaldos se tendrá en consideración el uso de las herramientas de encriptación para que la información pueda ser recuperada sola y exclusivamente por quién la generó. También tendremos duplicados los respaldos, esto es, mantener un respaldo a parte para mayor facilidad de recuperación, y otro respaldo fuera de las instalaciones de la empresa.

Políticas (normas y procedimientos de Backups)

El valor que tiene la información y los datos es absoluto, si falla el disco duro, el daño puede ser irreversible, puede significar la pérdida total de nuestra información, por esta razón debemos respaldar la información importante. La pérdida de información provoca gran daño de fondo como los siguientes:

- Pérdida de oportunidades de negocio
- Clientes decepcionados
- Reputación perdida

I.S.B.O.

GFORZE

3°BA

Las interrupciones se presentan de formas muy variadas: virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, hackers, errores humanos, incendios, inundaciones. Y aunque no se pueda prevenir cada una de estas interrupciones, nuestra empresa sí puede prepararse para evitar las consecuencias que éstas puedan tener ya que del tiempo que tarda en reaccionar nuestra empresa dependerá la gravedad de sus consecuencias.

ACTIVIDADES DESPUÉS DEL DESASTRE

Después de haber ocurrido el siniestro o desastre es necesario realizar las actividades que se detallan en el plan de contingencias establecido previo a su ejecución, se deben de tomar en cuenta los puntos que se detallaremos a continuación:

Evaluación de daños

Inmediatamente después que el siniestro o desastre haya concluido, deberemos evaluar la magnitud del daño que se ha producido, qué sistemas han sido afectados, qué equipos han quedado inoperativos, cuales se pueden recuperar, y en cuanto tiempo.

Para la evaluación de los daños se realizarán las preguntas o indagaciones necesarias por parte de la persona encargada de la supervisión del área en donde se produjo el siniestro.

El objetivo de establecer esta evaluación hace que los encargados de esa área en concreto puedan reconocer el tipo de desastre que se produjo, sea este en el ámbito físico o lógico.

Cuando se obtengan los resultados de la evaluación realizada, el personal encargado de la supervisión verificará en cuál de los puntos establecidos en el plan de contingencias encaja con el siniestro.

Si se tratase de un desastre en el ámbito lógico se deben verificar los siguientes puntos:

- Para la información ya existente en nuestra empresa deberemos de verificar la calidad e integridad de la misma (hacer las pruebas sobre los programas que antes del desastre funcionaban correctamente).

- Revisar la calidad e integridad de la información de respaldo.
- En lo posible intentaremos volver al estado original de la información antes del desastre.

Si se tratase de un desastre en el ámbito físico se deben verificar los siguientes puntos:

- Por una caída del suministro eléctrico, deberemos de confirmar el estado del hardware (Equipos de cómputo, Equipos de telecomunicaciones).
- Si se trata de un siniestro de fuerza mayor como son: incendios, inundaciones, maremotos, tornados, robo a la empresa; se deben seguir los lineamientos establecidos en el plan de contingencias para desastres de gran magnitud.

Evaluación de resultados

Una vez concluidas las labores de recuperación de los sistemas que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, qué circunstancias modificaron (aceleraron o entorpecieron) y cómo se comportó el personal frente a los siniestros.

En la evaluación, los resultados y el siniestro en sí, nos dará como resultado dos tipos de recomendaciones, una la retroalimentación del plan de contingencias para futuros problemas o males que puedan desmejorar a la empresa y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionó el siniestro.

Ciclo de Vida del Proyecto (Reformulación)

Después de haber visto el funcionamiento del equipo en todo el transcurso de la primera y segunda entrega, además la metodología seleccionada por el grupo que

I.S.B.O.

GFORZE

3°BA

sería la metodología ágil, podemos decir que hemos podido formular, gestionar y acoplarnos en todo el proceso de desarrollo del software.

Después del proceso de la primera entrega a petición del cliente, decidimos realizar y cómo debía ser, la reunión retrospectiva, donde nos ayudo para poder identificar muchos factores donde pudimos ver que el grupo fue mejorando y desarrollándose a medida que el mismo software lo hacía, obviamente con altibajos entre los distintos integrantes pero cada uno supo complementar el proyecto.

Lamentablemente, esta reunión de “retrospectiva” nos ayudó con algunos errores que cometimos durante todo el proceso de desarrollar el software, con respecto al sistema y a los integrantes.

Errores cometidos durante el proceso de desarrollo del software

lastimosamente sufrimos la baja del ex-coordinador Martin Mujica que por esa perdida sufrimos mucho por el desarrollo de la empresa, ya que nuestro ex-coordinador manejaba las actividades más importantes de la empresa, además si le sumamos que habían vez que las entregas o actividades con un tiempo límite no llegaban o no se entregaban en tiempo y forma, hacía imposible avanzar para suplir con las actividades y desarrollar el software de una manera ágil y rápida.

Actas de Reunion



Actas de Reuniones

I.S.B.O.

GFORZE

3°BA


Acta N*1 - SEGUNDA ENTREGA	
Fecha: 29/7/22	Hora: 17:00-20:00
Lugar: Virtual Discord	
Asistentes:	
Martin Mujica Facundo Farias Sheila Gonzalez Diego Vallejos	
Orden del día:	
Empezamos con la segunda entrega: Creación de Carpetas. Actualización del trello 4 semanas. Además se empieza con las carpetas de BASE DE DATOS II y Formación Empresarial. Repartición de Tareas.	
Puntos Tratados:	
Actualización DER BD II - RNE Forma Jurídica (Formación Empresarial).	
Firmas:	

I.S.B.O.

GFORZE

3°BA

Martin	Facundo
Sheila	Diego
Observaciones	

 <u>Actas de Reuniones</u>	
Acta N°2 - SEGUNDA ENTREGA	
Fecha: 05/08/22	Hora: 17:00-20:30
Lugar: Virtual Discord	
Asistentes:	
Facundo Farías Sheila González Diego Vallejos	
Orden del día:	
Reorganización de la distribución de materias. Observación de las carpetas ya creadas(ej: Base de Datos II). Sociología.(Segunda Entrega).	

Puntos Tratados:

Distribución de materias.
Elección de metodología de investigación.

Firmas:

	Facundo
Sheila	Diego

Observaciones

Dada la posible salida del integrante Martín Mujica ,estuvimos reorganizando la distribución de las materias.



Actas de Reuniones

Acta N°3 - SEGUNDA ENTREGA

Fecha: 12/08/22

Hora: 14:00-16:30

Lugar: UTU BRAZO ORIENTAL

Asistentes:

I.S.B.O.

GFORZE

3°BA

Facundo Farías
Sheila González
Diego Vallejos

Orden del día:

Base de Datos II
Análisis y Diseño de Aplicaciones Web

Puntos Tratados:

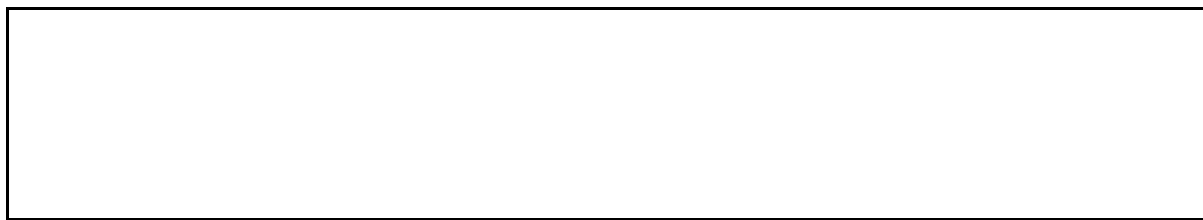
Creación y vinculación de tablas.
Modelo esencial , Diagrama de clases.

Firmas:

	Facundo
Sheila	Diego

Observaciones


Ninguna.



I.S.B.O.

GFORZE

3°BA

 <u>Actas de Reuniones</u>	
Acta N*4- SEGUNDA ENTREGA	
Fecha: 19/08/22	Hora: 14:00-16:00
Lugar: UTU BRAZO ORIENTAL	
Asistentes:	
Facundo Farías Sheila González Diego Vallejos	
Orden del día:	
Sistemas Operativos III Base de Datos II Formación Empresarial Diseño Web	
Puntos Tratados:	
Continuación del menú para los usuarios del Sistema. Estudio de roles. Matriz Foda. Wireframe.	

Firmas:

	Facundo
Sheila	Diego


Observaciones

Ninguna.

I.S.B.O.

GFORZE

3°BA

 <u>Actas de Reuniones</u>	
Acta N*5 - SEGUNDA ENTREGA	
Fecha: 23/08/22	Hora: 14:00-16:00
Lugar: UTU BRAZO ORIENTAL	
Asistentes:	
Facundo Farías Sheila González Diego Vallejos	
Orden del día:	
Sistemas Operativos III	
Puntos Tratados:	
Configuración del Firewall	

Firmas:

	Facundo
Sheila	Diego


Observaciones

Ninguna.

I.S.B.O.

GFORZE

3°BA

 <u>Actas de Reuniones</u>	
Acta N*7 - SEGUNDA ENTREGA	
Fecha: 01/09/22	Hora: 13:15-16:30
Lugar: UTU BRAZO ORIENTAL	
Asistentes:	
Facundo Farías Sheila González Diego Vallejos	
Orden del día:	
Programación web Base de Datos II Sistemas Operativos III Formación Empresarial Sociología Inglés	
Puntos Tratados:	
Estructura del proyecto en 3 capas siguiendo los conceptos de la POO. Finalizamos las carpetas de Formación Empresarial, Sociología, Inglés y Base de Datos II	

Firmas:

	Facundo
Sheila	Diego


Observaciones

Ninguna.

I.S.B.O.

GFORZE

3°BA

 <u>Actas de Reuniones</u>	
Acta N°8 - SEGUNDA ENTREGA	
Fecha: 00/09/22	Hora: 13:15-16:30
Lugar: UTU BRAZO ORIENTAL	
Asistentes:	
Facundo Farías Sheila González Diego Vallejos	
Orden del día:	
Puntos Tratados:	

Firmas:

	Facundo
Sheila	Diego

Observaciones

Ninguna.

CORRECCIÓN - ANEXO

Especificar qué versión de Fedora server.

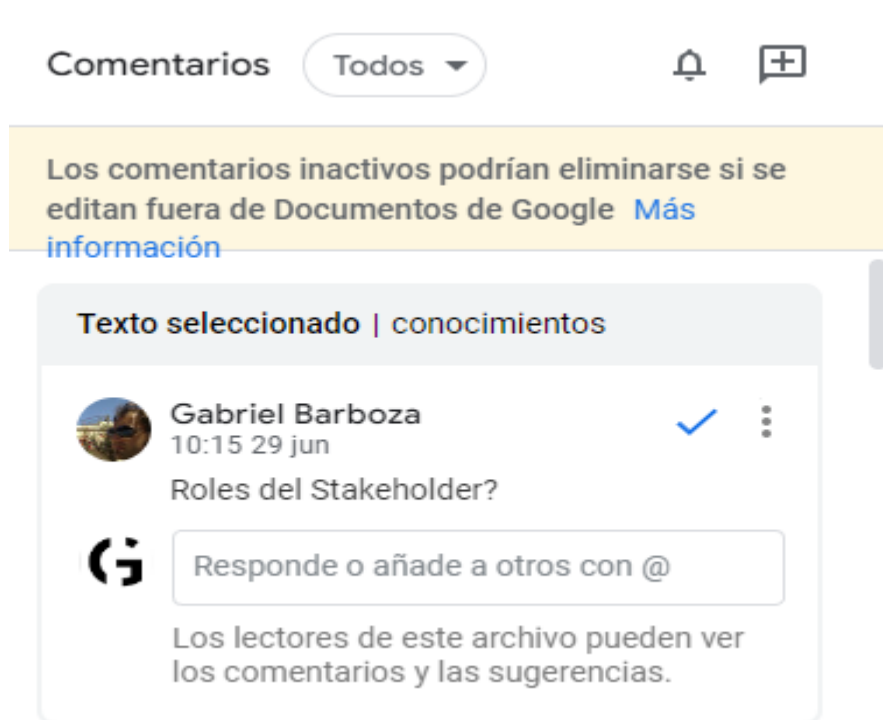
Fedora Server 36. Especificado [Primera entrega](#) Factibilidad Operativa ADA.

Ley de protección de datos (ley número 18371)-- factibilidad legal

Ley número 18371 especificada en Factibilidad Legal [Primera entrega](#).

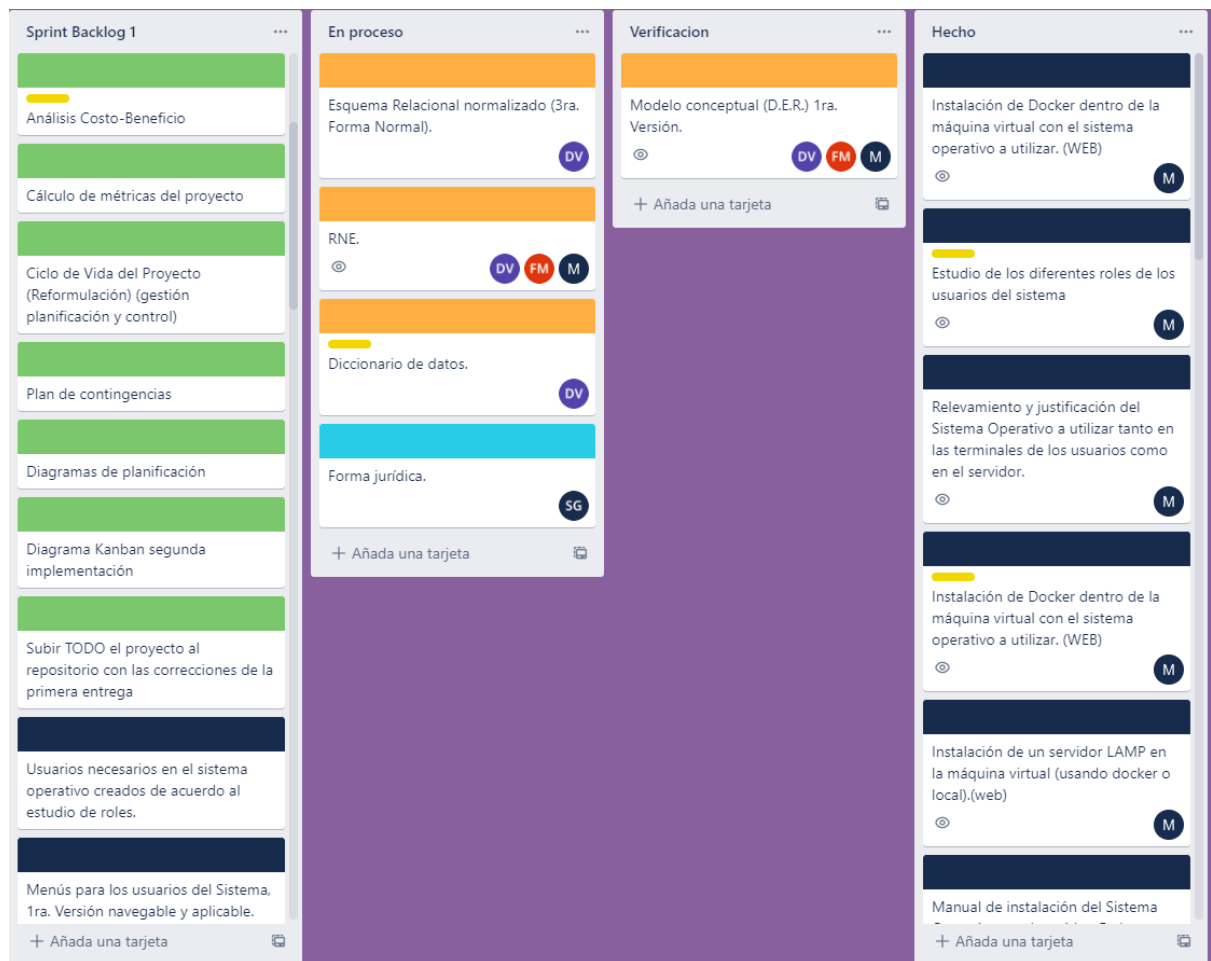
Usar comentarios propios del sistema en el drive

Comentarios fijados por una funcionalidad de drive [Primera entrega](#).



**Sprint backlog (semanas y no meses, promedio de 4 semanas) --
corresponde poner el nombre del libro de quién realiza la tarea o
crea dicha tarea en Trello**

Trello actualizado Sprint Backlog de 4 semanas (Trello de la Segunda Entrega),
Trello con todos los usuarios de nuestro equipo y trabajos comentados desde el
28/8/22.



Especificar el nombre de las materias (en sistemas operativos -> sistemas operativos III).

Nombre actualizado correspondientemente.

Usar app: camscanner

camscanner utilizado para escanear un documento formal.


I.S.B.O.

GFORZE


3°BA

Personalización de las actas de reunión(se debe de poner el logo en dicha presentación)

Actas de reuniones actualizadas tanto en la primera entrega como en la segunda.



Actas de Reunión

	
<u>Actas de Reunión Formal</u>	
Acta N°1	
Fecha: 06/05/22	Hora: 17:00
Lugar: Virtual Discord	
Asistentes:	
Martin Mujica Facundo Farias Sheila Gonzalez Diego Vallejos	
Orden del dia:	
Lectura del proyecto. Determinar el nombre del proyecto. Creación del correo electrónico. Creación de la carta de presentación de todas las materias.	
Puntos Tratados:	
Se realizaron todos los puntos anteriores en una sola reunión	
Firmas:	
Martin	Facundo
Sheila	Diego
Observaciones	

Documentación

Formulario de Sanción

[Virtual, Discord, 1/08/22]

Señor/a [Vallejos, Diego]

CI [5.493.546-5]

Asunto: Carta de Sanción.

La dirección de esta empresa ha tenido conocimiento de incumplimientos de la normas establecidas.

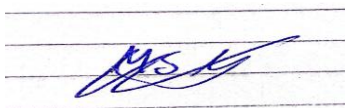
Los hechos se han desarrollado como siguen:

Llegar a tiempo con sus tareas, obviamente la tarea puede variar según cada uno por lo cual la idea sería avisar si van a tardar más del tiempo estimado.

Por todo ello y considerando que su conducta se encuentra tipificada como falta[Penalizable] según las normas establecidas, le comunicamos que usted es sancionado/a con amonestación por escrito.

Por último advertir que la reincidencia en faltas de esta u otra naturaleza serán sancionadas en lo sucesivo con mayor rigor.

Atentamente,
Mujica, Martin
Firma:

A handwritten signature in blue ink, appearing to read 'Mujica', written over three horizontal lines.

I.S.B.O.

GFORZE

3°BA

Referencias Bibliográficas

Para el plan de contingencias utilizamos como referencia o ayuda para desarrollar dicha actividad:

[Plan de contingencia | ¿Qué es un plan de contingencia? \(emprendepyme.net\)](http://emprendepyme.net)

[Como elaborar un plan de contingencia - YouTube](#)

Para el desarrollo de la actividad “Ciclo de Vida del Proyecto (Reformulación) (gestión planificación y control)” utilizamos como referencia o ayuda para desarrollar dicha actividad, el (los) siguiente(s) sitios: