PLAN CONTINGENCIAL

1. Introducción:

En este documento se enlistarán los riesgos, las estrategias de prevención y mitigación del impacto que dichos riesgos enlistados pueden tener sobre nuestro proyecto tecnológico.

2. Alcances y limitaciones:

Alcances:
Los alcances con el plan contingencial son:

- Cubrir todos los riesgos posibles con el propósito de evitar cualquier percance que perjudique el desarrollo del proyecto de tecnológico.
- Crear estrategias de mitigación para reducir el impacto de dichos riesgos.
- Desarrollar de manera efectiva las estrategias para obtener un buen resultado.

Limitaciones:
Las limitaciones son:

- Que los riesgos que ocurran estén fuera del alcance planeado.
- Que el equipo tecnológico no cubra con las necesidades requeridas.
- Que uno o mas miembros del equipo no cuenten con las capacitaciones solicitadas.

3. Identificación de riesgos:

En un proyecto tecnológico puede tener muchos riesgos en su realización, estos pueden ser:

1. Daño en el equipo.
2. Malware.
3. Perdida del código.
4. Robo del equipo.
5. Errores de sintaxis.
6. Muerte de un miembro del equipo.
7. Falta de capacitaciones de los desarrolladores.
8. Problemas emocionales.
9. Desastres naturales.
10. Entregas tardías.

4. **Evaluación de los riesgos:**

Según la identificación de riesgos determinamos lo siguiente:

- Los riesgos tecnológicos identificados tienen un efecto __**catastrófico**___ y una probabilidad _**no muy probable**__, algunos, como es el caso del riesgo __**3**__, que posee un efecto __**catastrófico**__ y probabilidad __**moderada**__, por lo que los tratamos con estrategias diferentes; según el esquema de valoración:

Riesgos Tecnológicos	Estrategias
1	Tener el proyecto tecnológico en dos o más equipos que tengan las mismas capacidades en caso de que se dañe el equipo principal.
2	No entrar a páginas web que no sean de total confianza.
3	Guardar más de una copia de seguridad y que cada miembro del equipo cuente con una de las copias.

- Los riesgos operativos identificados tienen un efecto __**leve**___ y una probabilidad _**alta**__, algunos, como es el caso del riesgo __**6**__, que posee un efecto __**leve**__ y probabilidad __**alta**__, por lo que los tratamos con estrategias diferentes; según el esquema de valoración:

Riesgos operativos	Estrategias
5	Programar de día y organizar bien nuestro tiempo para hacer las cosas con calma y lograr identificar los errores, ya que son muy probables que sucedan.
7	Contar con un equipo capacitado en diversas áreas para cubrir cada una de las necesidades.

- Los riesgos desconocidos tienen un efecto __**catastrófico**___ y una probabilidad _**no muy probable**__, algunos, como es el caso del riesgo __**4**_, que posee un efecto __**catastrófico**__ y probabilidad __**moderada**__, por lo que los tratamos con estrategias diferentes; según el esquema de valoración:

Riesgos desconocidos	Estrategias
4	1- Resguardar el equipo tecnológico en un lugar seguro
6	Que una persona cuente con las mismas capacidades para cubrir el área de trabajo de la persona fallecida.

- Los riesgos externos identificados tienen un efecto **__leve___** y una probabilidad **_moderada__**, algunos, como es el caso del riesgo **__10**_, que posee un efecto **__leve**__ y probabilidad **__moderada__**, por lo que los tratamos con estrategias diferentes; según el esquema de valoración:

Riesgos externos	Estrategias
8	Contar con apoyo emocional de parte de amigos o familiares.
9	Tener los dispositivos debidamente resguardados ya que los desastres naturales son totalmente inesperados.

- Los riesgos de calendario identificados tienen un efecto **__leve___** y una probabilidad **_no muy probable_**, algunos, como es el caso del riesgo **__11**__, que posee un efecto **__leve**_ y probabilidad **__moderada__**, por lo que los tratamos con estrategias diferentes; según el esquema de valoración:

Riesgos de calendario	Estrategias
10	1- Organizar bien el tiempo y trabajar en los horarios estipulados.

5. Planificar riesgos:

Tipo de riesgo	Descripción del riesgo	Efecto	Probabilidad	Estrategia
Tecnológico	Daño en el equipo que puede ocurrir por muchos factores	Catastrófico	No muy probable	Tener todas las medidas de seguridad y mantenimiento del equipo. Tener el proyecto en dos o más equipos que tengan las mismas capacidades para poder continuar con el proyecto.
Tecnológico	Ingreso de Malware en el dispositivo	Catastrófico	No muy probable	Instalar un antivirus para para proteger nuestro dispositivo.
Tecnológico	Perdida del código y no tener una copia de seguridad.	Catastrófico	Moderada	Guardar mas de una copia de seguridad en varios dispositivos.
Operativo	Error de sintaxis por parte de los desarrolladores, que impediría el avance de proyecto.	Leve	Alta	Tener un buen conocimiento de lógica y organizar bien el tiempo para hacer las cosas con calma y tener tiempo de revisar los errores. Además de programar de día y con la mente descansada.
Operativo	Falta de capacitaciones de los desarrolladores en algún lenguaje de programación solicitado	Leve	Moderada	Contar con un equipo con personas preparadas en distintas áreas para cubrir todas las necesidades. Si es individual prepararse en diversas áreas de la programación.
Desconocido	Posibilidad de sufrir un asalto y se roben el equipo	Catastrófico	No muy probable	Informar a las autoridades del

				ministerio de educación. Tener el código en otro dispositivo
Desconocido	Fallecimiento de un miembro del equipo, como, por ejemplo: el programador principal.	Catastrófico	No muy probable	Que uno o dos miembros mas del equipo cuenten con las mismas capacitaciones para que puedan continuar con el proyecto.
Externo	Problemas emocionales, como desánimos o frustraciones que impidan el avance del proyecto.	Leve	Alta	Organizar tiempos de descanso y entretenimiento.
Externo	Desastres naturales en la región que causen daños materiales.	Catastrófico	Moderada	Guardar copias de seguridad en caso de que se dañe el equipo de trabajo.
De Calendario	Entregas fuera del lapso estipulado con el cliente.	Catastrófico	Moderada	Organizar las actividades en un cronograma y cumplirlas lo mejor posible.

6. Supervisar los riesgos:

Actividad	Persona encargada	Fecha de inicio	Fecha final
Creación de copia de seguridad.	Gustavo Retana	15-10-2022	15-10-2022
Instalación del antivirus	Gustavo Retana	30-08-2022	30-08-2022
Verificar la seguridad y confiabilidad de las páginas de investigación	Gabriela olmedo	En cada investigación	En cada investigación
Creación del cronograma de actividades	Katherine Escobar	05-09-2022	19-09-2022
Organizar reuniones y tiempos de descanso	Team	Una vez por semana	Una vez por semana

7. Conclusión final:

En conclusión, es muy importante la creación de un plan contingencial ya que nos ayuda a identificar todos los riesgos posibles que puedan ocurrir en el desarrollo de nuestro proyecto tecnológico, analizar los efectos e impactos pueden tener y buscar estrategias de prevención y mitigación ante los riesgos, así como desarrolladores de software estaremos atentos a los problemas que surjan, teniendo medidas de resolverlo o mitigarlo para que el cliente final este satisfecho con el producto que estamos vendiendo.